Freie Universität Berlin

Doctoral Dissertation

Efficient Security and Privacy Protection for Large-scale Wireless Indoor Positioning Applications

Dissertation zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften (Dr. rer. nat.) am Fachbereich Mathematik und Informatik der Freien Universität Berlin

vorgelegt von

Mohammad Fal Sadikin

Datum der Disputation: 27. November 2015

Gutachter: Prof. Dr. Marcel Kyas
Department of Computer Science
Freie Universität Berlin

Prof. Ph.D. Rie Shigetomi YAMAGUCHI
Graduate School of Information Science and Technology
The University of Tokyo

Prof. Dr. Donghyun Kim
Department of Mathematics and Physics
North Carolina Central University

Eidesstattliche Erklärung

Ich versichere, dass ich die Doktorarbeit selbständig verfasst, und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit hat keiner anderen Prüfungsbehörde vorgelegen.

Mir ist bekannt, dass bei Verwendung von Inhalten aus dem Internet ich diese zu kennzeichnen und einen Ausdruck mit Angabe des Datums sowie der Internet-Adresse als Anhang der Doktorarbeit anzugeben habe.

I hereby declare to have written this thesis on my own. I have used no other literature and resources than the ones referenced. All text passages that are literal or logical copies from other publications have been marked accordingly. All figures and pictures have been created by me or their sources are referenced accordingly. This thesis has not been submitted in the same or a similar version to any other examination board.

Berlin, den Dezember 3, 2015

Mohammad Fal Sadikin

Abstract

The emerging of Wireless Indoor Positioning (WIP) technology has become prominent solution in the context of location awareness applications. Nevertheless, WIP system introduces tremendous security and privacy problem due to inherent vulnerabilities derived from various aspects. One of significant aspects is the vulnerable nature of wireless technology that every party has access to the system. In addition, the use of positioning and tracking technics can reveal sensitive information including the most critical one that related to client's privacy. Taking into consideration, enforcing standard security and privacy method such as traditional Public Key Infrastructure (PKI) is not suitable for the WIP system that has very strict requirements in term of resource availability (i.e. processing power, data-rate, battery/power supply, and memory storage). On the other hand, most of nowadays security and privacy solutions only focus on single aspect of security and privacy threats (e.g. only focusing on particular threats such as cloning attacks), rather than providing an integrity solution that covers the broader aspects of WIP problem. Indeed, the vulnerability in WIP system is inherent in complex aspects, reaching from physical layer threats (e.g. relay attacks), network and transport layer threats (e.g. cloning, impersonation, spoofing, resource consumption attacks, protocol attacks such as various technic of man-in-the-middle attacks, etc.), application layer threats (e.g. unauthorized information reading, unauthorized tracking, malicious code injection, etc.), to multi-layer threats such as denial-of-service, social engineering, traffic analysis, various techniques of replay attacks, and so forth.

Although it is rather unrealistic to provide a solution that can address the whole aspects of security and privacy problem, however the protection can be enhanced by providing a suitable solution that can cover the broader scopes of the addressed problem and combining it with corresponding policy enforcement. This thesis introduces a novel solution that can be relied to mitigate multi-layer security and privacy problem in broader aspects. The following list outlines our main contributions in order to achieve suitable and efficient security and privacy achievement in the constrained nature of WIP system.

- Investigation of the WIP application vulnerabilities both from security and privacy point of view in multi-layer problem. In particular, we collect various risks and threats as well as the attack scenarios that are susceptible for the WIP applications.

- The proposed design of security and privacy protocol tailored to the constrained nature of WIP system. Such protocol enables access control with mutual authentication and verification, as well as identity protection. Therefore, it can be relied to mitigate various threats in multi-aspects of WIP system.

- Key management System for the constrained nature of WIP system. We design corresponding service of the proposed authentication protocol to enable security update (i.e. private key), which is applicable for the system's limited resources.

- The evaluation of the security and privacy method. We prove that our proposed solution is suitable to provide protection from various aspects of security risks and threats inherited from the use of WIP technology.

- The performance evaluation of the proposed security and privacy method. We evaluate the cryptographic processing in order to prove that the processing overhead is feasible to be applied in the constrained nature of WIP system. In addition, we evaluate other parameters including the communication overhead and the memory storage in order to ensure that our proposed solution is suitable to tackle the challenge related to data-rate availability and limited memory storage.

In general, our analyses present that our proposed security and privacy solution can mitigate the addressed problem in broader aspects of WIP problem. In addition, the propose solutions are applicable for the constrained nature of WIP system.

Acknowledgement

First and foremost, I would like to thank Prof. Dr. Marcel Kyas for the opportunity to work in his research group, and giving me more space to explore new frontiers with great freedom to work according to my own fashion. It is the most important aspect that grows my creativity and confident to lead the completion of my Doctoral research work. In particular, I would like to thank him for his trust to let me work independently, as well as his dedication, encouragement, and for his comments which helped me improve this thesis.

I am also very grateful to have two external reviewers, Prof. Ph.D. Rie Shigetomi Yamaguchi from the University of Tokyo, and Prof. Dr. Donghyun Kim from the North Carolina Central University. Their comments were very worthwhile that contribute to this thesis. It was my pleasure to work with them and I would like to thank for that.

The unforgettable time that I spent at Computer Systems and Telematics research group would not be as nice as without all the research group members. I firstly would like to thank to M.Sc. Simon Schmitt for his friendship, and offered me so many helps during my time at this research group. Moreover, I would like to thank to the boards and senior members that contributed to the completion of my doctoral degree. In particular, I would like to thank to Prof. Dr.-Ing. Jochen Schiller, Prof. Dr. Katinka Wolter, and Dr.-Ing. Achim Liers for agreeing to act as the promotion committee. I express to thank to Ms. Stefanie Bahe for the administrative supports. I would like also to thank to all my colleagues for the fruitful friendship, discussions, all your friendly helps, particularly to Dipl.-Ing. (FH) Stephan Adler, Dr. Qiushi Wang, Dr. Yang Yuan, Dr. Yubin Zhao, Dr. Huaming Wu, and Mr. Agus Kurniawan.

I highly appreciate for my very first time opportunity to conduct research in Germany at the Fraunhofer Institute for Open Communication Systems (Fraunhofer FOKUS), particularly at the Next Generation Network Infrastructures (NGNI) Competence Center. In this regards, I would like to thank to Prof. Dr.-Ing. Thomas Magedanz for giving me opportunity to work under his supervision in the FP7 EU Project. I learned a lot of things during my time at this institute and such experience was one of the most important aspects that lead me to successfully pursue this doctoral achievement.

Last but not least, I express thank to my beloved wife and son, who always support and bring happiness to my life. Special thanks to dear our beloved and wonderful parents who have educated us, my bother Dr.-Ing. Syawaluddin Akbar who always encourage me, my sister dr. Heni Fitriani, and my two young brothers Mr. Yumriz Idznillah, Bsc. and Mr. Idul Rizhan (PhD candidate), for their support and affection.

.

Contents

Chapter 1

Introduction

1.1. Motivation

Wireless Indoor Positioning (WIP) is a prominent technology that is used in wide range of application domains. It is a tracking application that has been deployed for various purposes, reaching from industrial applications, health care, shopping, to the critical applications including application for security and protection. Nevertheless, WIP system introduces tremendous security and privacy problems in various aspects. On the other hand, WIP devices are mostly mobile node that have limited capabilities in term of processing power, bandwidth/data-rate, memory storage, communication overhead and power supply/battery. Such limited capabilities make the enforcement of common security solutions (e.g. using standard Transport Layer Security (TLS/SSL)) are not affordable to be applied for. Indeed, using standard Public Key Infrastructure (PKI) is too heavy-weight and can drainage the system's limited resources, affecting the lifetime of the mobile devices expire too early or even causing communications failures. On the other hand, nowadays state of the art solutions have particular drawbacks in term of providing suitable solution that can covers broader aspects of security and privacy in the WIP system.

In term of security issues, an adversary may exploit the vulnerability nature of wireless communication. Certainly, the wireless channel that is broadcasted makes any party within the range has access to the communication system. In this case, the adversary can observe and elicit the sensitive information on the broadcasted channel in order to perform various attacks, including various technics of Man-in-the-Middle (MITM) attacks (e.g. Denial-of-Service (DoS), impersonation, spoofing, etc.). One example attack scenario is the vulnerabilities related to the limited battery and bandwidth availability. Take into account that WIP system incorporates to various mobile nodes with limited capabilities, this application system is also highly susceptible to various threats on resource consumption attacks. Such attacks aim at overburdening and thwarting the system' services by flooding the amount of packets addressed to the mobile nodes. In this regards, such scenario can waste the limited bandwidth as well as drain the limited battery power, in order to target Denial-of-Service (DoS) to particular node.

In term of privacy issues, an adversary may reveal sensitive information such as the user's identity, and use it to perform further malicious activities such as unauthorized tracking, an authorized application data reading, revealing the user or company's activities and so on. Thus In general, this thesis aims at providing a novel solution to cope with the broader aspects of security and privacy problem, which is also tailored to specific challenges and requirements in WIP system.

1.2. Vulnerabilities and Problem Statement

Wireless Indoor Positioning system introduces tremendous security and privacy problems derived from various aspects. It ranges from the vulnerabilities that are inherited from the use of wireless communications, to the specific security and privacy problems derived from the use of tracking or positioning techniques itself. Furthermore, the system's limited resources of the WIP applications introduces a complex challenges in term of providing efficient security and privacy solution that can protect the whole system from various known threats and risks. In addition, the deployment of WIP applications in large-scale and distributed system definitely introduces more challenges in the face of establishing integrity protection as well as providing the security management. The following list describes the challenges that should be considered to design the security and privacy protection tailored to the constrained nature of WIP system.

- *Vulnerable nature of wireless communication*. The broadcast nature of wireless channel gives an adversary chance to perform various attacks based on active and passive eeavesdroppings including various technics of Man-in-the-Middle attacks, Denial-of-Service, MAC Address spoofing, Replay attack, impersonation, etc.

- *Limited CPU power*. The WIP clients or end-devices (i.e. WIP node or RFID tag) are typically low-cost devices with limited capability in term of clock frequency. Some of advanced end-devices (i.e. standard sensor platforms such as imote2) have sufficient CPU options ranging from 104 MHz, 208 MHz, 312 MHz to 416 MHz. Nevertheless, such CPU options are still not affordable to be used in the system that relies on upper layer method of standard security solution such as using TLS/SSL. Indeed, the standard method introduces high computation overhead that overburdens the limited capabilities of CPU, particularly in large-scale system where the security process including authentication and authorization as well as key management update might be frequently required.

- *Limited battery*. Most of common security solution partially relies on upper layer method (e.g. application layer). The use of upper layer method introduces high communication overhead since the size and number of fragmentation packets exchanged during the authentication process is higher. This issue mainly causes drainage of battery energy affecting the lifetime of the WIP's device expires soon.

- *Limited memory storage*. WIP is a prominent technology that is used in wide area application domains. One of them is embedded system which is integrated to Wireless Sensor Networks (WSN) applications. In this regards, such WIP system requires more memory storage to handle various parameter including application data and the security properties. On the other hand, most of standard embedded devices including sensor node have very limited memory storage. Therefore, the security and privacy method should provide efficient solution which requires less memory storage. Thus, the available memory storage is still spacious to handle other process including the data applications.

- *Low bandwidth/data-rate*. In order to achieve low-cost and efficient communication, most of end-devices in the WIP system are connected over low data-rate ubiquitous communication such as various standards IEEE 802.15.4. This limitation introduces more challenges, as the security method should provide sufficient integrity protection with various features including access-control, authentication, authorization, identity protection, security resistance from various threats, as well as providing efficient security management services. However in other hand, all security features must be feasible to be enforced over low-speed data connection.

- *Heterogeneity.* Some of WIP systems are heterogonous networks which consist of various access technologies, ranging from the use of WLAN technologies such as IEEE 802.11 standards, to WPAN technologies such as various standards of IEEE 802.15.4. Moreover, the WIP components are also heterogeneous devices with wide ranges of hardware capabilities. Thus, the security and privacy solution must have flexibility to be implemented over such heterogonous system.

- *High risk on various aspects of security and privacy threats*. The use of positioning technics over wireless communications (e.g. RSSI, Time of Arrival (ToA), Angle of Arrival (AoA) or using RFID) introduces specific security and privacy problems. For instance, an adversary may observe the meta-data of transmitted packets to infer the location of particular node based on the RSSI value or TOA. In addition, the adversary can reveal the movement profile and activities of particular users by identifying the MAC address. Furthermore, the WIP system is even highly susceptible from various threats related to physical manipulation. Take into account, most of end-devices are mostly placed in unsupervised environments, an adversary may steal the unsupervised devices and copy all security parameters in order to impersonate or compromise the legitimate devices. In this case an adversary may spoof the application such as manipulating the data application or reporting wrong location. The comprehensive problem of security and privacy in various aspects will be discussed in the chapter 2 of this thesis.

- *Insider threat*s. In WIP system, legitimate users may misuse their credentials in order to fools the system applications. In this regards, they may impersonate as other legitimate user to perform malicious activities such as reporting wrong attendance or even engage in some activities that are authorized only to specific users. In addition, the naughty insider also introduces more challenges in protecting the other user privacy, as the insider may use their privilege to eavesdrop the communication in order to reveal or access the sensitive information of other users such as movement profile and activities.

- *Large-scale distributed system*. The large number of deployed devices affects the enforcement of security and privacy requirements are more arduous. The addressed security and privacy threats inherited both from the vulnerable nature of wireless communication and the threats based on the use of positioning technics itself become more susceptible. Furthermore, various requirements such as security process (i.e. cryptographic processing) or even security update (i.e. key management service) might be more frequently required. Such issues implicate the system's limited resources of WIP system, which may impact to the system failure. Thus, the proposed security and privacy method should be applicable for large-scale distributed system.

- *Key management problem*. Authentication method is a complex security feature since it requires key management service. Most of common key management solutions such as using standard Public Key Infrastructure (PKI) rely on upper layer method. Therefore it is not doable for the constrained nature of WIP system. Indeed, the use of upper layer method is too heavy-weight solution that introduces expensive computation and communication overhead. On the other hand, conducting manual key management method by recalling the all WIP nodes in order to update their security properties are not feasible particularly in the large-scale system. The challenges become more complicated since security update may be required more frequently in large-scale scenario, however the bandwidth may not sufficiently provided. Thus, the proposed key management system (KMS) should satisfy the requirement in large scale scenario (e.g. the KMS should be available every time the security update is required).

In general, WIP system is highly susceptible from various security and privacy threats ranging from the threats that arise from physical layer vulnerabilities (e.g. relay attacks, active jamming, physical manipulation, etc.), network layer vulnerabilities (e.g. cloning, impersonation, spoofing, resource consumption attacks, protocol attacks such as various technic of man-in-the-middle attacks, etc.), application layer vulnerabilities (e.g. unauthorized tracking, malicious code injection, unauthorized data reading, malicious code injection such as SQL injection attacks, etc.) to various threats that are elicited from the exploitation of multi-layer problem including replay attacks, traffic analysis attacks, crypto analysis attacks, covert channel, social engineering, and so on. Nevertheless, enforcing security and privacy protection in the constrained nature of WIP is a complex problem. Common security solutions are not suitable since most of them require higher computation and communication resources. In other words, such tremendous security problem introduce the need on novel security and privacy protection that is more suitable to be implemented in system's limited resources such as limited date-rate, limited memory storage, limited CPU power and limited battery.

During the last decade, various research works have been introduced to solve the addressed problem, particularly in the system's limited resources including RFID based applications and embedded-device system such as WSN applications. Nevertheless, most of them rigidly focus on a single aspect of the security and privacy problem.

For instance, some of research works strictly focus to provide solution for privacy problem with various methods including using anonymous technics, location verification, and blocker techniques [13-20]. Nevertheless, such solutions are designed without considering other security aspects such as mutual authentication and verification, access control and key management system. Definitely, privacy preserving without any additional security features is considered as gammy protection since it left tremendous security problem. Furthermore, the similar cases that some of research works only focus to solve particular security threats such as cloning attacks or impersonations [3-6][8], without considering other aspects of security and privacy issues. In general, providing solution by just focusing on one or few aspects of security and privacy is not sufficient to achieve the integrity protection.

Moreover, various research works have demonstrated the weaknesses of some of security and privacy methods that are claimed as good solutions. One of example solutions is a RFID authentication protocol based on elliptic curve cryptography named EC-RAC [9]. The protocol is designed to minimize the computation workload, as well as to tackle several problems in RFID communications including scalability, cloning attacks and privacy problem. Nevertheless, just short time after, a research work show that this protocol has significant weaknesses that a tag can be tracked even can be impersonated if the one has been eavesdropped [10]. Further research works that aims at improving EC-RAC method have been proposed in [1][2]. In these works, the authors add several features such as protection for Replay Attack (Impersonation Attack), Security against the tracking attack, and Backward/Forward Un-traceability. Nevertheless, at least we found that two research works have broken the updated versions of EC-RAC methods by demonstrating various analyses that invalidate the claimed features in respect to privacy [11][12]. More detail about state-of-the-art security and privacy solutions are discussed in the chapter 2 of this dissertation.

It is to be noted that solving the entire security and privacy problem in WIP system is rather unrealistic goal. However, the security and privacy protection can be enhanced by providing a solution that can cover a broader scope of security and privacy problem and combining the solution with corresponding policy enforcement. In general, The WIP system needs a novel solution that can be relied to mitigate multi-layer security and privacy problem in broader aspects.

1.3. Contributions

The main contributions of this thesis address the broader aspects of security and privacy challenges in the constrained nature of WIP system, by introducing a feasible integrity protection method including access control with authentication and authorization, privacy preserving and security management. The following list outlines the methods of our main contributions in order to achieve suitable and efficient solution for the addressed problem.

- The first main contribution of this thesis is the investigation of the WIP application vulnerabilities both from security and privacy point of view. In particular, we collect various risks and threats as well as the attack scenarios that are possible to be conducted in the WIP applications.
- The second main contribution of this thesis is the proposed design of security and privacy protocols tailored to the constrained nature of WIP system. The protocols are applicable for WIP system based on both WLAN/WPAN and RFID system. Such protocols enable access control with mutual authentication and verification, as well as identity protection. Therefore, it can be relied to mitigate various threats and risks in broader aspects of WIP system.
- The third main contribution of this thesis is the evaluation of the security and privacy method. We prove that our proposed solution is suitable to provide protection from various security risks and threats inherited from the use of WIP technology.
- The fourth main contribution of this thesis is the performance evaluation of the proposed security and privacy method. We emulate the cryptographic processing of our proposed solution in order to prove that the processing overhead is feasible to be applied in the constrained nature of WIP system. In addition, we evaluate other parameters including the communication overhead and the memory storage in order to ensure that our proposed solution is suitable to tackle the challenge related to low-speed data-rate and limited memory storage.
- The fifth main contribution of this thesis is the proposed solution in term of security management service. We design the corresponding key management system of the

proposed authentication protocol. The service enables to update the security properties including key management update, which is feasible to be applied in the system’s limited resources including limited bandwidth availability.

In general, our contributions aim at providing the integrity security and privacy protection that can mitigate various threats and risks in broader aspects of WIP problem. In addition, our contributions aim at providing novel solution which is applicable for the system’s limited resources of WIP the system.

1.4. Objective and Requirements

In order to provide an integrity protection in the constrained nature of WIP system, a proposed security and privacy method should fulfil several features. The following list generally outlines such security and privacy features as the main objective of the thesis.

- *Access control*. The proposed security and privacy method should provide protection from unauthorized party that aims at getting illegitimate access to the WIP system. In this regards, the access control should enable legitimate users or nodes to define whether they try to connect to the legitimate or rogue peer (i.e. Coordinator or RFID reader). On the other hand, the access control should also enable the peer to define whether they are in process to connect to legitimate or malicious node. Thus, the access control feature can detect the malicious node or rogue peer in mutual way and subsequently discard the connection.

- *Mutual Authentication and Authorization*. The proposed security and privacy method should enable initial authentication in two-way verification before proceed the security procedure to the next phase. In this regards, all parties in the communication of WIP system must be mutually authenticated before revealing their sensitive information to each other. Thus, it ensures that only authorized party can be involved in the communication system. Thus, not only mitigating various threats on Man-in-the middle attacks but also such feature can provide a complementary protection to the sensitive information including the user identity from being revealed by unauthorized party.

- *Privacy*. The proposed solution should ensure the confidentiality of the whole communication process, which prevents the sensitive information including the identity from being eavesdropped or illegally revealed by unauthorized party.

- *Message integrity*. The proposed solution should ensure that all messages transported during the authentication and authorization process are not modified or transited by unauthorized party. In general, this feature should be able to prevent an adversary to engage in some activity related to MITM attacks. Thus, the existence of rogue devices or malicious nodes that impersonate as legitimate party can be detected as well.

- *Security resistance*. The constrained nature of WIP system is highly susceptible to various threats and risks, ranging from the physical layer to combination of various layer vulnerabilities. Take in to account that protecting the whole threats is unrealistic goal, the security method should provide sufficient protection at least for broader aspects of the security and privacy problem. Moreover, the security method should also manage to mitigate the complex challenges in large-scale and distributed scenario. In addition, the proposed solution should also manage to mitigate various threats based on multi aspects problem such as insider attacks that try to misuses their credentials, or several types of social engineering attacks that try to gain opportunity to launch particular attacks.

- *Communication overhead*. The security and privacy method should provide efficient communication overhead. In this regards, it should ensure that the size and the number of messages transported during the security process are affordable to be applied in the ubiquitous communication with low speed data-rate and limited battery power.

- *Computation overhead*. The security and privacy solution should be able to sustain the limited CPU power by providing a security protection with efficient processing overhead. Thus in general it is feasible to be applied to the system's limited resource of the WIP system.

- *Storage overhead*. Take into consideration that most of security solution requires bigger memory space to store their security properties, the proposed solution should ensure that all security parameters that are needed to construct the protection are feasible to be stored in the limited memory storage of the WIP devices.

- *Link layer security method*. The proposed security and privacy solution should entirely rely on link layer method. It is enforced in order to sustain the low-cost connectivity with efficient communication and computation overhead.

- *Efficient Security Management Service*. Take into account that a comprehensive security and privacy protection is a continuous and long-term effort, security management service including the KMS is a critical feature in order to ensure the integrity protection. In addition, the proposed security management method should provide efficient service in the constrained nature of WIP system.

- *Service Availability*. The security service including key management and security update should be available whenever the service is needed to any legitimate party. The availability means the proposed solution should ensure that the service is securely feasible to be applied in the constrained nature with limited connectivity and data-rate, without introducing major drawbacks that implicate the overall security and privacy protection.

- *Large-scale support*. The proposed solutions including the designed protocols and its corresponding KMS should ensure that such solutions can feasibly sustain the growth number of users or nodes without introducing the need to majorly reconfigure the security properties. Such solution should also be able to cope with the complex challenges in large-scale and distributed scenario.

In general, this thesis aims at providing a novel security and privacy solution that can satisfy the aforementioned objectives and requirements. Thus, the proposed solution can cover the broader aspects of the WIP's problem.

1.5. Proposed Solution

The proposed security and privacy protection comprises a protocol for WIP application for mobile and embedded devices [21] (e.g. smart phone, tablet, sensor node, etc.), which is based on WLAN (IEEE 802.11) and WPAN (IEEE 802.15.4). Furthermore, we also propose a security and privacy protocol specifically for the more sensitive challenge in the system's limited resources in WIP based on RFID system [23]. In addition, we also propose the corresponding key management system to provide integrity protection in such system's limited resources, particularly KMS for WIP based on RFID system [24][26].

In order to establish the security and privacy method for the aforementioned methods, the protection methods establish two-tier identity protection since in the beginning of authentication process. In this regards, the client identity (i.e. a binary MAC address) is firstly hashed into 128 bit integer and then the hashed value is included in the encrypted payload of the established session, in order to transport the message to the legitimate peer. Thus, an adversary must firstly break the session key and then break the hash function in order to reveal the identity. In general, by protecting the identity various risks related to privacy can be mitigated. In addition, this method is also effective to strengthen the security since most of state-of-the art attacks cannot be launched without revealing the identity.

Furthermore, we propose light-weight mutual authentication and verification. In this regards, the security mechanism entirely relies on data-link layer in order to minimize the computation and communication overhead. The authentication verification method is establishes in mutual way with particular cryptographic challenges. Thus, there is no chance for an adversary to play with man-in-the-middle attacks in order to impersonate either as legitimate client or peer, since he will not be able to answer the challenges by just intercepting the message. More detail about our proposed solutions is outlined in the next chapters of this thesis.

1.6. Scope of the Thesis

This thesis address the problem on security and privacy protection for WIP applications based on several positioning technics over various standard wireless technologies (e.g. WLAN or various 802.11 standards and WPAN or various 802.15.4 standards. In particular, it covers various positioning technics reaching from Receiver Signal Strength Indicator (RSSI), Time of Arrival (TOA), time-difference-of-arrival (TDOA), time-of-flight (TOF), Angle of Arrival (AOA), to using Radio-frequency identification (RFID).

The security and privacy problem over various other WIP technics including using infrared, ultrasound, magnetic signals, Global positioning system (GPS), vision analysis and audible sound are outside scope of this thesis.

WIP system based on various contexts of cellular network technologies including UMTS (universal mobile telecommunications system), GSM (groupe spécial mobile, global system for mobile communications), GPRS (general packet radio service), LTE (long-term evolution), CDMA (code division multiple access), HSPA (high speed packet access), etc. are outside scope of this thesis.

Security analysis and its protection on the vulnerabilities of cryptographic algorithms that are used in our security method are outside the scope of this thesis. We assume that the used cryptographic algorithms are adequate to provide protection from various threats on cryptanalytic attacks, ranging from various technics of brute force attacks, birthday attacks, to the capability to protect from various threats on discrete logarithm attacks.

Furthermore, we assume that any intermediate or peer device including the coordinator and RFID reader have sufficient resources in term of CPU power, memory/storage, bandwidth and energy supply. Therefore, the communication between such devices and the back-end server (e.g. PKG, PPS and database application server) is affordable to use standard security method such as TLS/SSL protocol. Thus, any possible threats that give an adversary chance to compromise the back-end server including access or modify the IBE parameters are outside scope of this thesis.

The security threats that involve the administrative privilege are also outside scope of this thesis. In IBE system, the administrators can potentially misuse their authorities by configuring the back-end server, such as configuring PKG and PPS to grant critical parameters including the private keys to unauthorized devices or users. In this regards, we assume that the administrators are trustworthy and strictly comply with the contractual policy of the security enforcement.

Policy on physical protection and placement for peer devices and back-end servers are also outside scope of our thesis. Although we provide access-control-based solution for potential physical security threads from the client side, an adversary may steal or physically compromise the peer device (e.g. RFID reader). In this case, an adversary may copy all security parameters stored in the memory of the reader including the private key, in order to impersonate as legitimate reader. In this regards, we assume that all peer devices and the servers are tightly supervised by the administrators in order to prevent physical manipulation. Furthermore, we highly recommend adopting the standards physical and operational security defined by NIST (Karygiannis et al.) [27].

Mitigating some of physical attacks that also involve the multi-layer problem is part of this thesis. The network-based verification can provide access control and authentication to the physical abuse including plating malicious node or rogue devices, as well as misusing the security parameters in order to impersonate as legitimate device. Furthermore, this thesis also provides identity protection to mitigate the physical attack based on man-in the-middle attacks problem, such as various technics of relay attacks that target the user privacy. However, other kind of physical attacks that engage in some activity based physical channel analysis such as passive interference and active jamming attacks are outside scope of this thesis.

All inherent threats related to the communication to the backend database, as well as security related to middleware architecture are outside scope of this thesis. We assume that the WIP-backend database communications is strongly protected since it is mostly connected through wired technology in highly supervised area. In addition, we assume that the system uses secure operating systems with suitable network and database configuration that gives very strict access control only to the authorized party. In case the connection still using wireless technology, we assume that the peer devices (i.e. Coordinator and RFID Reader) have sufficient resources to deal with high cryptographic processing such as standard TLS/SSL.

1.7. Publication List

The following list outlines the pre-published research works that are used as parts of this thesis.

Conference Proceedings:

I. **Mohammad Fal Sadikin**, Marcel Kyas, "IMAKA-Tate: Secure and Efficient Privacy Preserving for Indoor Positioning Applications," In Proceedings of the 5th International Conference on Smart Communications in Network Technologies (SaCoNet), June 2014, Vilanova i la Geltrú, Spain.

   DOI Link: (http://dx.doi.org/10.1109/SaCoNeT.2014.6867775).

II. **Mohammad Fal Sadikin**, Marcel Kyas, "Security and Privacy Protocol for Emerging Smart RFID Applications," In Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), July 2014, Las Vegas, Nevada, USA.

   DOI Link: (http://dx.doi.org/10.1109/SaCoNeT.2014.6867775).

III. **Mohammad Fal Sadikin**, Marcel Kyas, “RFID-tate: Efficient security and privacy protection for active RFID over IEEE 802.15.4,” In Proceedings of the 5th International Conference on Information, Intelligence, Systems and Applications (IISA), July 2014, Chania, Crete, Greece.

DOI Link: (http://dx.doi.org/10.1109/IISA.2014.6878787).

IV. **Mohammad Fal Sadikin**, Marcel Kyas, “Efficient Key Management System for Large-scale Smart RFID Applications,” In Proceedings of the 1st International Conference on Industrial Networks and Intelligent Systems (INISCom), March 2015, Tokyo, Japan.

DOI Link: (http://dx.doi.org/10.4108/icst.iniscom.2015.258316).

Journal Articles:

I. **Mohammad Fal Sadikin**, Marcel Kyas, “Efficient Security and Privacy Protection for Emerging Smart RFID Communications,” The International Journal of Networked and Distributed Computing (IJNDC), volume-issue: 2-3, pages: 156 – 165, ISSN: 2211-7946, Atlantis Press Paris, July 2014.

DOI Link: (http://dx.doi.org/doi:10.2991/ijndc.2014.2.3.5).

II. **Mohammad Fal Sadikin** and Marcel Kyas, “Light-weight Key Management Scheme for Active RFID Applications”, EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, ISSN: 2410-0218, Volume: 2, Issue: 5, 2015.

DOI Link: (http://dx.doi.org/10.4108/eai.17-9-2015.150286).

III. **Mohammad Fal Sadikin** and Marcel Kyas, “IMAKA-Tate: Secure and Efficient Privacy Preserving for Indoor Positioning Applications”, International Journal of Parallel Emergent and Distributed Systems,” ISSN: 1744-5760, Taylor & Francis, 2015.

DOI Link: (http://dx.doi.org/10.1080/17445760.2015.1058939).

1.8. Dissertation Structure

This dissertation is structured as follows: We begin this work in chapter 2 with a comprehensive review of security and privacy problem in various aspects of WIP system. This chapter also covers state-of-the art solutions with brief discussion about the weakness of such solutions. In addition, we also outline the fundamental of identity based encryption method and the background of choosing this method for the proposed solution in the constrained nature of WIP system.

Chapter 3 covers our proposed solution for WIP based on WLAN/WPAN system. We begin this chapter with the introduction of the addressed problem and motivation to provide suitable solution. We propose our solution called IMAKA-Tate, a light-weight mutual authentication, verification and key agreement protocol, tailored to the specific requirements of WIP system. We show in the section of security analysis that such protocol is effective to combat various threats, as well as preserve the privacy by protecting the identity (i.e. MAC address). This chapter extends our previous work in [21][192].

Chapter 4 covers the analysis of specific security and privacy problem in WIP based on RFID system. In this chapter we evaluate the possible implementation of IMAKA-Tate in RFID system and how it can mitigate the addressed security and privacy problem. The security evaluation shows that the proposed solution is effective to mitigate various threats in RFID system. However, such protocol is only suitable for the RFID system with sufficient computing resources. This chapter extends our previous works in [22][25].

Chapter 5 improves our previous solution in term of processing overhead by introducing RFID-Tate. In this chapter, we show that the performance is significantly improved without introducing significant security vulnerability. The performance can be improved since the RFID tag only requires to calculate one pairing for each session in the phase of mutual authentication. Nevertheless, this method sacrifices the key agreement feature of the previous protocol. In this regards, the RFID tag must comply with the session key generated by the reader, rather than negotiate its own session key with particular agreement. This chapter extends our previous work in [23].

Chapter 6 covers the key management system as complementary service for security update system, tailored to the constrained nature of WIP system. The key management system enables the light-weight security update (i.e. private key update) that complies with the specific security and privacy requirements for the WIP system. Thus, the comprehensive integrity protection can be achieved. This chapter extends our previous works in [24][26].

Finally, we discuss the conclusion of the whole work of this dissertation in chapter 7. It also covers various aspects of security and privacy that need to be done in the future work in order to cover all aspects of the integrity protection.

Chapter 2

Background and Motivation

This chapter comprehensively discusses various threats in WIP system ranging from the lowest layer called physical layer to the top layer including application layer as well as multi-layer threats that are composed based on combination of several layers. In addition, we also discuss the state of the art solutions and its weaknesses and risks, as well as the brief suggestion to mitigate such risks.

Furthermore, this chapter also outlines the brief theory background of Identity-based encryption, particularly short introduction about the Tate pairing over supersinglar curve. In addition we also discuss the reason of choosing the cryptographic method for the proposed protocols and the corresponding key management system of the WIP applications.

2.1. Security Threats and Risks in WIP system

2.1.1. Physical threats

WIP system relies on the vulnerable nature of wireless communication that every party can have access to the system. In addition, the low-cost devices are mostly deployed in unsupervised and lack of physical protection. This issue introduces chance to unauthorized party to perform physical manipulation, which makes the WIP system is highly susceptible to various threats on physical attacks.

Most of physical attacks aim at performing denial-of-service or sabotaging the service. However, physical attacks may be exploited also to achieve specific gain, including reveling the user privacy or to be used to launch further attacks on different layer. For instance, an adversary may observe the RF signal to find the time-of-arrival, which can be used to infer the node's location. Another example, an adversary may steal the node to find sensitive information (e.g. MAC address), in order to launch other attacks such as resource consumption attacks. The following list outlines various types of physical attacks that should be mitigated in the WIP system.

1. Jamming Attacks

An adversary can deliberately prevent the communication between the node and the peer by using radio jammer to block the wireless signal transmission. This attack aims at performing DoS attacks and it is well-known as frightening threats since up to now there is no suitable solution to combat radio jamming, particularly for wireless communication operated in constrained environment. Various type of jamming attacks to create DoS in wireless communications have in last decade attracted some attention. In particular Wireless Local Area Network (WLAN) technology, Noubir et al. [28] demonstrate successful jamming attacks at a very low energy cost particularly for IEEE802.11a and IEEE802.11b. In the field of Wireless Sensor Networks (WSN) application, Wood et al. [29][30] outline the jamming attack as well its prevention by mapping the jammed regions. In advance, Wenyuan Xu et al. [31] propose 4 types of jamming attacks including the constant jammer, the deceptive jammer, the random jammer and the reactive jammer. Not only on physical layer, but also jamming attacks can be conducted based on MAC layer. In particular, Wei Law et al. [32][33] propose MAC layer jamming attack by exploiting the semantics of the link-layer protocol (aka MAC protocol).

2. Relay Attacks

Relay attacks are one of the most arduous challenges to be tackled particularly in the constrained nature of WIP system. It is to be noted that the use of upper layer security protections even with very strong cryptographic primitives and well-designed protocol are not enough to mitigate the attacks. Take into account that an adversary can use transponders to act as Man-in-the-Middle. In this regards, the transponder devices that are logically placed between the two entities (i.e. the node and the peer) can intercept the message even it is transported over cryptographic protocol. Here, an adversary does not need to break the cryptographic protection, instead he just aims at revealing meta-data information attached on the radio signal in order to achieve particular gain (e.g. spoofing the legitimate node's location). Therefore, relay attacks cannot be combated by just using cryptographic protocol that relies on upper layer method.

By intercepting the message, an adversary can reveal some sensitive information such as the Time-of-Arrival (TOA) that implies the victim's position. Indeed, such information can be elicited from various communication mechanisms that are implemented at lower layer including collision detection and avoidance, demodulation, error detection and correction, synchronization and retransmission. During last decade, many types of relay attacks have been reported particularly in the field of RFID communications. Some of them introduce the vulnerability of contactless system (e.g. smart-cards) [34-37], while the other demonstrate about practical attack in the field of keyless entry and start systems for modern cars [38] and Near Field Communication (NFC)[39].

3. Signal Interference

The large-scale scenario of WIP deployment introduces particular challenges in signal interference problem. Indeed, the WIP system is susceptible from various aspects that disrupt the signal quality, ranging from electronic noise, metal composite around the devices, water, to various things that commonly exist in indoor environment such as power switching, room heater, wall, etc. All those things cause inaccurate position estimation, even may disturbs the overall communication system that might affects temporary DoS. In this case, an adversary may exploit this issue in order to gain malicious gain. For instance, a disturbance on RF signal may be performed by just generating electronic noise or covering the wall with metal composite in order to sabotage the WIP services.

4. Physical destruction

Take into account that most of WIP end-devices are not equipped with sufficient physical protection, an adversary can simply destruct the devices in order to get the specific gain such as performing disturbance or Denial-of-Service (DoS) attacks. In the case of physical point of view, DoS can be conducted just by manipulating one of node components such as by cutting the antenna off, removing the battery, applying pressure or throw down the device forcefully, or even by exploiting chemical substance to disable the device. This kind of attack even can be also applied to the peer (i.e. reader or coordinator), which affects larger impact on DoS since all nodes existing in particular range of the destructed peer cannot be detected.

5. Physical Manipulation

An adversary can perform temporary DoS by simply wrapping the node with conductor material (e.g. aluminum foil) in order to cover such node to receive Radio Frequency (RF) signal. Therefore, the communication between the node and the peer can be prevented. This attack even can be carried out in large-scale by instead just wrapping the peer (reader or coordinator). Thus, the presence of all nodes cannot be detected since the wrapped peer is not able to receive any RF feedback from any node. In general, this kind of physical manipulation also considered as frightening threat since anybody may easily conduct such attack with very low cost and without special technical skill.

6. Physical abuse

An adversary may physically compromise the WIP’s device in order to manipulate the service. For instance, an adversary may exploit the unsupervised node to manipulate the data in the memory device in order to get the specific benefit. An example is to copy the sensitive data (e.g. identity and security properties) to other device in order to impersonate as legitimate device. In addition, an adversary may use the compromised node to inject malicious code or malware. Thus, an adversary can spread virus/malware, which may infect the entire WIP system. The peer (i.e. reader or coordinator) is also susceptible from physical data manipulation. In this regards, an attacker can remove the legitimate peer and copy its sensitive data to the rogue device, in order to impersonate as legitimate peer. Thus, an attacker can fool all nodes within particular range to reveal their critical information (i.e. node's identity and its data application) to the rogue device. Another trivial scenario, an adversary can shift the peer's position, so that the position estimation will be calculated incorrectly.

2.1.2. State of the art solution for physical layer attacks

The intentional and unintentional physical attacks including attack both for permanent and temporary denial of services can be mitigated by applying traditional security surveillances. This method includes placing camera surveillances, employing personal security guards, applying physical access controls include fences, gates, locked doors, one-way-in, etc. More detail about physical security solutions are described by Karygiannis et al. [27]. Particularly in the WIP application that requires high security procedure such as in the air-port or government building, physical security screening should be applied. Thus, the threats can be mitigated by reasonably screening the suspicious things (e.g. screwdriver, hammer, aluminum foil, etc.) that can be used to launch physical attacks.

Any kind of physical manipulation including node or peer displacement can be mitigated by applying the same physical security surveillances. Additional, the security can be improved by placing such devices with strong mechanical bond. Especially for high cost WIP applications, physical security can be improved by adding alarm to the devices which is triggered when unauthorized displacement occurs. In addition, such alarm can also be triggered by attaching sensor to the device that can detect suspicious activities such as placement, pounding, or unusual temperature change.

To the best our knowledge, there is no better solution to mitigate the unintentional signal interference other than omitting or repositioning all things around the devices that might disturb the RF signal. In case of signal interference caused by dense of wireless signal, various research works propose solution on antenna technology to mitigate the problem. Leong et al. [40] propose guidelines for antenna positioning in RFID deployment zone in order to achieve safe distance between antennas in a dense reader environment. In addition, Chou et al. [41] present the design of a patch antenna array that reduces the interference in RFID applications. Another approach has been proposed by Ferrero et al. [42]. In this paper, the authors introduce an anti-collision protocol in dense RFID networks that aims at reducing interferences among readers.

In relay attack, the message is intercepted in the middle between the peer and the user affecting significant delay (e.g. the increase value of Round Trip Time (RTT) of the packet). Therefore, Instead of using cryptographic protocol, the use of physical distance as detection parameter is a promising solution to prevent relay attack. One famous solution particularly for RFID communications is proposed by Gerhard P. Hancke and Markus G. Kuhn [43] called Distance Bounding Protocol (DBP). Since the nature of DBP has disadvantages on noise and no error correction, two additional research works provide suitable solution to improve the disadvantages. The first one is proposed by Avoine et al. [44], which provide a computation framework of channel error probabilities. The second one is, Hancke et al. [45] introduce false-accept probability in term of the risks based on mafia and distance fraud threats.

Further research works try to improve the DBP from various aspects, including the improvement of security level as introduced in [46-50]. Moreover, few research works focus on efficiency of computational overhead such as presented in [51-52]. Furthermore, one interesting topic deals with the improvement in term of memory requirements [53]. Some of research works propose mutual DBP by focusing on critical security features including mutual identity and mutual distance verification [54-56]. Nevertheless, the aforementioned mutual DBP introduce particular weaknesses, such as the solution proposed by Capkun et al. [54] is too heavy-weight that may not be suitable for the constrained nature of WIP. Furthermore, several research works such as Cremers et al. [57], Desmedt et al. [58] and Reid et al. [59] reported that most of DBP are susceptible to various threats ranging from distance hijacking attack, distance fraud, mafia fraud, to terrorist fraud attack.

Radio jamming is the most difficult problem to be mitigated in wireless communication. An adversary always has chance to actively disturb the radio channel by generating the same range of radio signal that is used in the existing wireless communication. Solving this problem is even more difficult since an adversary can arbitrary use the radio jammer at any place within the range in order to launch the attack. To the best of our knowledge, there is no anti-jamming solution that can fully mitigate this problem. However, a lot of research works introduce strategic solution to hide from the attacks, reaching from anti-jamming in the field of wireless sensor networks [60-66], to the solution for RFID communications [67]. In addition, Wenyuan Xu et al. [68] introduce a solution for jamming attack based on MAC address. Another approach is by placing friendly jammer around the geographical zone to defense against malicious jamming [69-70]. Nevertheless, all the aforementioned jamming solution cannot prevent the attacks at all, since most of the solutions just aim at camouflaging the RF signal. In addition, such solutions introduce various major drawbacks. For instance, placing friendly jammer can interfere with other legitimate RF channels.

2.1.3. Network and Upper Layer Threats

In this section we collect various possible attack scenarios that may be launched in the charge of several communication layer vulnerabilities including network layer protocol, transport layer, and the upper layer. In addition, we also outline the state-of-the-art solution to mitigate the attacks, as well as briefly discuss the drawbacks of the solution.

1. Cloning Attacks

Although the manufacturer can produce a unique identity to each device as well as claim that it is not possible to replicate such identity, an adversary in fact can easily clone the identity to writable or reprogrammable device. In addition, an adversary may also conduct the same technic in order to impersonate as legitimate peer (i.e. coordinator or RFID reader). Various cases in cloning attacks particularly in the charge of the vulnerability of e-

Passports have been demonstrated. Most of them successfully conduct the attacks due to the vulnerability in access control mechanism. For instance, some of attacks are introduced by European Digital Rights (EDRI-gram) [71], Juels et al. [72], and some research works presented in [73-77]. In addition, Halamka et al. [7] report their evaluation of VeriChip product against cloning and spoofing attacks.

Take into account that most of WIP communications do not use sufficient security and privacy protection, this case makes an adversary can easily replicate the node or tag identity and any sensitive data in order to perform the cloning attacks.

2. *Spoofing Attacks*

Similar with cloning attacks, spoofing attacks aims at impersonating as a legitimate client in order to get privilege and full access to the valid communication channel. However, different with cloning, spoofing does not require physically clone of the node or RFID tag. Instead, such attacks require the knowledge of communication protocol as well as the sensitive properties including the cryptographic material that are used to secure the communications.

3. Impersonation

Taking into account that most of WIP communications are not sufficiently protected and it is naturally broadcasted that makes every party has access to, an adversary may have chance to reveal the legitimate node or peer identity. In this case, an adversary may try to play with MITM by transiting and modifying the messages in order to compromise the communication in between.

In addition, the revealed sensitive information of the peer may be used to replicate the device and plant it as rogue peer or devices in order to act as alike a legitimate Extended Service Set (ESS) in the wireless communication system. Such rogue devices are also can be exploited to trick the legitimate client or node to reveal their sensitive information.

4. Eavesdropping

Eavesdropping is one of the most frightening specters in wireless communication, as an adversary always has chance to carry out such malicious activity. An adversary can record the communication data from both directions which are client to the server and server to the client. All recorded communication can be further used for malicious activities (e.g. cloning, MITM, DoS, reveling the privacy, etc.).

5. Back-end Database Attacks

Most of WIP system particularly the coordinator and the RFID reader are connected to the back-end database. Like in common networked system, such connection is also susceptible from various threats that may give chance to the adversary to compromise the database. However, the connection parameters (e.g. network protocol, access control and operating system configuration) are considered as specific secured system, since the communication to the database infrastructure is mostly connected through wired communication. In this regards, the attacks are not trivial to be launched since it requires deep knowledge about protocol, policy and the internal middleware architecture.

6. Resource Consumption Attacks

Resource consumption attack is a variant of Denial-of-Service (DoS) attacks that aims at exploiting the system limited resources in order to extinguish the service. The attacks can be conducted by repeatedly sending amount of packets to the resource-restricted devices (e.g. sensor node, RFID tag, etc.) in order to waste the limited bandwidth and drainage the battery power. In addition, the attacks even can be launched to target the limited computational power, in order to coercively shut down the CPU operation. Thus, the flooding packet can overburden the constrained capacities of the devices, which affects malfunction of device.

2.1.4. State of the art solution for network and upper layer threats

1. Anti-Cloning Attacks

A potential solution to prevent cloning attacks is by establishing mutual authentication and verification protocol. This method provides access control to ensure that only legitimate entity can get connection into the system. Nevertheless, most of mutual authentication solution require high system's resources, therefore enforcing such method in the constrained nature of WIP system is a complex challenges.

Several previous works also tried to mitigate the cloning attack with diverse method, one of them was introduced by Ari Juels [4]. The author presented simple methods to reinforce the resistance of EPC (Electronic Product Code) tags against basic cloning attacks. Such methods were presented by establishing challenge response authentication with PIN-based access control method.

Some of researcher tried to use Physical Unclonable Function (PUF) technology to achieve unclonable identity. One of them was proposed by Pappu et al. [78-79] with physical one-way functions and it is demonstrated that they are collision resistant. Indeed, PUF is a promising technology to encounter the cloning attack due to the advantages defined by Tuyls et al. [80].

- *"Since PUFs consist of many random components, it is very hard to make a clone, either a physical copy or a computer model."*
- *"PUFs provide inherent tamper evidence due to their sensitivity to changes in measurement conditions."*
- *"Data erasure is automatic if a PUF is damaged by a probe, since the output strongly depends on many random components."*

In general, PUF can make the chips unique and practically impossible to be cloned. Moreover, PUF is a potential technology that can be implemented for challenge–response authentication. Thus, it is resistant to various risks on cloning attacks and spoofing attacks as well. Nevertheless, this technology introduce particular drawback. It is arduous to be characterized since its feature that uses many random components, which are introduced in the physical object during its manufacturing [81].

Tuyls and Batina [5] proposed off-line authentication method by using PUF technique. In particular, the authors presented an anti-cloning method based on PUFs that are attached to an Integrated Circuit (IC). In addition, the further works introduce the off-line verification protocol based on key generation and physical one-way function presented in [82-83]. In this works, the authors proved that their solution feasible on a constrained device such as an RFID-tag. Nevertheless, In order to minimize the area constraints of a tag, the involved cryptographic algorithms are sacrificed. In this regards, the elimination of some cryptographic function can harm the whole system from other threats and risks in various aspects.

Devadas et al. [3] present the design of PUF enabled “unclonable” RFIDs. Such design has been implemented in 0.18 μ technology. The extensive testing results demonstrated that PUFs can securely authenticate an RFID with minimal overheads. Furthermore, the PUF based RFID introduces the advantages in anti-counterfeiting and secure access.

In addition, Mitrokotsa et al. [81] explain the idea that cloning attacks and other variant of impersonations can also be mitigated by checking and verifying the user real time data and correlating such data to the movement profile stored in the database. In this regards, the access control should be aborted if the suspicious event is detected. In the WIP case, the suspicious can be defined if illogical event occurs, such as the same person exists concurrently in two or more different room. Similarly, the security will not permit someone to enter the building if according to the database the person is already inside the building or another case that the person is on business trip.

Mirowski and Hartnett [6] introduce an Intrusion Detection System (IDS) specifically for RFID system. The IDS works according to the audit log data (e.g. statistical classifier) in the back-end database and it mainly focus on cloning attack detection. Their experiment result shows that the true positive rate of anomaly detection varies in between 24.24% to 86.36%, on the other hand the false positive rate ranging from 2.17% to 10.77%. Although the authors have demonstrated promising experiment result, the idea of IDS for RFID system definitely need more investigation for further improvement.

Eun Young Choia et al. [8] propose a novel anti-cloning method specifically tailored to the EPCglobal Class-1 Generation-2 (C1G2) standard using particular function with unique serial number. This method is effective to combat cloning attack as well as preventing the information leakage and password disclosure. Nevertheless, the invariability of encrypted packet introduces chance to an adversary to trace the targeted devices (in this case RFID tag). Thus this method suffers from the problem related to user privacy.

2. Anti-Eavesdropping

Wireless communication is susceptible to eavesdropping threats. One of promising solution to mitigate the threat is by applying cryptographic method to protect the communication channel. Nevertheless, such cryptographic method must be carefully considered since it requires more demand in term or resource availability, which is contradictive with the system's limited resources of WIP system.

Other way to mitigate eavesdropping is by avoiding sensitive data to be stored in node's memory. Another similar method to mitigate the threats is by eliding such sensitive data including the critical security properties that are stored in the node's memory. In this regards, the protocol and back-end database should be able to accommodate suitable communication that enables to securely retrieve the important data whenever needed.

Quan et al. introduce several anti-collision algorithms based on EPC code with 96-bit identifier in RFID system. One of them is the tree-walking algorithm that can be useful to mitigate eavesdropping by securing the transmission of the tag identity. Nevertheless, the tree-walking procedure introduces particular drawback that slow-down the communication performance. In this case, the number of queries-responses and the number of bits transmitted increases excessively with the increase in the bit length of tag identifier [84].

3. *Anti-Spoofing and Impersonation*

Similar like the solution for cloning attack, spoofing and any kind of impersonation can be mitigated by performing authentication with challenge response method. In particular, one of methods to established authentication is by equipping all the nodes with pseudonymous identities such as using hash function. Thus, only authorized peer (i.e. RFID reader or Coordinator) can get access to the legitimate nodes or RFID tags.

Weis [85] present pseudonymous identities using hash locks that propose a simple access control mechanism based on one-way hash functions. In addition, Weis et al. [86] also present randomized access control with using randomized hash-lock. This method is effective to prevent the legitimate end-device (e.g. RFID tag) to respond predictably queries by unauthorized party. Thus, the RFID tag meta-ID is secured from being revealed by unauthorized party.

Ohkubo et al. [87] present user privacy protection using a low-cost hash chain mechanism. In particular, the authors use the hash chain technique to renew the secret information included in the tag. Thus, Through the use of a hash chain with two hash functions, the low cost protection and forward secrecy can be achieved.

In general, hash function technique is considered as cheap solution since such method can be applied by just implementing the hash function on each node’s memory. In this regards, the key and identity calculation are handled by the backend database. On the other words, the authentication procedures are partially handled by the backend database. Thus, it might be suitable for the system’s limited resources of the WIP system.

Nevertheless, from time to time various research works have proved that the hash protection can be broken in certain condition. Thus, the security method is considered as weak protection when it is just relaying on single hash function method. One example work is presented by Eli Biham and Rafi Chen [88]. In this work, the authors present a near-collision attack on SHA-0 based on differential collisions [89]. Joux et al. further made improvement of this attack by introducing a 4-block full collision of SHA-0 [90].

Xiaoyun Wang and Hongbo Yu [91] present a new powerful collision attack that is efficiently to be conducted on various MD5 hash function. Such attack is also efficacious for many other hash functions including MD4 [92], HAVAL-128 [93] and RIPEMD [94]. Even in the case of MD4, the attack can feasibly be done within less than a second. Wang et al. [95] comprehensively introduce Cryptanalysis of the Hash Functions MD4 and RIPEMD. In term of HAVAL technique, Wang et al. [96] present feasible attack that can break the HAVAL with 128-bit fingerprint. Furthermore, Wang et al. also present new collision search attacks on the hash function SHA-0 [97] SHA-1 [98]. In addition, a lot of research works have introduced various technics to break various hash function implementations [99-122], including various technics of Cryptanalysis, Preimage attacks Collision, and Multi-collision attacks. In general, the security method should combine several methods, rather than just relying the protection on single method of hash function.

4. Anti-Resource Consumption Attacks

In the context of Ad-hoc Networks, Stamouli et al. [123] present Real-time Intrusion Detection for Ad hoc Networks (RIDAN). This method aims at mitigating several threats including resource consumption attacks. This method might be potential to be implemented in WIP system since the experiment results show that RIDAN performed resource consumption attack detection with accuracy of 74.8%. Nevertheless, the use of intrusion detection components introduces the complexity, cost and maintenance. Therefore, this method is not suitable for the constrained nature of WIP system. Furthermore, this method introduces serious problems such as false alarms that can harm the overall communication system.

Yih-Chun Hu, Adrian Perrig and David B. Johnson [124] present other solution to combat resources consumption attack called Ariadne. In this paper, the authors propose secure ad-hoc routing protocol by re-designing Dynamic Source Routing protocol (DSR). In order to secure the routing, Ariadne establishes routing on demand by dynamically finding the route only when required. On similar solution, Sencun Zhu et al. [125] introduces hop-by-hop authentication to verify the validity of all packets transported in the network, and one-way key chain to establish trust among nodes. Nevertheless, such methods are tailored to mitigate resource consumption attacks which are conducted in particular routing protocol for ad-hoc networks. Thus, it is not appropriate with the security requirements in the WIP system.

To the best of our knowledge, the most effective way to mitigate resource consumption attack particularly for WIP system is by protecting the end-devices sensitive data including the identity. Thus, an adversary will not be able to arbitrary sending packet to the targeted device since the adversary has no knowledge about destination address of the targeted device (i.e. the MAC address).

2.1.5. Special Issue on Privacy Threats

Providing a location awareness service without impact on privacy issue is one of the biggest challenges in WIP applications. There are a lot of things that can be exploited by an adversary in order to reveal the users privacy. One of them is by exploiting the vulnerable nature of wireless communication, which is naturally broadcasted and every party has possible chance to eavesdrop the communication. The other issue is the use of positioning technics itself, which makes an adversary has chance to trace the user trail (e.g. the radio fingerprint). In addition, the nature of WIP system that is commonly deployed in unsupervised area makes an adversary might easily to perform malicious activities such as physically compromise the unsupervised nodes, in order to reveal the user privacy. Indeed, the privacy issue in WIP system is a complex problem that arises from various aspects, reaching from the problem on physical layer to application layer. The privacy problem even may arise from non-technical aspect such as social engineering and forgery.

Various example scenario related to the privacy have been introduced. For instance [27][81], the revealing information can be exploited to perform corporate spying in order to define strategy to win the business competition. In this case, an adversary may eavesdrop the communication or maliciously access the beck-end database in order to surreptitiously learn confidential information such as prices and marketing strategies, manufacturing schedules, item flow in the supply chain (e.g. delivery schedules), or even a critical information about list of items in warehouses.

During the last decade a lot of reported problems in the charge of technical aspect of privacy issue have been presented, one of them is the one introduced by Gildas Avoine [126]. In this paper, the author reveals the privacy issue in RFID banknote protection scheme that is previously introduced by Juels and Pappu [127]. In this case, although the banknote has already been equipped with cryptographic protection scheme, which is based on combination of optical access and RFID, the author demonstrated that the data stored in the smart device can still be accessed and modified without having optical access to the banknote. Such attack can be successfully launched by abusing the secure integration of asymmetric and symmetric encryption schemes [128], which is used to protect the banknote.

In term of WIP for library application, David Molnar and David Wagner [129] introduce the specific problem in RFID library application. The authors report that there are several possible attacks that can be conducted in such application. One of them is about detecting the tag presence that correlates to detecting the human presence, which introduces the privacy problem. The second problem is about static tag data and no access control that in general introduce a chance for an adversary to track the book and infer the origin of the person carrying the book. In addition, collision-avoidance IDs is listed as one of the potential problem since collision-avoidance behavior might allow unauthorized party to reveal the tag’s or user’ identity. Furthermore, the deployment of rewritable tag introduces chance for an adversary to rewrite or modify data in the tag in order to perform further misuses.

Gildas Avoine and Philippe Oechslin [130] present multilayer problem that implicate the privacy issues of RFID applications. In this paper, the authors prove that the privacy attack (i.e. information leakage and traceability) can be launched from three layers of RFID communication, which are application, communication and physical layer. They demonstrated that privacy is a complex problem that cannot be mitigated by only focusing into a single layer solution. In addition, they also proved that most of privacy solutions that only focus on application layer fail to cope with the multi-layer problem.

Furthermore, there are a lot of discussions about privacy issue raised from the characteristic of RFID communications that have been published in various scientific publications. Some of them discuss about the vulnerability of RFID system in political and philosophy point of view [131-133].

2.1.6. State-of-the-art Privacy Solution

Mitigating privacy threats is a complex challenges that the solutions must be comprehensively viewed on multi-aspects of the addressed problem. A lot of research works have been introduced to mitigate the privacy problem in various methods. It ranges from the use of light-weight cryptographic protocol, hash function, to the use of blocker method to prevent from unauthorized access.

Gildas Avoine and Philippe Oechslin [13] propose scalable hash-based privacy protocol based on the scheme proposed by Ohkubo et al. [87]. In this paper, the authors introduce a specific time-memory trade-off that enables the scalability as well as prove the privacy solution for RFID system. Using hash function is one of potential solutions to mitigate the privacy threats that is effectively protect the identity from being revealed by unauthorized party. This method is well known as cheap solution that is applicable to the system's limited resources. Nevertheless, various research works have reported that hash function method is feasible to be broken. In general using stand-alone hash-based solution without any additional security method is considered as weak security protection. Thus, this solution is not suitable anymore for state-of-the-art privacy protection in the WIP system.

Ari Juels [14] introduces minimalist cryptography for low-cost RFID tags by using pseudonym technique. This method also introduces one-time-pad security scheme that enables to re-use the pad to overcome the limited memory resources. Nevertheless, the re-use one-time-pad affects degradation to the general security protection.

Several researchers propose unique and elegant privacy solutions to address the privacy issue. For instance, Sastry et al. [15] present the concept of secure location verification by introducing Echo protocol. It is an extremely lightweight protocol that does not require time synchronization, cryptography, or any prior agreement between the client and verifier. Other approach is proposed by Marco Gruteser and Dirk Grunwald [16]. This work presents middleware architecture and algorithms that enable efficient anonymity to achieve privacy preserving. The adaptive algorithm enables to adjust the anonymity constraints based on the specific needs within a given area. In addition, Hong et al. [17] introduces architecture for privacy-sensitive ubiquitous computing called Confab. This toolkit enables to customize privacy mechanisms as well as managing the location privacy. In addition, this toolkit can address the need in providing spectrum of trust levels among the users.

Furthermore, Ari Juels et al. [18] also propose a unique method for selectively blocking the RFID tags in order to achieve the consumer privacy. This method allows to selectively prevent a certain tag from being read by un authorized party. In addition, Ari Juels and John Brainard [19] also introduce similar blocker solution which is more flexible and cheap. Similar approach is propsed by Günter Karjoth and Paul A. Moskowitz [20], whcich introduce a method that enable the RFID tag to be disabled with visible confirmation. This innovation use clipped tags method, which enables the user to physically detach the RFID tag from its antenna, in order to disable the connection to the reader. Nevertheless, the aforementioned solutions introduce particular drawback that the blocker must always require human intervention. In this regards, this method might not be practical particularly for the non-human-involved WIP applications.

Moreover, all solutions aforementioned above focus rigidly on a particular problem of privacy aspect, without considering other security aspects including authentication, other security risks, key distribution and management. In general, privacy preserving without any additional security features is arguably considered as uncompleted protection since it left tremendous security problem.

2.1.7. The Threats based on Application Layer Vulnerabilities

The threats on WIP applications are all possible attacks that aim at eliciting malicious gain in the context of application such as reveal the sensitive information, spoofing or modifying the information (e.g. body temperature or blood pressure in health care applications), impersonation, forgery, or even performing DoS.

1. Unauthorized Reading of the Application Data

Take into account the communication in WIP system is not equipped with sufficient authentication and encryption methods, an adversary can silently read the content of application without leaving any imprint. An example case is in a credit card application which is equipped with RFID chip to enable fast payment method. In this case, an adversary can silently use a reader (e.g. a smart phone with NFC) to scan the secret information of credit card saved in a pocket. In this regards, various information can be elicit including the name, credit card number and expiration, in order to further use the information for illegitimate payment. Here an adversary is just required to approach the target in particular proximity of NFC range, even without requiring any optical contact. On the other words, an adversary can easily read the credit card information without requiring any physical contact to the pocket of the victim.

2. Node modification

Take into account most of devices that employ in ubiquitous computing facilitate with reprogrammable and writable memory, this issue introduce implication that an adversary can modify or delete the data application stored in the devices. The success rate of this type of attack is even higher since most of pass-through devices (i.e. reader or coordinator) have no mechanism to differentiate whether or not they communicate with original or unmodified node.

Various implications arise from this issue, which the risk depend on the use of WIP in particular applications. An example scenario in RFID health-care applications is defined by Mitrokotsa et al. [81]. In this scenario, an adversary can modify the data in the RFID tag, in order to sabotage the service. In this case, the data application (e.g. blood pressure, body temperature, heart rate, etc.) can be modified. This malicious activity can impact serious problem that may trigger false alarm or inappropriate treatments such as mistakenness in defining the drug dosage.

3. Malware Attacks

Since most of WIP applications are connected to the backend database, this issue makes the WIP system is also susceptible from various threats on malware attacks. For instance, an adversary can exploit the node's free memory space to inject and spread viruses through the database services.

In the case of WIP system based on RFID technology, Rieback et al. [134] define that malware attacks can be classified in three different types. The first one is various types of exploit attack. Such attacks can be performed by exploiting the memory space in the client device, in order to launch several types of attacks including SQL injection, malicious code insertion and buffer overflow. For instance in the case of SQL injection attacks, the researchers also demonstrated example experimentations with particulars command that can shut down and delete specified database. The second type of malware attacks is worm attacks, which exploit the network connection to spread the exploit code to new RFID tag. Thus, the exploitation of network connection enables an adversary to access and executes malware from remote location. Furthermore, the third type of Malware is an RFID virus, which can disseminate to the RFID system without requiring an internet connection. In this regards, an adversary is required to have knowledge about the middleware architecture in order to enable the virus to replicate itself in to the beck-end database and then further the application software can rewrite it into the new RFID tag. In addition, on the two other works of the researchers defined in [135-136] demonstrate that the aforementioned types of attacks are even feasible to be launched from RFID tag that has very limited memory.

2.1.8. State-of-the-art Solution for Application Layer Vulnerabilities

Various research works have been proposed to mitigate the threats in application layer, some of them by introducing access control to the client device, in order to prevent unwanted scanning and modification. The blocker tag [18-19] is one example solution in RFID system, which propose a method that selectively block a rogue reader for protecting the consumers from unauthorized reading of RFID tag. Nevertheless, this method introduces various potential abuses, one of them is the scenario that an adversary may use malicious blocker tag to conduct denial-of-service attack in order to break the RFID reader protocol. In addition, two similar approaches to prevent unauthorized reading are proposed by Rieback et al. called RFID Guardian [137] and Juels et. al called RFID Enhancer Proxy (REP) [138]. Such two approaches introduce an intermediate device between the legitimate tag and its reader that acts as a personal RFID firewall. The intermediate device is equipped with powerful feature (e.g. real computing power), which can establishes a privacy zone and policy around the legitimate RFID system. Thus, only authenticated readers can have access to the legitimate tag. Nevertheless, these two conceptual approaches introduce logistical questions about how the intermediate device should acquire and release control of tags and their associated PINs or keys [139].

Enforcing encryption protocol and access control can be used as other option to protect the WIP system from unauthorized reading. Several examples are proposed in [140-142]. However, enforcing such method may introduce further problem such as computation and communication overhead that may not be suitable for the system's limited resource of WIP system.

Various type of malware attacks can be mitigated from the starting point of malware injection which is providing access control so that only authorized client can get access to the communication system. Nevertheless, the attacks can be launched by insider or an adversary who is able to steal the legitimate node. In this case, Rieback et al. [136] suggest for regularly reviewing the code and rigorously checking the sanity to ensure the entire RFID system is clean from vulnerabilities and bugs. In general, Mitrokotsa et al. [81]

suggest all unsubstantial database and middleware features (e.g. back-end scripting) must be turned-off to achieve the integrity protection.

2.1.9. The Threats based on Multi-aspect Vulnerabilities

This section covers various aspects of WIP vulnerabilities reaching from non-technical aspect such as social engineering threats, to various threats that exploit the combination of various vulnerabilities in several layers.

1. Social engineering

On the contrary of spending time for the big effort in technical hacking, an adversary may simply attempt to perform confidential trick to fool the legitimate user, in order to achieve particular gain. For instance, various social skills can be exploited to elicit the sensitive information, performing forgery, or even gain access to system. Various scenarios can be attempted by an adversary, one example is by physically lending the personal devices from authorized clients (e.g. token, tablet, RFID tag, etc.) in order to elicit the sensitive information (e.g. MAC address, security properties, etc.). The adversary even can use the lent device to launch particular attacks such as malware injection or impersonation as legitimate user in order to gain the privilege. An adversary may even pass the entry of restricted room by just trailing the legitimate users or compromising the personal security guard. Thus, based on the aforementioned scenarios, various types of social engineering should also be considered as parameter to achieve the integrity protection.

2. Covert channels

The use of wireless communication makes the WIP system is also susceptible from various technics of covert channel attacks. Such attacks aim at creating a capability to transfer sensitive information through the unused memory storage. It is launched by exploiting possible distinct or hiding channel, rather than use the legitimate one that is subject to access control and encryption process. Since the information is transferred surreptitiously, this type of attacks is arduous to be detected.

covert channel attack is basically can be launched by exploiting various vulnerabilities in several layers [143], reaching from the inherent vulnerabilities on the link layer with MAC addresses, network layer with IP addresses, to the vulnerabilities on transport layer with UDP/TCP port numbers. In the specific case of RFID communications, Bailey et al. [144] define several scenarios which covert channels can be problematic in RFID tags, which are listed as follows.

- "*Covert Sensors / Transaction Monitors: A verifier might use a covert channel to extract side information from a tag. For example, the verifier might obtain information from a hidden sensor, or unauthorized information about transactions performed by the tag.*"
- "*Covert Identification Channels: A manufacturer could implant a covert channel to create an independently and secretly configurable tracking system. Such a system can operate even without the collusion of authorized verifiers* [145]."
- "*Covert Authentication: Paradoxically, it is sometimes desirable for mobile devices like RFID tags to be cloneable; that is, not to authenticate themselves. Researchers have argued in favor of this property in human-implantable RFID tags [7]. If an attacker can easily clone such RFID tags, she will have little incentive to steal them; that is, physically extract the tags, thus harming their owners. The presence (or even the mere possibility) of a covert authentication channel can undermine this important assurance of safety*."

Although launching covert channel attacks is not trivial, particularly in the case of WIP system which the availability of bandwidth and memory storage are not spacious enough, somehow such threats may harm the users once it has successfully launched. Thus, further investigation should be considered in order to combat the addressed problem.

3. Denial of service attacks

Various vulnerabilities in several layers can be exploited in order to launch DoS attacks. It ranges from the vulnerabilities related to physical layer (e.g. physical manipulation), wireless protocol, network protocol, transport layer, to the application layer such as malware attacks. In addition, an adversary may also exploit the constrained nature of WIP system to target specific gain on DoS attacks. An example scenario is an adversary may perform various technics of resource consumption attacks in order to gain malicious benefit related to the limited bandwidth and battery power of WIP' devices. An adversary even may perform DoS by exploiting the other aspects of system's limited resources (e.g. flooding the memory or overburden the processing limit).

Furthermore, an adversary may also exploit the inherent vulnerabilities that are emerged from the particular drawbacks of common security and privacy solution. For instance, a blocker tags proposed by Juels et al. [8-19] is well-known solution proposed to cope with the problem related to user's privacy. Nevertheless, such approach can be misused by an adversary to perform DoS attacks, such as by maliciously using the blocker to break the reader protocol.

4. Traffic analysis

No matter the WIP system uses very strong cryptographic protection and a well-design of communication protocol, an adversary can learn the information pattern by intercepting the encrypted payload. In this regards, an adversary requires to gather the number of messages as much as possible in order to accurately infer the traffic.

Although the encrypted messages cannot be decrypted, an adversary can learn traffic pattern in order to infer the information. For instance, an adversary may be able to observe the traffic information and correlate to the real case based on several example questions, such as who changes to medium to medium which indicates the movement profile, who talks to whom can indicate the relationship among the clients, or who talks when may indicate the position, duty and activities profile of the clients.

5. Attacks on cryptographic algorithms

The WIP system's limited resources make the enforcement of strong cryptographic protection is not feasible to be implemented in. Indeed, it will overburden the limited CPU power, memory storage as well as drain the battery power. Therefore, most of common solutions in WIP system only use cheap cryptographic protection. This issue makes the constrained nature of WIP system is highly susceptible to various attacks on cryptographic algorithms, ranging from various technics of brute force attacks, birthday attacks, to the capability to protect from various threats on discrete logarithm attacks. For instance, Garcia et al. [146] perform reserve engineering attacks on the security method used in contactless smart card system called MIFARE classic. The system is used extensively in access control for office buildings, payment systems for public transport and various other applications. In this case, the researchers aim at addressing the vulnerabilities on the symmetric cipher, the designed authentication protocol, and the knocking procedure. Impressively, the attacker can recover the secret key by just using standard computing resources without any pre-computation and it is accomplished within less than a second. Moreover, the whole payload of the communication between the tag and the reader can be eavesdropped as well as decrypted. It is even feasible to be conducted although multiple authentications are enforced in the whole communications. As the results, this attack can gives particular advantages such as it enables to clone the card or even to restore the original card to a previous value.

6. Side channel attacks

Take into account that some of WIP devices are deployed in unsupervised environments and most of them are lack of physical protection, WIP system is also susceptible from various threats of side channel attacks. Such attacks aim at gaining the malicious advantages from the information leakage based on the vulnerabilities of physical implementation of a cryptosystem. Various parameters can be exploited to infer the valuable information including, power consumption analysis, electromagnetic leaks, time measurement analysis, thermal emission or even emitted sound can be exploited by an adversary in order to break the system (e.g. recover the secret key). In this regards, the successfully rate of such attacks is highly dependent to the technical knowledge of the internal process of the cryptographic system.

Various research works in the fields of side channel attacks have been introduced particularly in wireless environment for embedded devices with cryptographic applications. Gebotys et al. [147] introduces side channel attack in term of exploiting electromagnetic leaks, particularly on Personal Digital Assistant (PDA). Furthermore, Okeya et al. [148] introduce other types of side channel attacks on several Message Authentication Codes (MAC), particularly using Simple Power Analysis (SPA) and Differential Power Analysis (DPA) method. In this work, the authors demonstrate that several key bits can be extracted using SPA. In addition, DPA can be exploited to achieve selective forgery against several MACs including EMAC [149], OMAC [150], and PMAC [151].

7. Replay and Forgery attacks

The broadcast nature of wireless environment makes an adversary has chance to intercept the communications. The adversary can relay and copy the authentication message and later broadcast the message in order to impersonate as legitimate party. By reusing the relayed message, an adversary can impersonate either as legitimate node or peer. Thus, the legitimate parties (i.e. node and its peer) will grant access to each other since they are fooled to think that they communicate in proper manner. An adversary can further exploit this attack for various scenarios. For instance, by impersonating as legitimate client, an adversary can get access to the communication system. In addition, an adversary can further perform malicious activities such as injecting malicious code to propagate malware, getting access to restricted room or building, or performing other forgeries such as impersonating as legitimate reader to reveal the clients' privacy.

2.1.10. State of the art for the threats based on multi-aspect problem

1. Solution for Social Engineering

In order to effectively counter various threats on strategic attacks (e.g. social engineering), Mitrokotsa et al. [81] suggest long-term effort of security process. In this regards, security and data protection policy, as well as performing risk assessment should be established and maintained continuously, in order to specify potential threats and risks. In addition, the security policy should be adequately socialized to all users in order to achieve optimal protection. Furthermore, all organization‘s member should be continuously educated and trained in order to establish knowledge and awareness against critical data protection and organization security.

2. Solution for Side-channel Attacks

Most of side-channel attacks basically can only be launched by physically comprising the targeted devices and within valid range of the used wireless channel. Thus, It is difficult for an adversary to launch such attacks targeted to the personal devices that are typically attached to the human body (e.g. smart phone and body sensor), without firstly stealing the devices. In general, performing side channel attacks are very complicated work, since most of them cannot be done surreptitiously and remotely like common network-based attacks.

To the best of our knowledge, the best way to mitigate side-channel attacks for non-personal devices is by preventing the devices from theft or physically being compromised by an adversary. This can be done by applying standard physical security such as placing camera surveillances, employing personal security guards, applying physical access controls including fences, gates, locked doors, one-way-in, and so on. Thus, it can prevent an adversary to analyze the information leakage, since such attacks basically cannot be launched remotely.

Nevertheless, not every WIP devices are placed in highly supervised area. This issue introduces chance for an adversary to physically compromise the devices in order to analyze the information leakage. Some of research works have introduced various methods to mitigate the threats. Pongaliur et al. [152] introduce comprehensive countermeasures of side channel attacks in wireless sensor node applications. Firstly, the authors propose the use of power randomization, new circuit designs and obfuscation method in order to complicate power analysis attacks. Secondly, the authors also propose three different approaches to mitigate electromagnetic attacks, reaching from encompassing the node to prevent access to the component, using secret share method to divide the computation probabilistically, to the use of masking method to complicate the subset of secret key.

Thirdly, the authors also propose an approach to mitigate optical side channel attacks. Generally, it is recommended to disable all the LEDs function on sensor nodes including the debugging information which an adversary can get feedback about the LEDs information. In term of timing attacks, the authors suggest using more clock cycles so that branching does not affect the execution time. In order to combat fault analysis attacks, it is suggested to use redundancy to catch injected faults. Furthermore, using encapsulation with sound absorbing material is suggested as an effective way to combat sound Acoustic attacks. Moreover, the authors also introduce a method to random the acoustic noise by using similar frequency to obscure sound emissions from sensor nodes. And lastly, the authors suggest using dual-layer cases with different conducting surface in order to combat thermal Imaging attacks. In this case, the inside layer use high conducting material and the outside layer use non-conducting material. Thus, the dual-layer case can muffle heat emission.

Furthermore, various approaches have been introduced to mitigate side-channel attacks [153-156]. Nevertheless, most of aforementioned solutions introduce particular drawbacks including the increase of power consumption, as well as the increase in manufacturing cost. Thus, the aforementioned solutions are not suitable for the constrained nature of WIP system.

3. Solution for Replay and Forgery Attacks

Replay and forgery attacks as well as denial of service attacks can be mitigated by enforcing mutual authentication protocol with cryptographic challenge-response verification. In other words, the legitimate parties challenge their peer to each other in mutual-way with fresh and random cryptographic values for every established session. Thus, an adversary will not be able to answer the challenge by just replaying the old message, which is intercepted during the previous established session. In addition, Mitrokotsa et al. [81] also suggest several simple countermeasures such as use timestamps, one-time passwords, and clock synchronization in order to provide countermeasure for relay attacks. Nevertheless, the aforementioned methods may charge the limited system's resources of WIP applications. Thus, the proposed security protocol that uses the aforesaid methods must be carefully designed to avoid major drawbacks in term of computation and communication overhead.

Various research works have been introduced to mitigate replay attacks in the field of wireless sensor and ad-hoc network. For instance, Huei-Ru et al. [157] propose a protocol called “lightweight dynamic user authentication scheme” with several the features including reducing the risk on user’s password leakage, capability of changeable password, and better efficiency. Lingxuan Hu et al. [158] introduce a protocol with secure aggregation mechanism. This method prevents replay attacks since the sensor node keys are renewed every reading. Karlof et al. [159] present link layer security architecture called TinySec. This method uses application and routing layers to detect replay attacks by inferring information patterns about communication and the network’s topology. In addition, Boukerche et al. [160] introduce a method called “secure localization algorithms”, such method prevent the replay attacks by filters out malicious beacon based on round-trip time (RTT) evaluation that indicates extra delay. The aforementioned solution can be considered as promising solution for the addressed problem in system’s limited resources. Nevertheless, it needs further investigation whether or not it is suitable to be applied in the case of WIP system that has specific challenges and requirements.

4. Solution for Covert Channel Attacks

Detecting and combating various types of covert channel attacks is a complex work. The main problem here is nowadays even the legitimate user has tendency to launch such attacks for particular gain, such as creating different communication channel to bypass the company’s firewall. In technical point of view, various aspects need to be investigated to mitigate these attacks. However, strictly enforcing the security policy, as well as continuously performing security management and risk assessment can be relied to mitigate various threats on covert channel attacks.

5. Solution for Traffic Analysis Attacks

Several common methods can be applied in order to countermeasure against traffic analysis attacks. One of them is by changing radio call-signs frequently, which can confound an adversary to infer the traffic pattern. Other option to prevent traffic analysis is by camouflaging the traffic. It is can be done by sending dummy traffic or continuous encrypted signal so that the communications always looks busy. Thus, an adversary will not be able to accurately infer the traffic pattern. Nevertheless, changing radio call-signs frequently is not feasible for the WIP system that uses standard wireless technologies with different architecture. In addition, sending dummy traffic to camouflage the traffic is power sensitive that can drain the limited battery energy on WIP devices.

During last decade, various methods have been presented in the face of mitigating traffic analysis attacks. It ranges from network coding based [161], removing the correlation of each packet in the network traffic [162], to hop by hop cluster key encryption and sending rate control [163]. However, each solution has particular drawbacks in term of performance. To the best of our knowledge, the best way to mitigate traffic analysis attacks is by protecting the identity of the sender (i.e. source address) and the receiver (i.e. destination address) from being revealed by unauthorized party. This method can be done by including the identities in the encrypted payload. Nevertheless, the open question is how to cryptographically hide the identity without introducing major drawback in processing overhead.

2.2. Short Introduction to Identity-based Encryption

2.2.1. Why Choosing Identity Based Encryption

The idea of Identity-based cryptographic method was initially proposed in 1984 by Adi Shamir [164]. Identity-based Encryption (IBE) is a type of server-based Public Key Cryptography (PKC) that constructs the public key based on the calculation of identity and a set of particular mathematical functions. In addition, the corresponding private key is constructed based on the public key and its set of mathematical functions. In the beginning, Shamir proposed the IBE method to simplify the complexity of certificate management in e-mail system. In particular, Shamir proposed email address as identity to be calculated as public key. The idea of this method enables the client (i.e. sender) to encrypt email by using the public key string of the recipient email address. In this regards, the sender does not need to obtain the recipient's public key certificate. In other words, the sender can simply send the encrypted email to the recipient even if the public key certificate of the recipient has not been set up.

In the case of WIP system, we propose MAC Address to be used as identity since it is the lowest layer addressing method in wireless communication. This method also enables the proposed security mechanism to be performed over data-link layer. To enable the identity calculation, we firstly use hash function (e.g. MD5) to converts the binary MAC address to 128 bit integer. Thus, the hashed value of MAC address can be used to calculate pair of public key and its corresponding private key.

Comparing to common server-based Public Key Infrastructure (PKI), IBE has different characteristics that can give advantages to the constrained nature of WIP. The following list outlines the IBE system characteristics from WIP system point of view.

- Off-line encryption operations with efficient communication overhead. In the beginning, the clients and the authenticators are required to retrieve a set of public parameters and their private keys from the trusted third-party server. After this step, authentication and encryption process can be conducted repeatedly without further connection to the server. This mechanism is different compare to common server-based systems (e.g. certificate system) that always require connection to the server for each encryption and authentication process. In general, this feature can save the bandwidth consumption, which is suitable to the WIP system that has limitation in term of data-rate.
- Efficient privacy protection. Privacy preserving is a critical aspect in WIP system. IBE system establishes security mechanism that includes the identity in the

encrypted payload. Thus the privacy is effectively preserved since the identity is protected from being revealed by unauthorized party.

- Minimizing the risk on private key misuse. Common PKI system such as certificate system introduces significant risk on private key misuse [Bruce Schneier]. One of distinction of IBE system is that all clients in the communication system including the peers and its clients cannot arbitrary generates their own private key. In this regards, the master secret key that is used to generate the private key is only own by the trusted third-party server. Thus, the misuse can be controlled since only the server can generate the corresponding private key for all clients.
- Simplified the infrastructure requirement and trust relationship. Common PKI system requires complex infrastructure to manage and distribute the certificate. In addition, the most difficult problem is to build trust relationship that might demand higher requirements in term of communication and computation resources. In IBE system, the one and only challenge is to build the trust relationship with the server that generates the private keys. Thus, compared to common PKI system, the IBE system requires modest infrastructure and trust relationship to renew the expired security properties including private key update.

In general, the use of IBE method is more suitable for the constrained nature of WIP system that demands efficient resources consumption.

2.2.2. Pairing Based Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is a type of PKC that relies on elliptic curves defined over finite fields. Compared to non-ECC cryptography such as RSA method, ECC introduces particular advantages. Among such advantages, ECC offers smaller key size in the same level of security protection. According to NIST recommendation, a 160 bit ECC method is equivalent to a 1024 bit traditional public key method such as RSA. Thus, the advantage on smaller key requirement introduces further benefit in term of computation and communication overhead. Indeed, ECC offers faster computation and efficient bandwidth and energy consumptions, as well as smaller memory requirement. Thus, in general ECC is suitable for the constraint nature of WIP system.

In order to optimize computation efficiency, we use the Tate (ηT) Pairing, which is known as the fastest Pairing Based Cryptography (PBC) over super singular elliptic curves [166]. In particular, the pairing method is defined over ternary field $F_{3^{509}}$ [168] with embedding degree 6 ($F_{3^{509} x 6}$). Such extension field provides advanced-level 128 bit security strength, which is claimed has about same security level as 1024 bit RSA modulus [170]. The construction of Tate pairing is based on Discrete Logarithm Problem (DLP), more detail about Tate pairing is defined in [165][167].

Chapter 3

Proposed Solution for WIP Based on WLAN/WPAN Technologies

3.1. Introduction & Motivation

Due to their considerable advantages, Wireless Indoor Positioning (WIP) techniques based on IEEE 802 including Received Signal Strengths (RSS), Time of Arrival (TOA) and Angle of arrival (AoA), have driven much more attention in research and development during the last decade. Indeed, such positioning techniques introduce various advantages reaching from economical aspects like low cost implementation and maintenance, to technical aspects like arguably more reliable as well as its flexibility to be implemented in the existing wireless communication system.

Nevertheless, WIP based on IEEE 802 is naturally vulnerable system that introduces tremendous problems in security and privacy. The following list outlines the security and privacy challenges as well as threat models in WIP system.

- One of critical challenges is to establish privacy preserving. Adversary always has chance to reveal the user attendance and activities based on identity revealed in the communication process.

- WIP system is vulnerable to various attacks based the existence of rogue devices. Adversary might install the rogue device to perform malicious activities, reaching from fraudulence like reporting wrong attendance, unauthorized tracking, data manipulation, cloning attack, to various Man-in-the-middle (MITM) attacks like Denial of Services (Dos), replay attack, reflection attack, etc.

- WIP system is highly susceptible to insider attack. Legitimate users might misuses their authorization to reveal other user privacy and have better chance to perform all aforementioned attacks.

- WIP system is typically a heterogonous network consisting of various access technologies including IEEE 802.11 and IEEE 802.15.4. In addition, WIP system typically consists of various device characteristics, including embedded sensor node with limited capabilities in term of data rate, CPU, memory, and battery/power. Therefore, the enforcement of security and privacy mechanism in WIP system is complicated. On the other hand, using common security solutions such as Transport Layer Security (TLS) is not feasible for the constrained nature of WIP.

- WIP system is also susceptible to various attacks like in Wireless Sensor Networks (WSN). One example is various techniques of resource consumption attacks, which aim at wasting bandwidth as well as draining the battery power. It can be performed by repeatedly sending amount of packets that overburden the limited capabilities of the embedded devices.

In this chapter we introduces IMAKA-Tate, a light-weight Identity Protection, Mutual Authentication and Key Agreement based on cryptographic Tate (ηT) pairing. It is defined over ternary field $F_{3^{509}}$ [168], which is known as the fastest pairing over super singular elliptic curves [166]. IMAKA-Tate aims at providing novel security and privacy method tailored to tackle the aforementioned security and privacy challenges in WIP system.

3.2. Related Work

Our work touches vast field of research works as WIP IEEE 802 system is established based on various aspects of wireless communication system. In this section we briefly outline several existing solutions that relate to our work.

Mulkey, Kar and Katangur [181], purposed IBE method for efficient authentication and privacy for wireless networks IEEE 802.11. Mainly, they enhanced the existing WPA solution by applying such IBE method. Nevertheless, MAC Address or client identity is sent in clear message on the beginning of authentication request. This issue introduces an opportunity for an adversary to reveal the user position and activities based on the observed identity. Furthermore, an important feature like mutual authentication was not provided in this solution.

In WSN domain, Szczechowiak and Collier [169] designed TinyIBE using ηT pairing, which successfully rebutted the common misconception that IBE method is too heavy for sensor node. They proved that using ηT pairing is feasible even on at very constrained sensor nodes. Nevertheless, mutual authentication was not proposed on the TinyIBE and it was designed only for static nodes. Thus, it is not suitable for WIP system that deals with dynamic or mobile nodes.

Kolesnikov and Sundaram proposed Identity-Based Authenticated Key Exchange Protocol (IBAKE) [171]. It aims at improving AKE that suffers from key escrow problem [172][173]. This work was continued in [174], which defined the authentication and key agreement using B-Franklin [175] and B-Boyen [176] method. Moreover, IBAKE is being improved in the on-progress work [177], by defining mechanism to transmit IBAKE message through Extensible Authentication Protocol (EAP). Nevertheless, IBAKE employs expensive cryptographic processing as well as high communication overhead. Moreover, such protocol partially relies on upper layer method called Transport Layer Security (TLS), which introduces expensive communication overhead.

3.3. Proposed Scheme

3.3.1. Preliminaries

In order to tackle the WIP challenges, IMAKA-Tate establishes encryption of the communication data starting with the initial step of authentication process. In this regards, the entire communication payloads including the user identity are transmitted in encrypted channel. Furthermore, in order to achieve light-weight as well as strong security protection, we particularly apply ηT pairing, which relies on extension ternary field $F_{3^{509 x 6}}$ defined in [168]. Such extension field provides high-level 128 bit security strength, which is about same security level as 1024 bit RSA [170].

We assume in the WIP system that two parties which are coordinator and node establish mutual authentication to each other. The coordinator is a static point that calculates and defines the position of other party called nodes, while the nodes are commonly user mobile devices or might be also embedded sensor node, which their position are mapped by the coordinator.

3.3.2 Setup Phase

The setup phase is conducted before network deployment and it is established by the trusted third-party called Key Generation Function (KGF), which is handled by the administrator. In other word, the existence of KGF is no longer needed after the administrator successfully distributes all parameters that are required to construct the IBE method.

On the setup phase, the KGF generates all secret parameters that would be trustily preloaded to each device's memory. The generated parameters include a 128 bit integer master secret key *s*, where $s \in Z_q^*$. The KGF also defines supersingular elliptic curve over F_q^*, where $F_q^* = F_{3^{509}}$. Furthermore, several public parameter are generated, the first one is a random point on elliptic curve *P*, where $P \in E(F_q)$. The second one is another random point *Q*, where $Q \in E(F_q)$ and *Q* = *sP*. The last one is *g*, where $g = e(P, P)$ and *e* is a

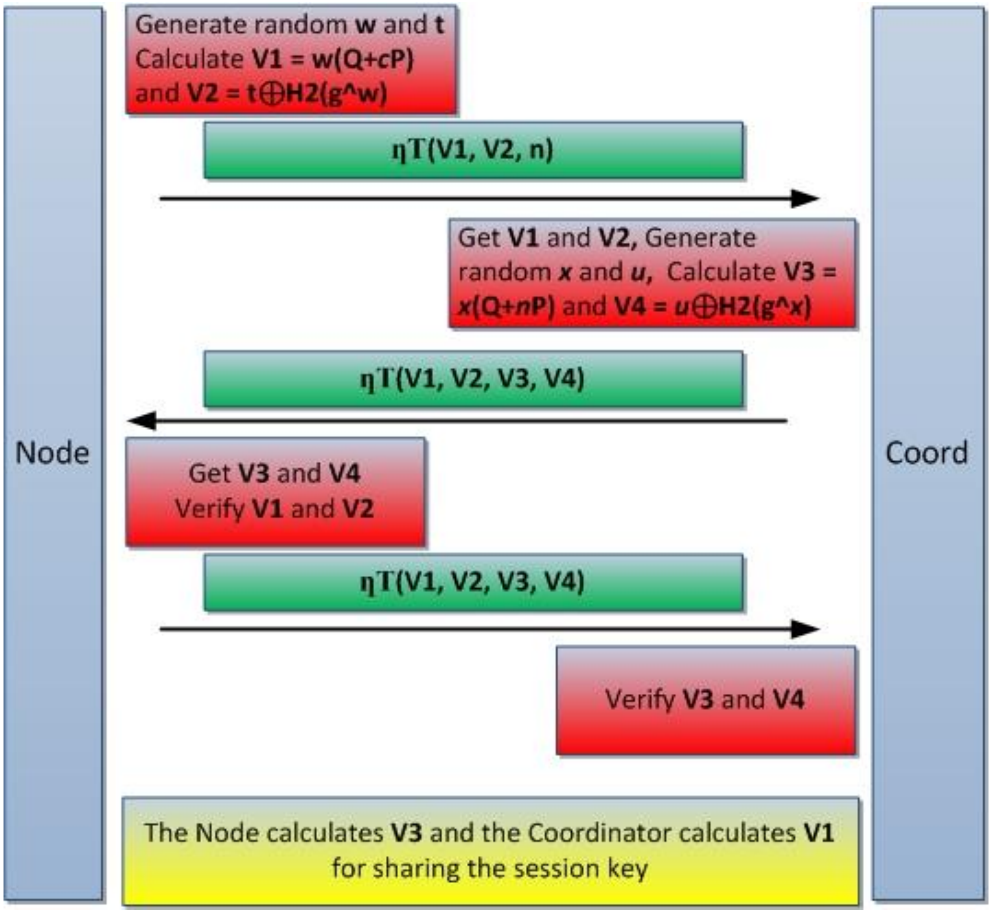


Figure 3.1. Three-way handshake of mutual authentication and key agreement.

function which maps $E(F_{3^{509}})$ x $E(F_{3^{509}}) \to F_{3^{509\,x\,6}}$. Moreover, the KGF defines two hash functions, *H1* is the function to transform a binary MAC address to a 128 bit integer, where *H1* : $\{0,1\}^* \to Z_q^*$. Another hash function is *H2*, which convert the extension filed $F_{3^{509\,x\,6}}$ to a 128 bit integer, where H2 : $F_q \to \{0,1\}^n$.

In order to keep minimum computation overhead on each node, the KGF generates and distributes all private keys of each node based on the master secret key *s*. The KGF generates a private key for each node *N*, by calculating $N = \frac{1}{s+n}P$, in this context, *s* is master secret key and *n* is public key of each node calculated as *n* = *H1(node MAC address)*. Similarly, the KGF also generates another private key for the coordinator, $C_{Ord} = \frac{1}{s+c}P$, where *c* = *H1(coordinator MAC address)*. In general, all parameters that are preloaded to the coordinator and each node memory are: Private Key (C_{Ord} or N), P, Q, g, $H1$ and $H2$.

3.3.3. Authentication and Key Negotiation Phase

In this phase the coordinator and the node perform three-way handshake for mutual authentication and session key negotiation. Figure 1 illustrates the three-way handshake as described as follows.

1. The node randomly generates two 128 bit integer *t* and *w*, where *t* is temporary session key. The node also calculates the coordinator's public key *c* = *H1(coordinator MAC address)*, by assuming that the coordinator periodically broadcasts its beacon frame. Thus the node can easily find the MAC address for calculating the public key.
2. The node then generates two ciphertexts $V1 = w(Q + cP)$ and $V2 = t \oplus H2(g^{w})$. The node subsequently requests to join in the WIP system by sending the two ciphertexts to the coordinator. The node also includes its MAC address *n* = *H1(node MAC address)* in the encrypted payload, in order to protect its identity from being revealed by unauthorized party. In this case, all contents in the message including the session key *t* and the node MAC address are encrypted using the coordinator public key. Thus, only the coordinator can decrypt the message.
3. The coordinator receives and decrypts the messages using its private key C_{Ord}. The coordinator can recover the session key *t* by calculating $t = H2(e(C_{Ord}, V1)) \oplus V2$. In order to achieve efficient communication, the coordinator tentatively saves the key *t* and the value of V1 for further steps. Each message created by the node in the three-way handshake will use the initial session key *t* and the value of *V1* will be used to calculate primary session key.

The temporary session key are shared based on the pairing function calculated as follows.

$$t = H2(g^{w}) \oplus V2 \qquad (3.1)$$

since

$$e(C_{Ord}, V1) = e\left(\frac{1}{s+c}\, P, w(Q + cP)\right)$$

$$= e(P, Q + cP)^{\frac{w}{s+c}}$$

$$= e(P, (s + c)P)^{\frac{w}{s+c}}$$

$$= e(P, P)^{w} = g^{w} \qquad (3.2)$$

4. In the second message of the three-way handshake, the coordinator generate *x* and *u* as two random 128 bit integers, where *u* is temporary session key for processing all messages created by the coordinator. The coordinator afterward generates and send two ciphertexts *V3 = x(Q + nP)* and *V4 = u ⨁ H2(g^{x})*. The coordinator also includes the values of *V1* and *V2* in the encrypted message to be further verified by the node.

5. The node then receives and decrypts the message which contains temporary session key *u* using its private key *N*. It is conducted by calculating *u = H2(e(N, V3)) ⨁ V4*. The node further verifies the value of *V1* and *V2*. The further step is then continued only if the two values are same as the two values of *V1* and *V2* generated by the node on the first message. Otherwise, the node aborts the authentication. The node also saves the value of *V3* in order to calculate the primary session key.

6. The node then sends back the value of *V3* and *V4* to be verified by the coordinator. The coordinator then process the message using the session key *t* that has been collected before. The further step is continued if the received values are equal as the values generated by the coordinator on the second message. Otherwise, the coordinator sends failure notification to abort the connection.

Up to this step, both parties have mutually authenticated to each other. In addition, they also effectively succeed to share the 128 bit primary session key. It is conducted by computing the two random values of *V1* and *V3* that have been securely exchanged on the three-way handshake. In this case:

- The node computes *H2(*$e(N, V3)^{w}$*)*
- The coordinator computes *H2(*$e(C_{Ord}, V1)^{x}$*)*

Both parties calculate the same session, since:

$$\begin{aligned}
\mathrm{e}(C_{Ord}, \mathrm{V1})^{x} &= \mathrm{e}(C_{Ord}, w(\mathrm{Q} + c\mathrm{P}))^{x} \\
&= e\left(\frac{1}{s+c}\,\mathrm{P}, w(s\mathrm{P} + c\mathrm{P})\right)^{x} \\
&= e(\mathrm{P}, (s\mathrm{P} + c\mathrm{P}))^{\frac{wx}{s+c}} \\
&= e(\mathrm{P}, \mathrm{P})^{wx} \qquad (3.3)
\end{aligned}$$

and

$$\begin{aligned}
\mathrm{e}(\mathrm{N}, \mathrm{V3})^{w} &= \mathrm{e}(\mathrm{N}, x(\mathrm{Q} + n\mathrm{P}))^{w} \\
&= e\left(\frac{1}{s+n}\,\mathrm{P}, x(s\mathrm{P} + n\mathrm{P})\right)^{w} \\
&= e(\mathrm{P}, (s\mathrm{P} + n\mathrm{P}))^{\frac{wx}{s+n}} \\
&= e(\mathrm{P}, \mathrm{P})^{wx} \qquad (3.4)
\end{aligned}$$

3.3.4. Mutual Authentication over EAP

To support efficient and scalable communication for heterogeneous wireless IEEE 802, IMAKA-Tate transports the authentication messages through standard EAP method (RFC 3748) [178]. As illustrated in Figure 2, all authentication messages are transported in encrypted payload. Thus, it prevents adversary to reveal the credentials in order to perform malicious activities such as various techniques of MITM attacks (e.g. replay attack, relay attack, reflection attack, etc.). Furthermore, IMAKA-Tate simplifies the authentication by

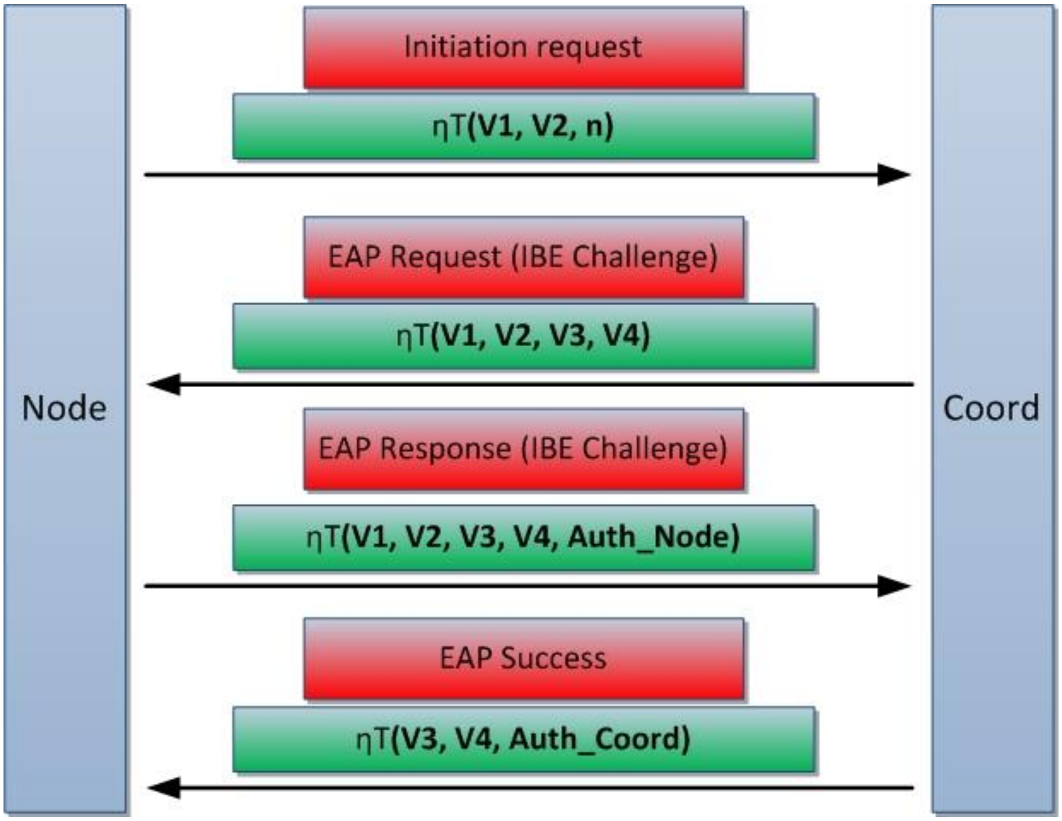


Figure 3.2. IMAKA-Tate over EAP.

eliminating the identity exchange. This mechanism is different like in common EAP method, as our protocol specifically works based on MAC Address.

IMAKA-Tate aims at providing light-weight security protocol that maintains the size of authentication payload as optimally minimum. As illustrated in figure 3, IMAKA-Tate defines new header field called IMAKA-Tate Exchange. It is one-octet in length that identifies the encrypted-authentication messages. The values are identified as follows.

- 1 = IBE Challenge-EAP Request/Respond
- 2 = IBE Failure Notification

Furthermore, IMAKA-Tate transports encrypted payloads, which are composed as follows.

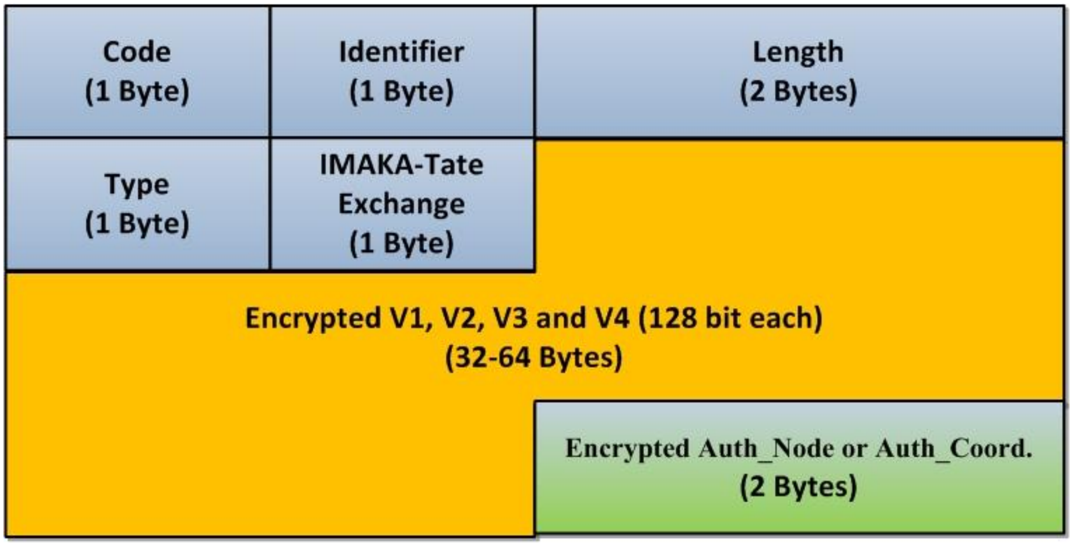


Figure 3.3. EAP IMAKA-Tate message format.

- The Values of V1, V2, V3, and V4 are each encrypted 16 Bytes that are transported during the IBE Challenge request and respond message.

- Either Auth_Node or Auth_Coordinator is 2 Bytes notification message attached in the encrypted payload.

3.4. Security Analysis

This section presents the security strength of IMAKA-Tate against various risks and attacks, as well as discusses security features that enable the integrity protection in WIP system.

3.4.1. Access Control, Rogue Devices and the Insiders

In WIP system, an adversary can create rogue coordinator in order to spoof legitimate users to reveal their credentials. Hence, an adversary can exploit the revealed credentials to conduct malicious actions (e.g. reporting wrong attendance, unauthorized tracking, data manipulation, DoS, cloning attack, etc.). Nevertheless, an adversary has no chance to reveal all parameters (i.e. *e, P, Q, g, H1* and *H2*) that secretly pre-load before the network deployment. In this case, the rogue coordinator is not able to perform mutual authentication and key agreement on the three-way handshake. Thus, IMAKA-Tate can mitigate the aforementioned threats by preventing the rogue coordinator to be authenticated in WIP system.

Let us presume that the rogue coordinator has different parameters (i.e. *e', P', Q', g', H1'* and *H2'*). In this case, the rogue coordinator is not able to respond the three-way handshake requested by the node. Moreover, the rogue coordinator does not possess the master secret key *s*, which is known only by the KGF. Hence, the rogue coordinator wrongly generates its private key. Let us presume that the rogue coordinator has different master secret key r ≠ s. The rogue coordinator then incorrectly generates its public key $c_{Rog} \neq c$ and private key $C_{Rog} \neq C_{Ord}$:

$$c_{Rog} = H1'(\text{rogue coordinator MAC address}) \qquad (3.5)$$

$$C_{Rog} = \frac{1}{r + c_{Rog}} P' \qquad (3.6)$$

Moreover, the rogue coordinator is not able to correctly calculate the initial session key *t*, since:

$$t \neq H2'(e'(C_{Rog}, V1)) \oplus V2 \qquad (3.7)$$

Since the initial session key *t* is calculated incorrectly, the rogue coordinator is not able to decrypt the initiation message *ηT(V1, V2, n)*. Hence, the rogue coordinator is not able to find the node MAC Address in order to respond the message. Moreover, the challenge is more complicated for adversary, as it is not possible to convert *n* value to node MAC address based on the incorrect parameter H1', since:

$$n \neq H1'(\text{node MAC address}) \qquad (3.8)$$

An adversary may conduct social engineering to inquiry the user's MAC Address. However the adversary is still not able to correctly generate the user public key and the two ciphertexts. This issue makes the node is not able to calculate the temporary session key *u*. Let us presume that the rogue coordinator generates $n' \neq n$, $V3' \neq V3$ and $V4' \neq V4$:

$$n' = H1'(node\ MAC\ address) \qquad (3.9)$$

$$V3' = x(Q' + n'P') \qquad (3.10)$$

$$V4' = u \oplus H2'(g'^{x}) \qquad (3.11)$$

However the node wrongly calculates the key *u*, since:

$$u \neq H2(e(N, V3')) \oplus V4' \qquad (3.12)$$

Hence, the node aborts the connection as the value of *V1* and *V2* attached on *ηT(V3', V4', V1, V2,)* cannot be verified.

Furthermore, both parties are not able to correctly generate and share the primary session key, as the node calculates:

$$\begin{aligned} e(N, V3')^{w} &= e(N, x(Q' + n'P'))^{w} \\ &= e\left(\frac{1}{s+n}\ P, x(rP' + n'P')\right)^{w} \\ &= e(P, (rP' + n'P'))^{\frac{wx}{s+n}} \\ &= e(P, P')^{\frac{wx(r+n')}{s+n}} \qquad (3.13) \end{aligned}$$

On the other hand the rogue coordinator calculates:

$$\begin{aligned} e'(C_{Rog}, V1)^{x} &= e'(C_{Rog}, w(Q + cP)\ )^{x} \\ &= e'\left(\frac{1}{r+c_{Rog}}\ P', w(sP + cP)\right)^{x} \\ &= e'(P', (sP + cP))^{\frac{wx}{r+c_{Rog}}} \end{aligned}$$

$$= e'(P', P)^{\frac{wx(s+c)}{r+c_{Rog}}} \qquad (3.14)$$

By taking into account an insider who already owns all parameter that pre-loaded in his valid device's memory. In this scenario, an adversary can abuse his authority to create the rogue coordinator. However, the master secret key *s* is owned only by the KGF and it is never shared to any party, neither to the coordinator nor to the node. In this case, the insider is not able to generate the correct private key for the rogue coordinator. Let us presume that the rogue coordinator use incorrect master secret key $r \neq s$. The rogue coordinator incorrectly generates its private key:

$$C_{Rog} = \frac{1}{r+c_{Rog}} P \qquad (3.15)$$

Hence the rogue coordinator is not able to generate correct initial session key *t* as described in equation (1) and (2), since:

$$e\left(C_{Rog}, V1\right) = e(C_{Rog}, w(Q \ + \ cP)$$

$$= e\left(\frac{1}{r+c_{Rog}}\ P, w(sP + cP)\right)$$

$$= e(P, (sP + cP))^{\frac{w}{r+c_{Rog}}}$$

$$= e(P, P)^{\frac{w(s+c)}{r+c_{Rog}}} = g^{\frac{w(s+c)}{r+c_{Rog}}} \qquad (3.16)$$

In this case:

$$t \neq H2(g^{\frac{w(s+c)}{r+c_{Rog}}}) \oplus V2 \qquad (3.17)$$

In general, IMAKA-Tate can prevent the node from being arbitrary read by the existence of rogue device (e.g. rogue coordinator). This method is enforced by providing access control that prevents both authorized coordinator and malicious node to get access into the WIP system. In addition, the proposed protocol can also mitigate malicious threats from the insiders who misuse their access right.

3.4.2. Privacy Issue and Attack Based on Revealed Identity

Protecting the identity is a crucial aspect in WIP system. An adversary can observe the user identity and use it to perform malicious activities, which are listed as follows.

- An adversary can inquiry the user attendance, as well as reveal the user activities based on the attendance and movement profiles. In WIP application, it is definitely a serious problem that must be tackled as it contradicts with the crucial aspect of user privacy.

- An adversary can perform various techniques of resource consumption attacks. The adversary can waste the node bandwidth and drain the battery by insistently sending packets to the revealed identity as destination address.

- An adversary initially reveals the user identity as one of requirements that is needed in order to successfully perform various attacks (i.e. node capture attack, reflection attack, replay attack, and various attacks based on revealed identity).

Nevertheless, IMAKA-Tate performs the encryption method that includes the node identity since in the initiation request of mutual authentication. Particularly, the node firstly hashes its MAC Address to 128 bit integer *n = H1(node MAC address)*. Subsequently, it is enclosed to the encrypted payload of the initiation request $\eta T(V1, V2, n)$. Hence, there is no chance for an adversary to reveal the user identity since it encrypts even before the mutual authentication is started.

3.4.3. Special Issue on Physical and Multi-layer Threats

IMAKA-Tate provides an integrity protection that covers the security and privacy problem in broader aspects of WIP vulnerabilities. The following list outlines various threats that can be mitigated by the proposed protocol, ranging from the threats based on inherent vulnerabilities in physical layer (e.g. relay attacks), inherent vulnerabilities in network and transport layer, to various threats that exploit and combine several vulnerabilities in multi-layer problem.

1. Relay Attacks

Relay attacks are one of the most difficult challenges to be tackled particularly in the constrained nature of WIP system. It is to be noted that the use of upper layer security protections even with very strong cryptographic primitives and well-designed protocol are not enough to mitigate the attacks. Take into account that an adversary can use transponders to act as Man-in-the-Middle. In this case, the transponders that are logically placed in between the two legitimate parties (i.e. the node and the coordinator) can intercept the message even it is transported over cryptographic protocol. Here, an adversary does not need to break the cryptographic protection, instead he just aims at revealing meta-data information attached on the radio signal in order to achieve particular gain. For instance, an adversary can relay the message and spoof the node's location information by modifying the Time-of-Arrival (TOA). Therefore, relay attacks cannot be combated by just using cryptographic protocol that relies on upper layer method.

By just intercepting the message, an adversary can reveal some sensitive information such as the TOA that implies the victim's position information. Indeed, an adversary may infer various meaningful information that are implemented at lower layer including collision detection and avoidance, demodulation, error detection and correction, synchronization and retransmission.

To mitigate relay attacks, IMAKA-Tate establishes the security and identity protection in the lowest possible layer (i.e. Data-link layer). It is performed by establishing two tier protection methods. Firstly, by hashing the MAC address to 128 bit integer value:

$$n = H1(node\ MAC\ address) \qquad (3.18)$$

and then by including the hashed value to the encrypted payload of the session:

$$V3 = x(Q + nP) \qquad (3.19)$$

In this case, an adversary may be still able to reveal the location information of the particular node based on the meta-data information (i.e. time of arrival). Nevertheless the adversary will not be able to recognize the node identity which is included in the encrypted payload in the data-link layer. In other word, an adversary may still be able to launch the relay attacks, however he will not be able to gain significant benefit since there is no chance to identify the node, particularly in density environments. Indeed, an adversary must firstly break the session key to infer the hash value *n* that is included in *V3 = x(Q + nP)*:

$$u = H2(e(N, V3)) \oplus V4 \qquad (3.20)$$

And then an adversary must break the hash value n to infer the MAC address:

$$n = H1(node\ MAC\ address) \qquad (3.18)$$

In conclusion, eliciting the position information without revealing the identity (i.e. the MAC address) is considered as meaningless information.

2. Network and Transport Layer Attacks

Various types of attacks can be launched based on inherent vulnerabilities in network and transport layer. It ranges from resources various technics of Man-in-the-Middle attacks, resource consumption attacks, impersonation, eavesdropping, node capturing, spoofing, to various types of attacks that aim at breaking the network protocol. Nevertheless, the aforementioned attacks cannot be conducted without revealing the identity (i.e. the MAC address). In our case, the identity is included in the two tier encryption methods.

$$\mathrm{n = H1(node\ MAC\ address)} \qquad (3.18)$$

$$\mathrm{V3 = x(Q + nP)} \qquad (3.19)$$

Take into account that all successful attacks that are conducted in the network and transport layer require to initially reveal the identity (i.e. MAC address), thus protecting the identity is effective approach to mitigate the aforementioned attacks.

We take an example on resources consumption attacks, an adversary will not be able to send amount of dummy packets to the particular node without firstly revealing the node's MAC address. In this case, an adversary must firstly perform formidable work to break the session key, the value of *V3,* the hash value of n in order to elicit the MAC address. In the same case, there are no chances for an adversary to perform various attacks based on inherent vulnerabilities in network and transport layer without revealing the MAC address.

Furthermore, IMAKA-Tate performs mutual authentication and verification methods that strengthen the security and privacy protection in these layers. These methods are established by performing session encryption using the public key of the recipient. Thus, only corresponding private key of the particular recipient can correctly recover the session key and the cryptographic challenges attached in the encrypted payload. In this case, the coordinator authenticates the node using its private key C_{Ord}:

$$t = H2(e(C_{Ord}, V1)) \oplus V2 \qquad (3.21)$$

The node authenticates the coordinator using its private key *N*:

$$u = H2(e(N, V3)) \oplus V4 \qquad (3.20)$$

In addition, both parties perform challenge-respond verification by matching the random cryptographic values attached in the encrypted payload. In this case, the node verifies the received value of *V1* and *V2* that were generated in the first message of the tree-way handshaking, while the coordinator verifies the received value of *V3* and *V4* that were generated in the second message of the mutual authentication. Thus, the access will be aborted if the values do not satisfy the verification rule.

Thus, there is no chance for an adversary to maliciously modify the messages and play with malicious activities such as man-in-the-middle attacks. In general, IMAKA-Tate establishes mutual authentication and challenges-respond verification that enable access control and mitigate various threats in network and transport layer.

3. Replay and Forgery Attacks

An adversary can relay and copy the authentication message and later broadcast the message in order to impersonate as legitimate party. By reusing the relayed message an adversary can impersonate either as legitimate node or coordinator. Thus, the legitimate parties (the node and its peer) will grant access since they are fooled to think that they communicate in proper way. An adversary can further exploit this attack for various scenarios. For instance, by impersonating as legitimate client to access into the communication system, an adversary can further perform malicious activities such as injecting malicious code to propagate malware, getting access to restricted room or building, or performing other forgeries such as impersonating as legitimate coordinator to reveal the clients' privacy.

Replay and forgery attacks can be mitigated by enforcing mutual authentication protocol with cryptographic challenge-response verification. In other words, the legitimate parties challenge their peer to each other in mutual-way with fresh and random cryptographic values for every established session. Thus, an adversary will not be able to answer the challenge by just replaying the old message, which is intercepted during the previous established session.

Let us presume that an adversary intercepts and uses the old authentication message *V1* and *V2* that were generated on the previous session:

$$V1 = w(Q + cP) \tag{3.22}$$

$$V2 = t \oplus H2(g^{w}) \tag{3.23}$$

In order to establish a new session, the legitimate node randomly generate two fresh 128 bit integer t' and w', where t' is temporary session key. The random values are used to calculated new chippertexts *V1'* and *V2'*:

$$V1' = w'(Q + cP) \tag{3.24}$$

$$V2' = t' \oplus H2(g^{w'}) \tag{3.25}$$

In this case, the node decrypts the old message sent by the adversary and on the verification phase the node find that the value of $V1' \neq V1$ and $V2' \neq V2$. Thus, the legitimate party (e.g. the node) will discard the services by aborting the request. To mitigate this issue, we design

IMAKA-Tate that can satisfy the mutual authentication and verification features with fresh and random challenges generated for every session.

4. Traffic Analysis Attacks

No matter the WIP system uses very strong cryptographic protection and well-design of communication protocol, an adversary can learn the information pattern by intercepting the encrypted payload. In this regards, an adversary requires to gather the number of messages as much as possible in order to accurately infer the traffic information.

Although the encrypted messages cannot be decrypted, an adversary can learn and infer specific information such as who changes to medium to medium which indicates the movement profile, who talks to whom can indicate the relationship among the clients, or who talks when may indicate the position, duty and activities profile of the clients.

IMAKA-Tate can mitigate traffic analysis attacks by protecting the identity of the node from being revealed by unauthorized party. This method can be done by firstly hashing the identities into 128 bit integer and attaching the hash value in the encrypted payload.

$$n = H1(\text{node MAC address}) \tag{3.18}$$

$$V3 = x(Q + nP) \tag{3.19}$$

In this case, an adversary will not be able to particularly infer the traffic pattern since he will not be able to reveal the encrypted identity transported in the encrypted payload. Thus, the adversary will not be able to reveal the source and destination address of the traffic, as these are critical data to infer the traffic. In other world, an adversary may be still able to intercept and learn the pattern of the encrypted messages. However, without revealing the identity, the adversary will not be able to answer particular questions such as who changes to medium to medium which indicates the movement profile, who talks to whom which can indicate the relationship among the clients, or who moves when which may indicate the position, duty or values of the particular node. In general, there is no chance for an adversary to infer the traffic information without revealing the packets' identity.

3.4.4. Additional Security Features

The following list outlines the security features offered by IMAKA-Tate, which aim at providing trust and integrity protection in WIP environment.

- Mutual Authentication and Key Agreement: IMAKA-Tate establishes mutual authentication that each participant generates random challenge, which is encrypted by the corresponding public key of the recipient. Such mechanism ensures that only targeted recipient can decrypt and correctly answer the challenge. This procedure is conducted in mutual way. In this case, they exchange and verify the ciphertexts of (*V1, V2)* and (*V3, V4)*. This feature can also prevent various MITM attacks (e.g. replay attack, reflection attack, DoS, etc.). Furthermore, both parties simultaneously negotiate the primary session key based on the exchanged challenge. In particular, the coordinator and the node calculate the same session key:

$$e(C_{Ord}, V1)^x = e(N, V3)^w = e(P, P)^{wx} \qquad (3.26)$$

- Perfect Forward and Backward Secrecy: On each established session, both participants freshly generate random 128 bit integer attached in the encrypted message that they exchange to each other. In particular, the node generate random 128 bit w enclosed in chipper text *V1* = $w(Q + cP)$, while the coordinator generate 128 bit x enclosed in *V3* = $x(Q + nP)$. Thus, both participants generate the same session key, since the coordinator generates:

$$e(C_{Ord}, w(Q + cP)\,)^x = g^{wx} \qquad (3.27)$$

  And the node generates:

$$e(N, x(Q + nP))^w = g^{wx} \qquad (3.28)$$

Hence, in case an adversary with very good fortune is able to compromise the past session, he/she somehow will not able to compromise the following session, since the established session is always fresh and will not correspond to any past or even future session.

- Light-weight communication overhead: To achieve efficient battery and bandwidth consumptions, IMAKA-Tate maintains the communication overhead as minimum as possible. According to IMAKA-Tate packet format depicted in figure 3, the maximum size of authentication packet is only 72 Bytes, which is transported in EAP respond-IBE Challenge (see figure 3.2). Therefore, it is suitable for WIP nature that associates to limited resources including low-date rate, low CPU and battery power.

- Light-weight cryptographic operation with high-level security strength: IMAKA-Tate applies 128 bit security strength of ηT paring method. This method is known as the most light-weight cryptographic operation, even it is enforceable for a sensor node [4]. In addition, such security strength is approximately same as the 1024 bit of RSA method. Thus, the WIP system is adequately protected from various techniques of brute-force attacks.

- Link layer Security method: IMAKA-Tate relies on data link layer over EAP method. This feature is to ensure efficient and feasible authentication and key agreement for the constrained nature of WIP. Furthermore, it can also prevent tremendous security problem derived from the use of upper layer method (e.g. various security problem derived from the use of PKI method [179], various TLS renegotiation attacks [180], MITM attacks, etc.).

In general, the security features can strengthen the security and privacy protection and mitigate various threats in broader aspects of WIP system.

3.4.5. Potential Drawback and its Mitigation

The system's limited resources of WIP application prevent the use of very strong cryptographic protection to be applied in. Surprisingly, a recent research work presented by Gora Adj et al. [185] report that 128 bit security level of cryptographic Tate pairing over $F_{3^{509x6}}$ is less resistant to attacks on the elliptic curve Discrete Logarithm Problem (DLP). In this work, the authors estimate that the logarithms can be computed in $2^{81.7}$ time unit, by using combination algorithms introduced by Joux [186] and Barbulescu et al. [187]. Although computing $2^{81.7}$ is obviously a very hard challenge, the authors argue that it might be possible in the foreseeable future for a very well-funded adversary or at least for the one who has access to a massive number of processors (e.g. 2^{30} processors). The authors predict that the use of such massive number of processors can execute the computing challenge within one year.

To mitigate the potential drawbacks, we design IMAKA-Tate that generates random cryptographic value for every established session. In particular, the node always generates two fresh 128 bit integer *t* and *w* to produce fresh chippertexts *V1* and *V2*, while the coordinator generates two fresh 128 bit integer *x* and *u* to produce fresh chippertexts *V2* and *V3*. Therefore, In the WIP's mobile environment which the parameter and the session are changed very fast (e.g. just in a couple of seconds or minutes), breaking the communication in one day is even not useful. In general, an adversary will not be able to compromise the WIP system by just using the session key that was generated in previous year.

In addition, the mutual session key agreement as explained in equation (3.26) is effective to strengthen the protection. In this regards, an eavesdropper cannot acquire sufficient information to afford brute force guess of the generated session key. Indeed, the node and the coordinator can confuse an adversary since they calculate different cryptographic parameter to generate the same primary session key. In particular, the node calculates *H2*($e(N, V3)^w$), with:

$$e(N, V3)^w = e(N, x(Q + nP))^w = e(P, P)^{wx} \qquad (3.29)$$

While the coordinator calculates *H2*($e(C_{Ord}, V1)^x$), with:

$$e(C_{Ord}, V1)^x = e(C_{Ord}, w(Q + cP))^x = e(P, P)^{wx} \qquad (3.30)$$

In general, an advanced security and privacy protection can be achieved even using the lower options of cryptographic protection. Thus, IMAKA-Tate protocol is designed with various features that can mitigate the potential drawback of the cryptographic Tate pairing over $F_{3^{509x6}}$.

TABLE 3.1. ESTIMATION OF IMAKA-TATE COMPUTATION IN 1000 ITERATIONS

Phase	Main Operations	Time Estimation
Mutual Authentication	1 ηT Pairing	6.426 ms
	1 Exp. $F_{3^{509 x 6}}$	0.169 ms
	2 Multipl. $F_{3^{509 x 6}}$	0.043 ms
	Total	6.639 ms
Primary Session Key	1 ηT Pairing	6.426 ms

3.5. Computation Overhead

In order to ensure that cryptographic processing in IMAKATate is feasible for the system's limited resources of the WIP system, we estimated computation overhead by conducting benchmark test adopted from [181][168]. The benchmark test executed all parameters that are needed to construct 128 bit ηT pairing over $F_{3^{509 x 6}}$. The code of such benchmark test is written in C++ adapted from [168], which was compiled with Visual Studio 2008. The Tate pairing benchmark test was executed in our platform under Windows 7 with 64-bit Intel 2 Cores at 1.8 GHz.

In order to obtain accurate benchmark test result with minimum standard deviation, each main operation of the cryptographic Tate pairing was executed iteratively in multiple times (i.e. 1000 iteration), afterwards the average of computation time was calculated based on the number of iterations. In this regards, by taking large number of samples (e.g. 1000 samples), the benchmark test result is optimally accurate with very low variance. On the other words, the results are very identical to each other, each time the benchmark test is re-executed or reproduced. In order to ensure the accuracy, we executed the 1000 iteration of basic operations in several time (i.e. 10 time executions). In this experiment, we obtain the standard deviation of Pairing computation is only in 0.035 milliseconds. It is even not easy to recognize the variance of other basic operations such as multiplication over $F_{3^{509 x 6}}$. Indeed, such basic operation has extremely tiny variance to each other, which is only in 1.11 microseconds. Thus, by calculating the average of 1000 samples, the variance result is very tiny and will not give any significant impact to overall calculation of mutual authentication and session key agreement of the proposed protocol.

In the ηT pairing benchmark test shown in Table 3.1., we further calculated basic operations of each phase in IMAKA-Tate. The first phase is three-way handshake of mutual authentication, while the second phase is primary session key generation. Table I summarizes computation overhead of IMAKA-Tate calculated by each node and coordinator. On the mutual authentication phase, each participant calculates the same parameters which are two Multiplication over $F_{3^{509\,x\,6}}$ (Multipl. $F_{3^{509\,x\,6}}$), one Exponentiation over $F_{3^{509\,x\,6}}$ (Exp. $F_{3^{509\,x\,6}}$) and one ηT Pairing. After both parties have successfully authenticated to each other, they afterward generate the primary session key by each calculating one more ηT Pairing. In overall, IMAKA-Tate computation time can be interpreted by enumerating both computation time of mutual authentication phase and the primary session key agreement, which were executed in 6.426 ms + 6.639 ms = 13.065 milliseconds. In extraordinary WIP case where the assumption that the node may move very fast from one room to other room just in a couple of seconds, in this case we define that the protocol computation time is acceptable as long as the overall execution time is not more than 0.25 second or 250 milliseconds. Thus, the node and the coordinator will still have feasible spare time to establish a new session for each movement. In general, by executing the cryptographic processing just in about 13 milliseconds, IMAKA-Tate well satisfies the computation requirement even in the aforementioned extraordinary case. Further detail about the IMAKA-Tate performance, particularly the execution time on lower clock frequencies will be discussed in chapter 4.

3.6. Conclusion

IMAKA-Tate offers light-weight identity protection that satisfies the specific requirement for privacy preserving in WIP environment. In this regards, the proposed solution performs encryption of the node/user identity even before the mutual authentication is started. This method prevents the user identity from being revealed by unauthorized party. Therefore, privacy preserving can be achieved well. Furthermore, the security analysis of IMAKA-Tate has demonstrated that the light-weight mutual authentication and verification can mitigate various threats and risks in broader aspects of WIP system, ranging from the physical layer (e.g. relay attacks), network and transport layer attacks (e.g. cloning, impersonation, spoofing, resource consumption attacks, and protocol attacks such as various technic of man-in-the-middle attacks), application layer attacks (e.g. unauthorized tracking, etc.), to multi-layer attacks such as traffic analysis attacks, denial-of-service attacks, and replay attacks. In addition, such security features can also mitigate the insiders who basically have better chance to perform various attacks as well as reveal the other users' privacy. In general, our proposed solution satisfies the requirements in providing protection that covers wider aspects of security and privacy in WIP system.

Chapter 4

Proposed Solution for WIP based on RFID Applications

4.1. Introduction & Motivation

The emerging of sensor integration to RFID system called smart RFID has recently attracted a lot of interest in research and development. It is a prominent technology that is projected to be massively deployed in various applications, ranging from e-Health, transportation, human and device tracking, to distinctive applications like in military system. Indeed, such technology introduces considerable advantages reaching from economical aspects like low cost implementation and maintenance, to technical aspects like reliability and accuracy, as well as its flexibility to be integrated in large-scale system.

Nevertheless, smart RFID system introduces tremendous security and privacy issues derived from the vulnerability nature of Wireless Sensor Network (WSN) applications, as well as various issues elicited from the use of tracking and positioning techniques itself. The following list outlines such issues that must be tackled in smart RFID system.

- The nature of RFID tag which basically can be read without authorization introduces tremendous security risks, particularly various risks from passive and active eavesdropping. This issue makes the RFID system is susceptible from various threats ranging from cloning attack, spoofing or data manipulation, collision attack, to various techniques of Man-in-the-Middle (MITM) attacks like Denial-of-Service (DoS), replay attack, and so on.

- By taking in to account common RFID communication is not mutually authenticated, the RFID system is highly susceptible from various impersonation techniques. This issue makes unauthorized parties can easily perform malicious activities related to privacy threats including unauthorized tracking, spying, or analyzing the information leakage to reveal the user activities.
- Smart RFID tag is basically a device with limited resources in term of CPU, memory, bandwidth/data-rate, and energy/battery storage. Such limitations make the smart RFID tag is highly susceptible to various threats that are also common in WSN. One of them is various techniques of resource consumption attacks. These attacks are conducted by repeatedly sending packet to drain the battery and misspend the bandwidth.
- The constrained nature of RFID system makes the security enforcement is more complicated. On the other hand, common security and privacy solution, such as using Transport Layer Security (TLS/SSL) is not feasible. Indeed, TLS/SSL suffers from various problems reaching from various security threats (e.g. MITM attacks), to communication and computation overheads that would overburden the limited capabilities of smart RFID system.

This chapter studies how our proposed solution called IMAKA-Tate can be implemented to mitigate various threats derived from inherent vulnerabilities in the smart RFID communications. In addition, we also studies how the protocol can be implemented in the system's limited resources with lower clock frequency options.

4.2. Protocol Design

4.2.1. Preliminaries

To tackle the specific challenges in smart RFID system, IMAKA-Tate [21] early establishes encryption even before the authentication is started. In this context, the entire communication data including the RFID tag identity are transported in encrypted payload. Furthermore, to achieve light-weight and feasible communication overhead, we apply ηT pairing that is known as the fastest pairing method [166]. In Principal, the cryptographic processing relies on ternary field $F_{3^{509}}$ defined in [168], specifically using the extension field $F_{3^{509\,x\,6}}$. Such extension field is applied in order to provide advanced-level 128 bit security strength of IBE, which is about same security level as 1024 bit RSA method [170].

In the smart RFID networks, we propose two parties (i.e. RFID reader and RFID tag) perform mutual authentication to each other. Particularly, they communicate over standard IEEE 802.15.4f, which defines standard wireless Physical (PHY) and Media access control (MAC) for active RFID.

Furthermore, the integration of RFID tag to the sensor node has been proposed in many commercial and research works, for instances are proposed by Xiaoyong Su et al. [194] and Liu et al. [193]. In these two example works, the authors proposed the integration of RFID tags with the sensor nodes, where the analog signal of the sensors is converted into digital form by the A/D module and the resulting data is forwarded by readers to the base station. In this thesis, we assume that the sensor node (i.e. imote2) is integrated with RFID tag. In this case, we assume that the RFID tag's processing power joins to the node's CPU, which is used as co-processor for the tag. Thus, each smart RFID tag has sufficient co-processor to perform cryptographic processing, as the tag is integrated in standard sensor platform, such as Imote2 with diverse options of core frequency (i.e. 104, 208, 312 and 416 MHz).

4.2.2. Setup Phase

On the setup phase, the Key Generation Function (KGF) privately distributes all parameters that are needed to construct the IBE method. The KGF is handled by the administrator, who privately preloads all parameters to each legitimate reader and smart RFID tag memory. It is to be noted that all parameters are shared prior to network deployment. In this case, the existence of KGF is no longer needed after the KGF successfully shares all parameters including private keys and all public parameters. This method is to ensure that only legitimate entity can participate in the smart RFID system.

During the setup phase, the KGF initially generates overall parameters that will be confidentially preloaded to each reader and RFID tag's memory. The generated secret parameters include a 128 bit integer master secret key *s*, where $s \in Z_q^*$. Supersingular elliptic curve define over $F_q^*, where\ F_q^* = F_{3^{509}}$. A random point on elliptic curve *P* as part of public parameter, where $P \in E(F_q)$. Additional random point as another part of public parameter *Q*, where $Q \in E(F_q)$ and *Q* = *sP*. Furthermore, the KGF also generates public parameter *g* = *e(P, P)*. In this context, *e* is a function that maps $E(F_{3^{509}})\ x\ E(F_{3^{509}}) \rightarrow F_{3^{509\,x\,6}}$. In addition, two more parameters are defined as hash functions. The first one is *H1*, it is hash function to convert a binary RFID identity to a 128 bit integer, where *H1* : $\{0,1\}^* \rightarrow Z_q^*$. The second one is *H2*, this hash function is to convert a parameter on extension filed $F_{3^{509\,x\,6}}$ to a 128 bit integer, where *H2* : $F_q \rightarrow \{0,1\}^n$.

Instead of distributing the master secret key *s*, the KGF generates all private keys of all RFID devices and then preloads all the keys on the setup phase. This mechanism is conducted in order to simplify key distribution and to achieve feasible computation overhead. In the other word, the readers and RFID tags do not have to generate their own private keys, thus efficient computation effort can be achieved. The private key for each RFID tag generated by KGF is denoted as $T = \frac{1}{s+t}P$, where *s* is master secret key and t = *H1*(RFID tag MAC Address) is a public key of the RFID Tag. The same way to calculate reader private key $R = \frac{1}{s+r}P$, where *r* is public key of the reader calculated as *r* = *H1*(reader MAC Address). In overall the KGF preloads (*Private Key (T or R), e, P, Q, g, H1 and H2*) to each legitimate RFID Tag and RFID Reader's memory.

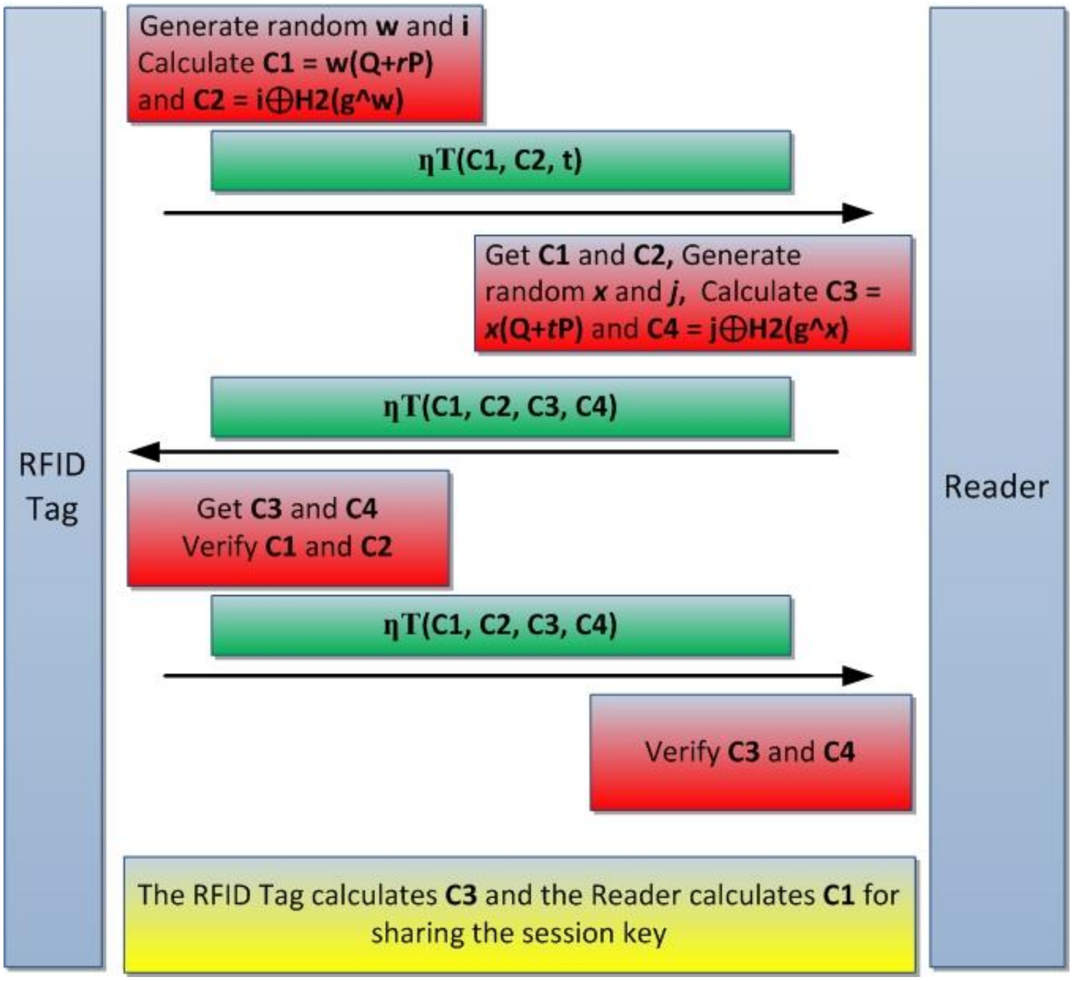


Figure 4.1. Three-way handshake of IMAKA-Tate over RFID system.

4.2.3. Authentication and Key Negotiation Phase

After all public parameters and private key are successfully distributed, the reader and the tag are now ready to carry out mutual authentication and simultaneously negotiate the primary session key. Figure 1 illustrates the mutual authentication and key agreement by performing encrypted three-way handshake negotiation. The authentication procedure is identical with IMAKA-Tate mechanism defined in chapter 3, where the RFID tag initiatively commences the authentication procedure when the existence of RFID reader is detected. This method is conducted to protect a legitimate RFID tag from being read by a rouge reader. In addition, the same procedure like defined in previous chapter, the RFID tag

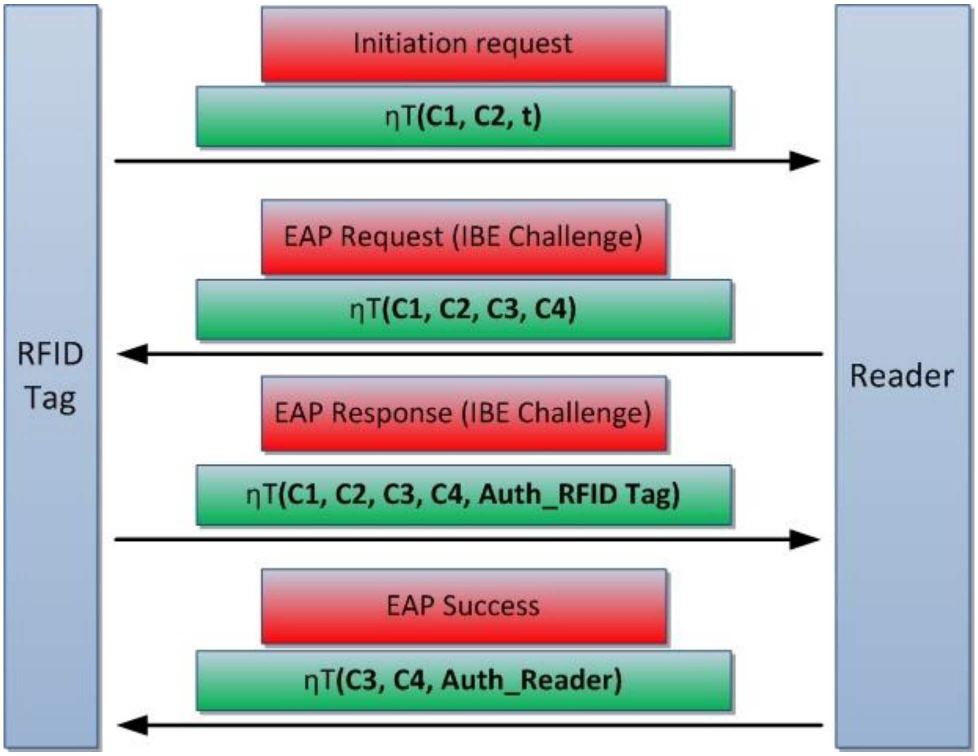


Figure 4.2. EAP IMAKA-Tate over RFID system.

and the reader perform verification procedure to mitigate various threats in multi-layer vulnerabilities. It ranges from the vulnerabilities in network and transport layer such as impersonation, various technics of man-in-the-middle attacks, spoofing, to the vulnerabilities that exploit the inherent problem in several communication layers such as replay attacks.

4.2.4. Mutual Authentication over EAP

In order to achieve efficient and flexible communication that can be used for large-scale RFID system, IMAKA-Tate transports the authentication messages through standard EAP method as described in (RFC 3748) [178]. Figure 4.2 illustrates the IMAKA-Tate over EAP, which is described as follows.

1. Initiation request: Initially, the tag starts the three-way handshake by sending the two encrypted values of C1 and C2 to the reader. The tag also includes its identity (i.e. the tag public key) in the encrypted payloads. In this regards, only the targeted

recipient, which is the legitimate reader can decrypt the message. This mechanism protects the tag identity from being revealed by unauthorized party. It is to be noted that the tag can easily find the reader MAC Address since it is periodically broadcasted by the reader through the beacon frame. Moreover, distinct to common EAP method, IMAKA-Tate over EAP bypass the identity exchange, since it works based on MAC Address.

2. EAP Request IBE Challenge: Upon receiving the initiation request, the reader decrypts the message, sequentially saves the value of C1 for calculating the primary session key. The reader challenges the legitimate tag as described in the three-way handshake, by sending the encrypted values of C3 and C4, as well as sends back the values of C1 and C2 to be further verified by the tag.

3. EAP Response IBE Challenge: Upon receiving the IBE Challenge, the tag decrypts the message and verifies the values of C1 and C2. The tag sends Auth_Tag if the values of C1 and C2 received from the reader are same as the Value s of C1 and C2 created on the initiation request. Otherwise the tag sends authentication failure and the connection is discarded. If the values are verified, the tag then saves the value of C3 created by the reader to further calculate the primary session key.

4. EAP Success: Upon receiving response IBE Challenge, the reader verifies the values of C3 and C4 sent by the tag. The reader send the encrypted EAP success if the values are matched as the values created by the reader on the EAP Request IBE Challenge. Otherwise the reader discards the connection by sending the authentication failure.

Up to this step, both parties have successfully carried out mutual authentication and negotiated the primary session key. In order to ensure the freshness of each established session, all generated random values in this case *t, w, u,* and *x* must be deleted each time the session will be established. In same way, all the random values are also eradicated when mutual authentication is not successfully conducted. Thus, this mechanism prevents various threats on man-in-the-middle attacks, such as performing spoofing and replay attacks.

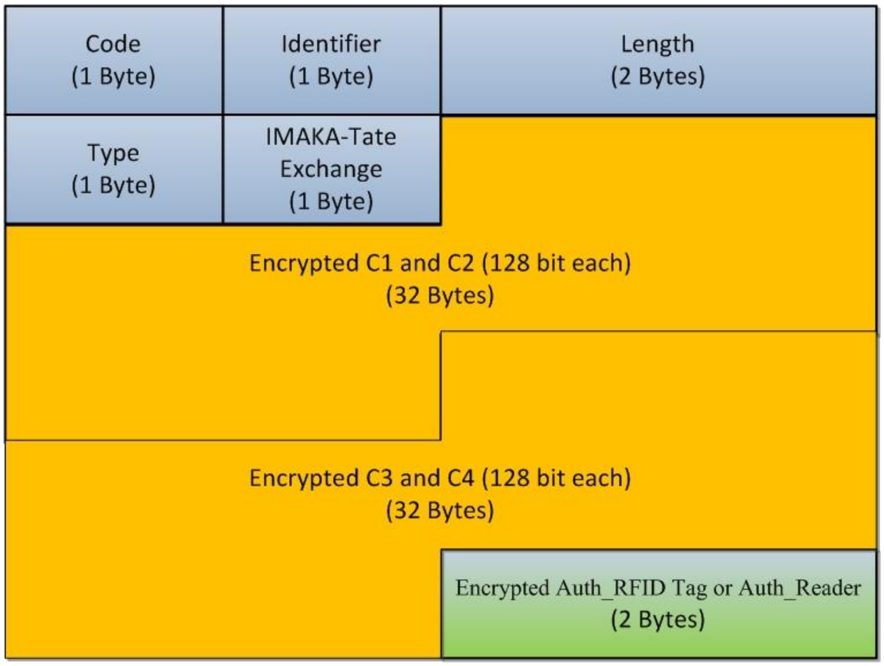


Figure 4.3. EAP IMAKA-Tate packet format.

4.3. EAP IMAKA-Tate Message Format

IMAKA-Tate aims at providing light-weight security protocol that maintains the size of authentication payload as optimally minimum. This feature is to enable efficient communication overhead which mitigates the common problem RFID system (i.e. drainage of battery power). Figure 3 illustrates IMAKA-Tate packet format transported over EAP, including 6 Bytes packet header, 32-64 Bytes encrypted payload, and 2 Bytes Authentication message.

The packet header is structured as standard EAP fields defined in (RFC 3748), including one-octet Code, one-octet Identifier, two-octet Length and one-octet Type. In addition, IMAKA-Tate proposes complement header field called IMAKA-Tate Exchange, is one-octet in length that identifies the encrypted-authentication messages. The values are identified as follows.

- 1 = IBE Challenge-EAP Request/Respond
- 2 = IBE Failure Notification

Furthermore, IMAKA-Tate transports encrypted payload in IBE Request and Respond challenge message. The encrypted payloads are composed as follows.

- The Values of C1, C2, C3, and C4 are each encrypted 16 Bytes that are transported during the IBE Challenge request and respond message.
- Either the Encrypted Auth_Tag or Auth_Reader is 2 Bytes notification from the tag that is attached during the IBE Challenge respond message.

According to IMAKA-Tate packet format depicted in figure 3, the maximum size of authentication packet is 72 Bytes, which is transported during IBE Challenge respond message (see figure 2). Therefore, it is definitely suitable for RFID system that associates to limited resources (i.e. low-date rate, low CPU and battery power).

4.4. Security Analysis

In this section, we analyses the security strength of IMAKA-Tate [13] against various risks in smart RFID system. In addition, we discuss the security features that enable trust and integrity protection in large-scale smart RFID applications.

4.4.1. Attacks from RFID Reader Side

In RFID system, an adversary may impersonate as legitimate reader by creating rogue reader in order to elicit sensitive information. Hence, an adversary can exploit the sensitive information to perform malicious activities and attacks, which are listed as follows.

- Spoofing information: An adversary may exploit the rogue reader to perform fraudulence, such as RFID data manipulation, reporting wrong identification, even it can be exploited to perform various MITM attacks (e.g. replay attack, Dos, etc.).

- Fooling RFID tags: The existence of rogue reader may be used to trick the legitimate RFID tags to reveal their credentials. In this case, the RFID tags are fooled that they are communicating with legitimate reader. Hence, an adversary can use the revealed credentials to impersonate as legitimate tags. In this case the attacker can launch various attacks based on impersonation technique (i.e. cloning attacks, tag emulating, and collision attack).

Nevertheless, an adversary cannot acquire the critical parameters (i.e. *e, P, Q, g, H1* and *H2*) that secretly pre-load before the network deployment. This issue makes the rogue reader calculates wrong session key and will not able to perform mutual authentication on the three-way handshake. Thus, IMAKA-Tate can mitigate the aforementioned threats by preventing the rogue reader to be connected and authenticated in the smart RFID system.

Let us presume that the rogue reader uses different parameters (i.e. *e', P', Q', g', H1'* and *H2'*). In this case, the rogue reader is not able to respond the three-way handshake requested by the tag. Moreover, the rogue reader is not able to find the crucial parameter called master secret key *s*, as it is known only by the KGF. Hence, the rogue reader is not able to correctly generate its private key. Let us presume that the rogue reader uses different master secret key $k \neq$ s. The rogue reader then incorrectly generates its public key $r_{Rog} \neq r$ and private key $R_{Rog} \neq R$:

$$r_{Rog} = H1'(rogue\ reader\ MAC\ address) \qquad (4.1)$$

$$R_{Rog} = \frac{1}{k+r_{Rog}} P' \qquad (4.2)$$

Moreover, the rogue reader cannot correctly calculate the initial session key *i*, since:

$$i \neq H2'(e'(R_{Rog}, C1)) \oplus C2 \qquad (4.3)$$

Since the initial session key *i* is calculated incorrectly, the rogue reader cannot decrypt the initiation message *ηT(C1, C2, t)*. Hence, the rogue reader cannot find the tag MAC Address in order to respond the message. Moreover, the challenge is more complicated for adversary, as it is not possible to convert *t* value to tag MAC address based on the incorrect parameter *H1*', since:

$$t \neq H1'(tag\ MAC\ address) \tag{4.4}$$

An adversary may conduct social engineering to inquiry the tag's MAC Address attached on the user device. However, the adversary in this case the rogue reader is still not able to correctly generate the tag's public key and the two ciphertexts based on the incorrect parameters. This issue makes the tag is not able to calculate the temporary session key *j*. Let us presume that the rogue reader generates $t' \neq t$, $C3' \neq C3$ and $C4' \neq C4$:

$$t' = H1'(tag\ MAC\ address) \tag{4.5}$$

$$C3' = x(Q' + t'P') \tag{4.6}$$

$$C4' = j \oplus H2'(g'^{x}) \tag{4.7}$$

However the tag wrongly calculates the key *j*, since:

$$j \neq H2(e(T, C3')) \oplus C4' \tag{4.8}$$

Hence, the tag aborts the connection as the value of *C1* and *C2* attached on $\eta T(C3', C4', C1, C2,)$ cannot be verified.

Furthermore, both parties are not able to correctly generate and share the primary session key, as the tag calculates:

$$\begin{aligned} e(T, C3')^{w} &= e(T, x(Q' \; + \; t'P'))^{w} \\ &= e\left(\frac{1}{s+t}\ P, x(kP' + t'P')\right)^{w} \\ &= e(P, (kP' + t'P'))^{\frac{wx}{s+t}} \\ &= e(P, P')^{\frac{wx(k+t')}{s+t}} \end{aligned} \tag{4.9}$$

On the other hand the rogue reader calculates:

$$e'(R_{Rog}, C1)^x = e'(R_{Rog}, w(Q\ +\ rP)\ )^x$$

$$= e'\left(\frac{1}{k+r_{Rog}}\ P', w(sP+rP)\right)^x$$

$$= e'(P', (sP+rP))^{\frac{wx}{k+r_{Rog}}}$$

$$= e'(P', P)^{\frac{wx(s+r)}{k+r_{Rog}}} \qquad (4.10)$$

By taking into account an adversary has chance to steal the unsupervised RFID tag. In this case, an adversary can copy all valid parameters (i.e. e, P, Q, g, H1 and H2) that are needed to impersonate as rogue reader. However, the master secret key *s* is owned only by the KGF and it is never shared to any party, neither to the reader nor to the tag. This challenge makes the adversary cannot generate the correct private key for the rogue reader. Let us presume that the rogue reader use incorrect master secret key $k \neq s$. The rogue reader incorrectly generates its private key R_{Rog}:

$$R_{Rog} = \frac{1}{k+r_{Rog}} P \qquad (4.11)$$

Hence the rogue reader is not able to generate correct initial session key *i* as described in equation (1) and (2), since:

$$e\big(R_{Rog}, C1\big) = e(R_{Rog}, w(Q\ +\ rP)$$

$$= e\left(\frac{1}{k+r_{Rog}}\ P, w(sP+rP)\right)$$

$$= e(P, (sP+rP))^{\frac{w}{k+r_{Rog}}}$$

$$= e(P, P)^{\frac{w(s+r)}{k+r_{Rog}}} = g^{\frac{w(s+r)}{k+r_{Rog}}} \qquad (4.12)$$

In this case:

$$i \neq H2(g^{\frac{w(s+r)}{k+r_{Rog}}}) \oplus C2 \tag{4.13}$$

In general, IMAKA-Tate is also suitable to provide security and privacy protection for the smart RFID system. By providing access control, the threats based on the existence of rogue reader can be mitigated. Thus, it prevents an adversary to arbitrary read the RFID tag contents using rogue reader.

4.4.2. Privacy Issue and Attacks from RFID Tag Side

As RFID tag can naturally be read without authorization, this issue introduces tremendous problem related to privacy of RFID user. An adversary can reveal the tag identity and observe sensitive information, in order to perform malicious activates, which are listed as follows.

- An adversary may conduct unauthorized tracking based on the revealed identity. This issue definitely introduces tremendous problem as an adversary may conduct further malicious activates (e.g. espionage, theft, robbery, etc.).
- An adversary may conduct unauthorized tag reading in order to elicit sensitive information that can be used for impersonation activities (e.g. masquerading as legitimate RFID tag). This issue makes an adversary has chance to conduct unwanted activities such as fraudulence.
- An adversary can perform various techniques of resource consumption attacks based on the revealed identity. The adversary can waste the tag bandwidth and drain the battery by insistently sending packets to the revealed identity as destination address.
- An adversary initially reveals the user identity as one of requirements that is needed to successfully perform various attacks (i.e. replay attack, sybil attack, and various attacks based on revealed identity).

Nevertheless, IMAKA-Tate performs the encryption method that includes the tag identity since in the initiation request of mutual authentication. Particularly, the tag firstly hashes its MAC Address to 128 bit integer *n = H1(tag MAC address)*. Subsequently, it is enclosed to the encrypted payload of the initiation request *ηT(C1, C2, n)*. Hence, there is no chance for an adversary to reveal the user identity since it encrypts even before the mutual authentication is started. In addition, the feature on mutual authentication enables an RFID tag to selectively respond the communication request from the reader. In this case, the tag will discard the connection when the existence of rouge reader is detected.

4.4.3. Security Features

The following list outlines the security features offered by IMAKA-Tate [21], which is also match to provide trust and integrity protection in smart RFID environment.

- Mutual Authentication and Key Agreement: IMAKA-Tate establishes mutual authentication that each participant generates random challenge, which is encrypted by the corresponding public key of the recipient. Such mechanism ensures that only targeted recipient can decrypt and correctly answer the challenge. This procedure is conducted in mutual way. In this case, they exchange and verify the ciphertexts of (*C1, C2)* and (*C3, C4)*. This feature can also prevent various MITM attacks (e.g. replay attack, reflection attack, DoS, etc.). Furthermore, both parties simultaneously negotiate the primary session key based on the exchanged challenge. In particular, the reader and the tag calculate the same session key:

$$e(R, C1)^x = e(T, C3)^w = e(P, P)^{wx} \qquad (4.14)$$

- Session robustness: On each established session, both participants freshly generate random 128 bit integer attached in the encrypted message that they exchange to each other. In particular, the tag generate random 128 bit *w* enclosed in chipper text *C1* = $w(Q + rP)$, while the reader generate 128 bit *x* enclosed in $C3 = x(Q + tP)$. Thus, both participants generate the same session key. The reader generates:

$$H2(e(R, w(Q + rP))^{x}) = g^{wx} \tag{4.15}$$

And the tag generates:

$$H2(e(T, x(Q + tP))^{w}) = g^{wx} \tag{4.16}$$

Hence, in case an adversary with very good fortune is able to compromise the past session, he/she somehow will not able to compromise the following session, since the established session is always fresh and will not correspond to any past or even future session.

- Light-weight communication overhead: To achieve efficient battery and bandwidth consumptions, IMAKA-Tate maintains the communication overhead as minimum as possible. According to IMAKA-Tate packet format depicted in figure 3, the maximum size of authentication packet is only 72 Bytes, which is transported in EAP respond-IBE Challenge (see figure 4.2). Therefore, it is suitable for RFID system's limited resources with low-date rate, limited CPU and battery.

- Light-weight cryptographic operation with high-level security strength: IMAKA-Tate uses 128 bit security strength of ηT paring. This method is known as the most light-weight cryptographic operation, even it is feasible for the most constrained sensor node [4]. In addition, such security strength is about same as the 1024 bit of RSA method. Thus, it is adequate to protect the RFID system against various techniques of brute-force attacks.

4.4.4. Special Issue on Network and Transport Layer in RFID systems

We already proved on the chapter 3 that IMAKA-Tate can mitigate the security and privacy threats in multi-aspect vulnerabilities, ranging from the attacks raised from the vulnerabilities in physical layer such as relay attacks, vulnerabilities in network and transport layer including resources consumption attacks and various technics of man-in-the-middle attacks, to various threats raised from multi-layer problem including replay attacks and traffic analysis attacks. In this section, we analyze additional security problem raised from inherent network and transport layer vulnerabilities on specific RFID case, including cloning attacks, network protocol attacks (e.g. spoofing), impersonation, and eavesdropping.

Common RFID chip manufacturers claim that they can produce a unique identity to each RFID tag as well as affirm that the identity is not replicable. Nevertheless, in real case an adversary can easily clone the identity to writable or reprogrammable device. In the worst case, an adversary even may conduct the same technic in order to impersonate as legitimate peer (i.e. RFID reader). Thus, all RFID tag within the particular range will reveal their sensitive information, since they are fooled to think that they communicate to authorized reader. This issue makes RFID system is susceptible from various technics of cloning and impersonation.

Similar with cloning attacks, spoofing attacks aims at impersonating as a legitimate client in order to get privilege and full access to the valid communication channel. However, different with cloning, spoofing does not require physically clone of the node or RFID tag. Instead, such attacks require the knowledge of communication protocol as well as the sensitive properties including the cryptographic material that are used to secure the communications. In general, to launch all attacks in network and transport layer, it requires to initially record the sensitive information through eavesdropping techniques.

To cope with the aforementioned threats, IMAKA-Tate enables encryption method with mutual authentication and verification, as well as identity protection. These methods can combat various threats on network and transport layer vulnerabilities by preventing an authorized party to eavesdrop the communication.

Similar like in the case for WIP based on WLAN/WPAN defined in chapter 3, the tag's MAC address is firstly hashed in to 128 bit integer and then it is used to calculate the chippertext C3. Furthermore, the chipertext is transported in the encrypted payload of the established session *j*, which can be recovered using the private key of the tag *T*.

$$t = H1(tag\ MAC\ address) \tag{3.17}$$

$$C3 = x(Q + tP) \tag{3.18}$$

$$j = H2(e(T, C3)) \oplus C4 \tag{3.19}$$

Therefore, an adversary will not be able to find the sensitive information including the tag identity and the entire content of the messages transported in the encrypted payload. In general, various threats such as cloning, spoofing and impersonation can be prevented by protecting the identity and the communication contents.

Furthermore, both RFID tag and the reader perform mutual authentication and verification methods that strengthen the security and privacy protection. In this regards, a RFID tag encrypts the communication contents including the identity using the reader public key, while the reader encrypts the communication contents using public key of the tag. Thus, only the corresponding private key of the particular recipient (i.e. RFID tag or reader) can correctly recover the encrypted messages and generated session. In this case, the reader authenticates the tag using its private key *R*:

$$i = H2(e(R, C1)) \oplus C2 \tag{3.20}$$

The tag authenticates the coordinator using its private key *T*:

$$j = H2(e(T, C3)) \oplus C4 \tag{3.21}$$

Moreover, similar like in IMAKA-Tate procedure the RFID tag and the reader perform challenge-respond verification to ensure the integrity of the message as well as prevent the message from being altered or modified by unauthorized party. In particular, the RFID tag verifies the chippertexts of *C1* and *C2*, and the reader verifies the chippertexts of *C3* and *C4*. Thus, the connection is discarded in case the chippertext values are not matched according to the verification rule defined in chapter 3.

In general, the security and privacy method prevent an authorized party to play with man-in-the-middle, in order to perform various attacks in the network and transport layer including eavesdropping, impersonation, spoofing, and cloning attacks.

4.5. Computation Analysis

In order to ensure that cryptographic processing in IMAKA-Tate is feasible for smart RFID system, we estimated computation overhead by conducting benchmark tests adopted from [181]. The benchmark tests estimated the computation overhead of all parameters that are needed to construct 128 bit ηT pairing over $F_{3^{509 x 6}}$. The code of such benchmark test is written in C++ adapted from [168], which was compiled with Visual Studio 2008. The benchmark test was executed in our platform under Windows 7 with 64-bit Intel 2 Cores at 1.8 GHz. In order to emulate the smart RFID system, we forced the processor to run in single core and scaling down the clock frequency according to three options of Imote2 platform (i.e. 104 MHz, 208 MHz and 416 MHz). In addition, to achieve accurate estimation the benchmark test executed the cryptographic operations in multiple times (i.e. 1000 iterations).

We further calculated basic operations of each phase in IMAKA-Tate. The first phase is three-way handshake of mutual authentication, while the second phase is primary session key generation. Table I summarizes computation overhead of IMAKA-Tate calculated by each smart RFID tag. On the mutual authentication phase, each participant calculates the same parameters which are two Multiplication over $F_{3^{509 x 6}}$, one Exponentiation over $F_{3^{509 x 6}}$ and one ηT Pairing. After both parties have successfully authenticated to each other, they afterward generate the primary session key by each calculating one more ηT Pairing. It is to be noted that we only show the computation result of RFID tag, as we assume that the reader has stronger processor clock to process the cryptographic operation.

TABLE 4.1. ESTIMATION OF RFID TAG COMPUTATION IN 1000 ITERATIONS

Phase	Processor	Time Estimation
Mutual Authentication	104 MHz	57.32 ms
	208 MHz	35.93 ms
	416 MHz	23.57 ms
Generating Primary Session Key	104 MHz	54.54 ms
	208 MHz	34.34 ms
	416 MHz	22.79 ms

According to the benchmark test implied in Table I, the RFID tag at 416 MHz calculated both phases which are mutual authentication and generating primary session key in 46.36 milliseconds. On the other hand, the RFID tag at 104 MHz calculated both phases in 111.86 milliseconds. It is therefore concluded, IMAKA-Tate method is remarkably feasible to be applied in smart RFID system since the computation time is still much more lower than the baseline of extraordinary case definition defined in chapter 3 (i.e. 250 ms). In addition, the computation time is even affordable for the smart RFID tag with lower co-processor frequency option at 104 MHz.

4.6. Conclusion

IMAKA-Tate offers light-weight identity protection and mutual authentication that satisfies the specific requirement for security and privacy in smart RFID system. In this regards, the proposed solution performs encryption of the smart RFID tag identity even before the mutual authentication is started. This method prevents the tag identity from being revealed by unauthorized party. Therefore, privacy preserving can be achieved well. Furthermore, the security analysis of IMAKA-Tate has demonstrated that it can mitigate various security threats and risks in the smart RFID system, including unauthorized tracking and tag reading, cloning attack, impersonation, and resource consumption attack. In addition, the proposed solution can mitigate same security threats in WIP system that can also be launched in RFID system. Moreover, we demonstrated in the computation analysis that IMAKA-Tate is affordable to be applied in the constrained nature of smart RFID system.

Chapter 5

The Protocol Refinement for RFID-based Applications

5.1. Introduction & Motivation

Take into account that some of smart RFID applications are deployed in well trusted environment where physical security and the surveillance of employed personal security guards are well facilitated, the risk on key escrow and the existence of suspicious adversary are significantly smaller. In this situation, the clients (e.g. RFID tag) will be more concern about the performance rather than expecting more in the security protection.

In this chapter, we improve the security and privacy protection in term of computation performance, which is more suitable for the specific smart RFID application that has more concern about the system's limited resources and its performance. In this regards, we introduce RFID-Tate, which improves the performance of IMAKA-Tate without significantly decrease the security protection. In particular, we eliminate a feature called session key agreement affecting the number of some basic cryptographic operations (i.e. one pairing function) is eliminated. Thus, it is significantly improve the computation performance since the pairing function is the most time and energy consuming in the construction of pairing based authentication method.

5.2. Protocol Design

5.2.1. Preliminaries

To tackle the specific challenges in active RFID system, RFID-Tate early establishes encryption even before the authentication is started. In this context, the entire communication data including the RFID tag identity are transported in encrypted payload. Furthermore, to achieve light-weight and feasible communication overhead, we apply ηT pairing that is known as the fastest pairing method [166]. In Principal, the cryptographic processing relies on ternary field $F_{3^{509}}$ defined in [168], specifically using the extension field $F_{3^{509x6}}$. Such extension field is applied in order to provide advanced-level 128 bit security strength of IBE, which is about same security level as 1024 bit RSA method [170].

In the active RFID networks, we propose two parties (i.e. RFID reader and RFID tag) perform mutual authentication to each other. Particularly, they communicate over standard IEEE 802.15.4f, which defines standard wireless Physical (PHY) and Media access control (MAC) for active RFID. In addition, we assume that each active RFID tag has sufficient co-processor to perform light-weight cryptographic processing. For example, it is integrated to standard platform Imote2 with diverse options of core frequency (i.e. 104, 208, 312 and 416 MHz).

5.2.2. Setup Phase

On the setup phase, the Key Generation Function (KGF) privately distributes all parameters that are needed to construct the IBE method. The KGF is handled by the administrator, who privately preloads all parameters to each legitimate reader and active RFID tag memory. It is to be noted that all parameters are shared prior to network deployment. In this case, the existence of KGF is no longer needed after the KGF successfully shares all parameters including private keys and all public parameters. This method is to ensure that only legitimate entity can participate in the active RFID system.

During the setup phase, the KGF initially generates overall parameters that will be confidentially preloaded to each reader and RFID tag's memory. The generated secret parameters include a 128 bit integer master secret key s, where $s \in Z_q^*$. Supersingular elliptic curve define over $F_q^*, where\ F_q^* = F_{3^{509}}$. A random point on elliptic curve *P* as part of public parameter, where $P \in E(F_q)$. Additional random point as another part of public parameter *Q*, where $Q \in E(F_q)$ and *Q* = *sP*. Furthermore, the KGF also generates public parameter g = *e(P, P)*. In this context, *e* is a function that maps $E(F_{3^{509}})\ x\ E(F_{3^{509}}) \rightarrow F_{3^{509\, x\, 6}}$. In addition, two more parameters are defined as hash functions. The first one is *H1*, it is hash function to convert a binary RFID identity to a 128 bit integer, where *H1* : $\{0, 1\}^* \rightarrow Z_q^*$. The second one is *H2*, this hash function is to convert a parameter on extension filed $F_{3^{509\, x\, 6}}$ to a 128 bit integer, where *H2* : $F_q \rightarrow \{0, 1\}^n$.

Instead of distributing the master secret key *s*, the KGF generates all private keys of all RFID devices and then preloads all the keys on the setup phase. This mechanism is conducted in order to simplify key distribution and to achieve feasible computation overhead. In the other word, the readers and RFID tags do not have to generate their own private keys, thus efficient computation effort can be achieved. The private key for each RFID tag generated by KGF is denoted as $T = \frac{1}{s+t}P$, where *s* is master secret key and t = *H1*(RFID tag MAC Address) is a public key of the RFID Tag. The same way to calculate reader private key $R = \frac{1}{s+r}P$, where *r* is public key of the reader calculated as *r* = *H1*(reader MAC Address). In overall the KGF preloads (*Private Key (T or R), e, P, Q, g, H1 and H2*) to each legitimate RFID Tag and Reader's memory.

5.2.3. Authentication and Key Negotiation Phase

After all public parameters and private key are successfully distributed, both parties are now ready to carry out mutual authentication. Figure 1 illustrates the mutual authentication and key agreement by performing encrypted three-way handshake negotiation. The following list describes the three-way handshake procedure.

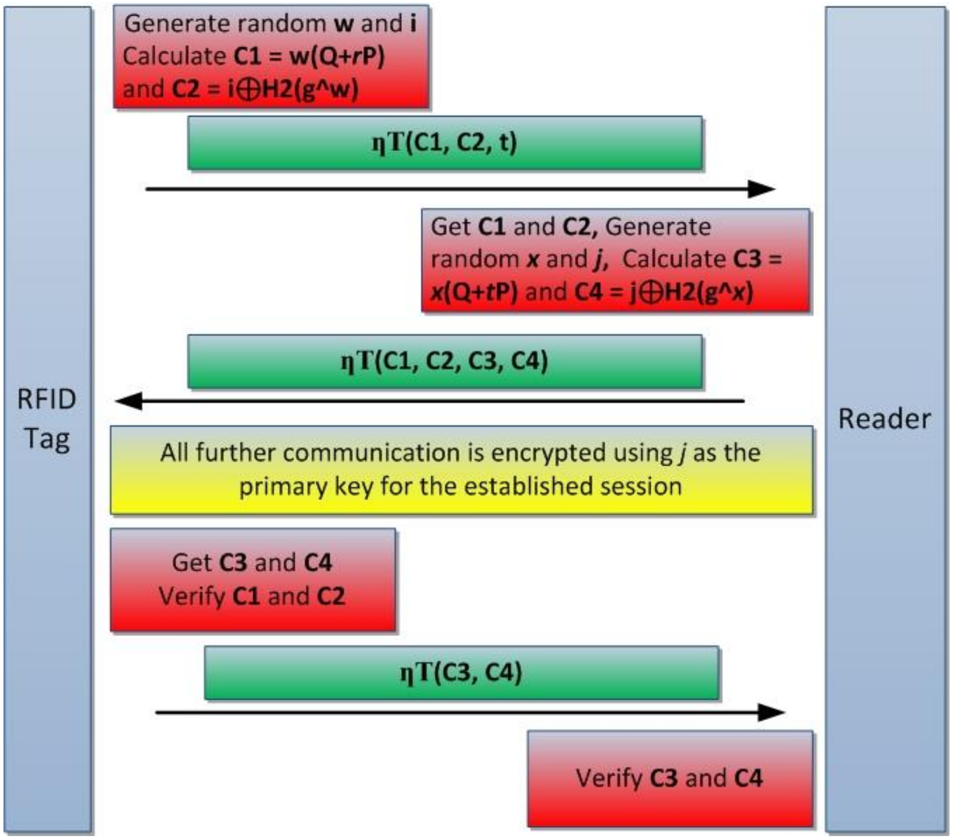

RFID Tag
Generate random **w** and **i** Calculate **C1 = w(Q+*r*P)** and **C2 = i⊕H2(g^w)**
ηT(C1, C2, t)
Get **C1** and **C2,** Generate random ***x*** and ***j***, Calculate **C3 = *x*(Q+*t*P)** and **C4 = j⊕H2(g^x)**
ηT(C1, C2, C3, C4)
All further communication is encrypted using *j* as the primary key for the established session
Get **C3** and **C4** Verify **C1** and **C2**
ηT(C3, C4)
Verify **C3** and **C4**
Reader

Figure 5.1. RFID-Tate Mutual Authentication Scheme.

1. We presume that the RFID tag initially sleeps and wakes up after receiving beacon frame broadcasted by the RFID reader. Hereafter, the tag calculates the reader public key as *r = H1(reader MAC address)*. Subsequently, the tag randomly generates two 128 bit integer *i* and *w*, where *i* is temporary session key.

2. The tag then generates two ciphertexts $C1 = w(Q + rP)$ and $C2 = i \oplus H2(g^{w})$. The tag subsequently requests to join in the RFID system by sending the two ciphertexts to the reader. The tag also includes its MAC address *t = H1(tag MAC address)* in the encrypted payload, in order to protect its identity from being revealed by unauthorized party. In this case, all contents in the message including the session key *i* and the tag MAC address are encrypted using the reader public key. Thus, only the reader can decrypt the message.

3. The reader receives and decrypts the messages using its private key *R*. The reader can recover the session key *i* by calculating *i = H2(e(R, C1))* $\oplus$ *C2*. In order to achieve efficient communication, the reader tentatively saves the key *i* and the value of *C1* for further steps. Each message created by the tag in the three-way handshake will use the initial session key *i* and the value of *C1* will be used to calculate primary session key.

The temporary session key is shared based on the pairing function calculated as follows.

$$i = H2(g^{w}) \oplus C2 \qquad (5.1)$$

since

$$\begin{aligned} e(R, C1) &= e\left(\frac{1}{s+r} P, w(Q + rP)\right) \\ &= e(P, Q + rP)^{\frac{w}{s+r}} \\ &= e(P, (s + r)P)^{\frac{w}{s+r}} \\ &= e(P, P)^{w} = g^{w} \qquad (5.2) \end{aligned}$$

4. In the second message of the three-way handshake, the reader generate *x* and *j* as two random 128 bit integers, where *j* is primary session key that is used to encrypt all further communication in the established session. The reader afterward generates and send two ciphertexts *C3 = x(Q + tP)* and *C4 = j* $\oplus$ *H2*(g^{x}). The reader also includes the values of *C1* and *C2* in the encrypted message to be further verified by the tag.

5. The tag then receives and decrypts the message which contains temporary session key *j* using its private key *T*. It is conducted by calculating *j = H2(e(T, C3))* $\oplus$ *C4*. The tag further verifies the value of *C1* and *C2*. The further step is then continued only if the two values are same as the two values of *C1* and *C2* generated by the tag on the first message. Otherwise, the tag aborts the authentication.

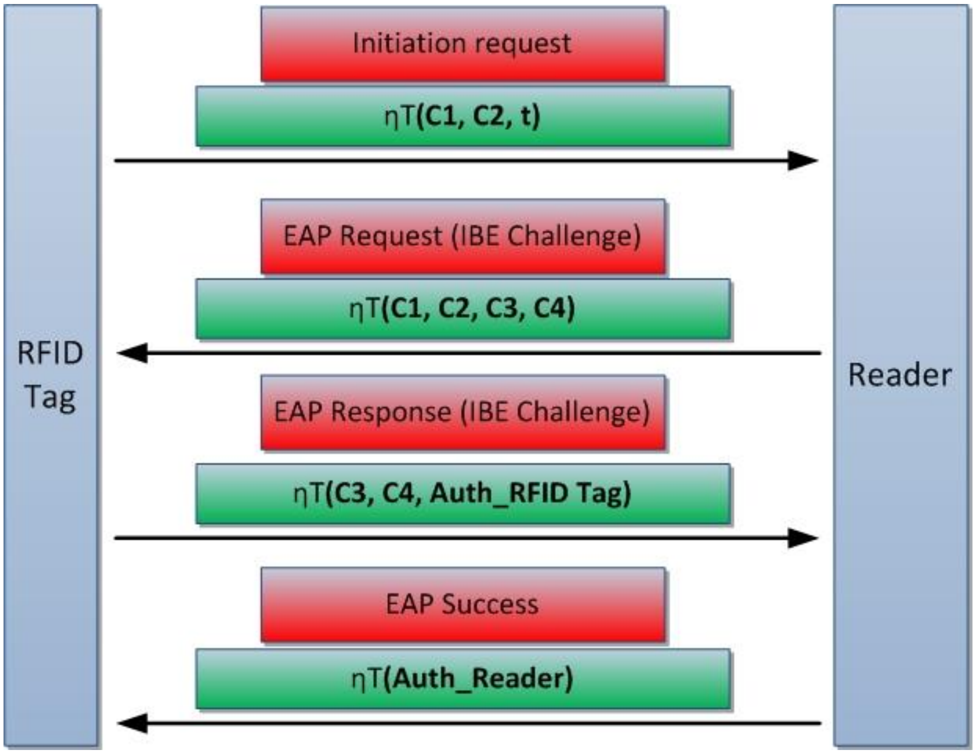


Figure 5.2. RFID-Tate over EAP.

6. The tag then sends back the value of *C3* and *C4* to be verified by the reader in the encrypted-payload. The further communication is continued if the received values are equal as the values generated by the reader on the second message. Otherwise, the reader sends failure notification to abort the connection.

Up to this step, both parties have mutually authenticated to each other. The reader and the tag generate fresh random values of *x* and *w* for every new session. Hence, such method enables the session robustness, which differentiates the established session from the past or even the future session.

5.2.4. Mutual Authentication over EAP

In order to achieve efficient and flexible communication that can be used for large-scale RFID system, RFID-Tate transports the authentication messages through standard EAP method as described in (RFC 3748) [12]. As illustrated in Figure 5.2, all authentication messages are transported in encrypted payload. Thus, it prevents adversary to reveal the credentials in order to perform malicious activities such as various techniques of MITM attacks (e.g. replay attack, relay attack, reflection attack, etc.). Furthermore, RFID-Tate simplifies the authentication by eliminating the identity exchange. This mechanism is different like in common EAP method, as it specifically works based on MAC Address.

5.3. Computation analysis

In this section we analyzed the computation overhead of RFID-Tate, as well as compared it with our previous solution in IMAKA-Tate. In this regards, we conducted benchmark test of IBE ηT pairing computation adopted from [1][3]. The benchmark test execute all parameters that are needed to construct 128 bit ηT pairing over $F_{3^{509\,x\,6}}$. In addition to our work, we further calculated and compared basic operations to perform mutual authentication and key agreement both for RFID-Tate and IMAKA-Tate. The benchmark test was executed in our platform under Windows 7 with 64-bit Intel 2 Cores at 1.8 GHz. In order to emulate the active RFID system, we forced the processor to run in single core and scaling down the clock frequency according to three options of standard Imote2 platform including 104 MHz, 208 MHz and 416 MHz. In addition, to achieve accurate estimation the benchmark test executed the cryptographic operations in 1000 iterations.

Table I shows computation overhead of IMAKA-Tate calculated by each tag at 416 MHz. On the mutual authentication phase, each participant calculates the same parameters which are two Multiplication over $F_{3^{509\,x\,6}}$ (Multipl. $F_{3^{509\,x\,6}}$), one Exponentiation over $F_{3^{509\,x\,6}}$ (Exp. $F_{3^{509\,x\,6}}$) and one ηT Pairing. After both parties have successfully authenticated to each other, they afterward generate the primary session key by each calculating one more ηT Pairing.

Table II shows computation overhead of RFID-Tate calculated by each tag at 416 MHz. On the mutual authentication phase, each RFID tag and reader calculate the same parameters which are two Multipl. $F_{3^{509\,x\,6}}$, one Exp. $F_{3^{509\,x\,6}}$ and one ηT Pairing. Instead of generating new session key, the session key j generated by the reader on the three-way handshake is

TABLE 5.1. ESTIMATION OF IMAKA-TATE COMPUTATION AT 416 MHZ

Phase	**Main Operations**	**Time Estimation**
Mutual Authentication	1 ηT Pairing	*22.79 ms*
	1 Exp. $F_{3^{509 \, x \, 6}}$	*0.577 ms*
	2 Multipl. $F_{3^{509 \, x \, 6}}$	*0.181 ms*
Primary Session Key	1 ηT Pairing	*22.79 ms*
	Total	***46.33 ms***

TABLE 5.2. ESTIMATION OF RFID-TATE COMPUTATION AT 416 MHZ

Phase	**Main Operations**	**Time Estimation**
Mutual Authentication & Generating Primary Session Key	1 ηT Pairing	*22.79 ms*
	1 Exp. $F_{3^{509 \, x \, 6}}$	*0.577 ms*
	2 Multipl. $F_{3^{509 \, x \, 6}}$	*0.181 ms*
	Total	***23.54 ms***

TABLE 5.3. SUMMARY OF IMAKA-TATE COMPUTATION (104, 208, 416 MHZ)

Phase	**Processor**	**Time Estimation**
Mutual Authentication & Generating Primary Session Key	104 MHz	*111.86 ms*
	208 MHz	*70.27 ms*
	416 MHz	*46.33 ms*

TABLE 5.4. SUMMARY OF RFID-TATE COMPUTATION (104, 208, 416 MHZ)

Phase	**Processor**	**Time Estimation**
Mutual Authentication & Generating Primary Session Key	104 MHz	57.32 *ms*
	208 MHz	35.93 *ms*
	416 MHz	23.54 *ms*

used as the primary session key. This mechanism enables efficient computation, as both RFID tag and reader do not have to calculate one more ηT pairing in order to generate the session key. In other words, each participant only need to calculate one paring to perform mutual authentication and session key generation.

Table III and Table IV summarize the computation performance of mutual authentication and session key generation both for IMAKA-Tate and RFID-Tate in the three processor options. In general the computation performance of IMAKA-Tate is quite feasible for RFID tag, particularly for the processor option at 416 MHz, which computes mutual authentication and session key agreement in 46 milliseconds. IMAKA-Tate method is also affordable for the processor option at 104 MHz, which perform the computation in 111 milliseconds. Based on the example of extraordinary case explained in chapter 3, which define the baseline is 250 ms, it is concluded that IMAKA-Tate is remarkably very efficient protocol. Nevertheless, IMAKA-Tate performance is not optimally efficient and might not be suitable for very low cost RFID tag which associates to very constrained resources including low CPU, memory and battery power.

According to comparison of benchmark tests implied in Table III and Table IV, we improve the RFID-Tate performance, which is about two times faster than IMAKA-Tate performance. RFID tag with co-processor at 416 MHz computed the mutual authentication and session key generation in about 23 milliseconds, while RFID tag with co-processor at 104 MHz computed the cryptographic processing in 57 milliseconds. Indeed, both the RFID tag and reader only need to calculate one pairing for each established session. Hence, the computation overhead is maintained as optimally minimum. In graph visualization, figure 5.2. shows the significant improvement of RFID-Tate protocol, particularly for the lower option of clock frequency (i.e. 104 MHz). Indeed, the graph shows in each clock frequency options that the performance of RFID-Tate is almost two times faster than the performance of IMAKA-Tate. Therefore, it is concluded that the RFID-Tate is more suitable to the RFID system that has more concern in computation performance.

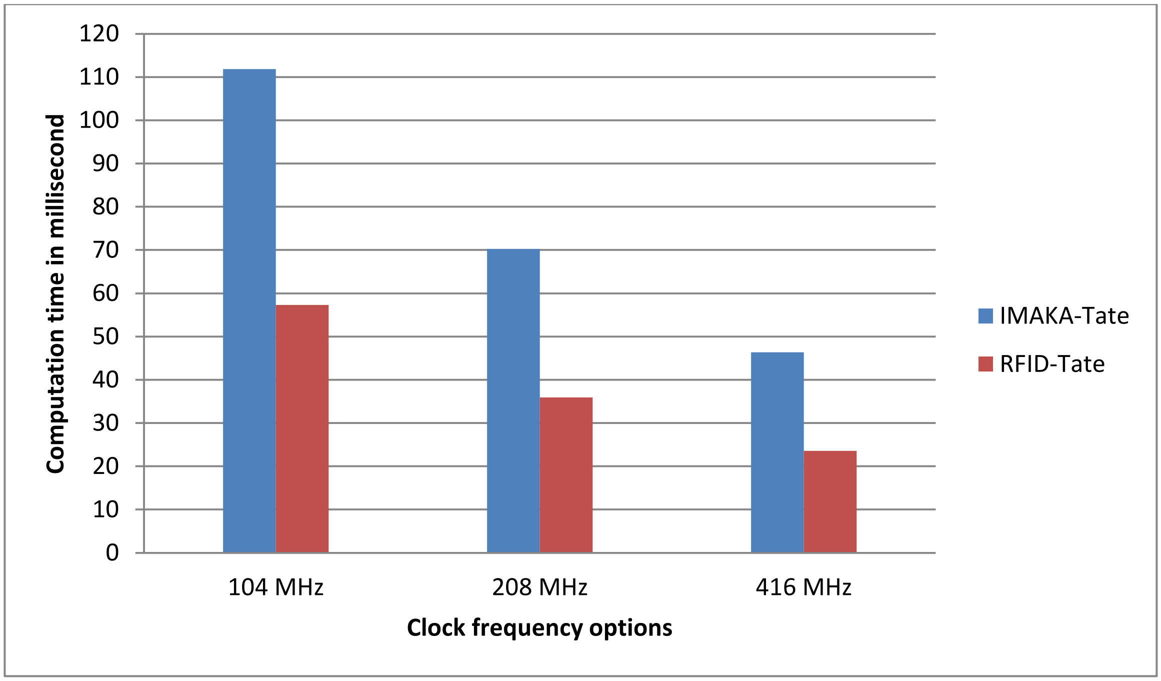


Figure 5.3. Comparison of IMAKA-Tate and RFID-Tate performance.

5.4. Security Analysis

In this section, we analyses the security strength of RFID-Tate against various risks in active RFID system. In addition, we discuss the security features that enable trust and integrity protection in large-scale active RFID applications.

5.4.1. Attacks from RFID Reader Side

In RFID system [14], an adversary may impersonate as legitimate reader by creating rogue reader in order to elicit sensitive information. Hence, an adversary can exploit the sensitive information to perform malicious activities and attacks, which are listed as follows.

- Spoofing information: An adversary may exploit the rogue reader to perform fraudulence, such as RFID data manipulation, reporting wrong identification, even it can be exploited to perform various MITM attacks (e.g. replay attack, Dos, etc.).

- Fooling RFID tags: The existence of rogue reader may be used to trick the legitimate RFID tags to reveal their credentials. In this case, the RFID tags are fooled that they are communicating with legitimate reader. Hence, an adversary can use the revealed credentials to impersonate as legitimate tags. In this case the attacker can launch various attacks based on impersonation technique (i.e. cloning attacks, tag emulating, and collision attack).

Nevertheless, an adversary cannot acquire the critical parameters (i.e. *e, P, Q, g, H1* and *H2*) that secretly pre-load before the network deployment. This issue makes the rogue reader calculates wrong session key and will not able to perform mutual authentication on the three-way handshake. Thus, RFID-Tate can mitigate the aforementioned threats by preventing the rogue reader to be connected and authenticated in the active RFID system.

Let us presume that the rogue reader uses different parameters (i.e. *e', P', Q', g', H1'* and *H2'*). In this case, the rogue reader is not able to respond the three-way handshake requested by the tag. Moreover, the rogue reader is not able to find the crucial parameter called master secret key *s*, as it is known only by the KGF. Hence, the rogue reader is not able to correctly generate its private key. Let us presume that the rogue reader uses different master secret key $k \neq$ s. The rogue reader then incorrectly generates its public key $r_{Rog} \neq r$ and private key $R_{Rog} \neq R$:

$$r_{Rog} = H1'(\textit{rogue reader MAC address}) \quad (5.3)$$

$$R_{Rog} = \frac{1}{k+r_{Rog}} P' \quad (5.4)$$

Moreover, the rogue reader cannot correctly calculate the initial session key *i*, since:

$$i \neq H2'(e'(R_{Rog}, C1)) \oplus C2 \quad (5.5)$$

Since the initial session key *i* is calculated incorrectly, the rogue reader cannot decrypt the initiation message $\eta T(C1, C2, t)$. Hence, the rogue reader cannot find the tag MAC Address in order to respond the message. Moreover, the challenge is more complicated for adversary, as it is not possible to convert *t* value to tag MAC address based on the incorrect parameter *H1*', since:

$$t \neq H1'(\text{tag MAC address}) \qquad (5.6)$$

An adversary may conduct social engineering to inquiry the tag's MAC Address attached on the user device. However, the adversary in this case the rogue reader is still not able to correctly generate the tag's public key and the two ciphertexts based on the incorrect parameters. This issue makes the tag is not able to calculate the temporary session key *j*. Let us presume that the rogue reader generates $t' \neq t$, $C3' \neq C3$ and $C4' \neq C4$:

$$t' = H1'(\text{tag MAC address}) \qquad (5.7)$$

$$C3' = x(Q' + t'P') \qquad (5.8)$$

$$C4' = j \oplus H2'(g'^{x}) \qquad (5.9)$$

However the tag wrongly calculates the key *j*, since:

$$j \neq H2(e(T, C3')) \oplus C4' \qquad (5.10)$$

Hence, the tag aborts the connection as the value of *C1* and *C2* attached on *ηT(C3', C4', C1, C2,)* cannot be verified.

By taking into account an adversary has chance to steal the unsupervised RFID tag. In this case, an adversary can copy all valid parameters (i.e. e, P, Q, g, H1 and H2) that are needed to impersonate as rogue reader. However, the master secret key *s* is owned only by the KGF and it is never shared to any party, neither to the reader nor to the tag. This challenge makes the adversary cannot generate the correct private key for the rogue reader. Let us presume that the rogue reader use incorrect master secret key $k \neq s$. The rogue reader incorrectly generates its private key R_{Rog}:

$$R_{Rog} = \frac{1}{k+r_{Rog}} P \qquad (5.11)$$

Hence the rogue reader is not able to generate correct initial session key i as described in equation (1) and (2), since:

$$e\left(R_{Rog}, C1\right) = e(R_{Rog}, w(Q\ +\ rP)$$

$$= e\left(\frac{1}{k+r_{Rog}}\ P, w(sP + rP)\right)$$

$$= e(P, (sP + rP))^{\frac{w}{k+r_{Rog}}}$$

$$= e(P, P)^{\frac{w(s+r)}{k+r_{Rog}}} = g^{\frac{w(s+r)}{k+r_{Rog}}} \qquad (5.12)$$

In this case:

$$i \neq H2(g^{\frac{w(s+r)}{k+r_{Rog}}}) \oplus C2 \qquad (5.13)$$

The same features like in IMAKA-Tate, the RFID-Tate also provide access control by establishing mutual authentication and two-way verification. Thus, the proposed protocol can also prevent various threats based on the existence of rogue reader that may arbitrary read the RFID tag's contents.

5.4.2. Privacy Protection and Attacks from RFID Tag Side

As RFID tag can naturally be read without authorization, this issue introduces tremendous problem related to privacy of RFID user. An adversary can reveal the tag identity and observe sensitive information, in order to perform malicious activates, which are listed as follows [22].

- An adversary may conduct unauthorized tracking based on the revealed identity. This issue definitely introduces tremendous problem as an adversary may conduct further malicious activates (e.g. espionage, theft, robbery, etc.).
- An adversary may conduct unauthorized tag reading in order to elicit sensitive information that can be used for impersonation activities (e.g. masquerading as

legitimate RFID tag). This issue makes an adversary has chance to conduct unwanted activities such as fraudulence.

- An adversary can perform various techniques of resource consumption attacks based on the revealed identity. The adversary can waste the tag bandwidth and drain the battery by insistently sending packets to the revealed identity as destination address.
- An adversary initially reveals the user identity as one of requirements that is needed to successfully perform various attacks (i.e. replay attack, sybil attack, and various attacks based on revealed identity).

Nevertheless, RFID-Tate performs the encryption method that includes the tag identity since in the initiation request of mutual authentication. Particularly, the tag firstly hashes its MAC Address to 128 bit integer *n = H1(tag MAC address)*. Subsequently, it is enclosed to the encrypted payload of the initiation request *ηT(C1, C2, n)*. Hence, there is no chance for an adversary to reveal the user identity since it encrypts even before the mutual authentication is started.

5.4.3. Security Features

The following list outlines the security features [14] offered by IMAKA-Tate that are also valid for the case of RFID-Tate, which aims at providing trust and integrity protection.

- Mutual Authentication and Key Agreement: RFID-Tate establishes mutual authentication that each participant generates random challenge, which is encrypted by the corresponding public key of the recipient. Such mechanism ensures that only targeted recipient can decrypt and correctly answer the challenge. This procedure is conducted in mutual way. In this case, they exchange and verify the ciphertexts of (*C1, C2)* and (*C3, C4)*. This feature can also prevent various MITM attacks (e.g. replay attack, reflection attack, DoS, etc.).

- Session robustness: On each established session, both participants freshly generate random 128 bit integer attached in the encrypted message that they exchange to each other. In particular, the tag generate random 128 bit w and i enclosed in chipper text $C1 = w(Q + rP)$ and $C2 = i \oplus H2(g^{w})$, while the reader generate 128 bit x and j enclosed in $C3 = x(Q + tP)$ and $C4 = j \oplus H2(g^{x})$. Hence, in case an adversary with very good fortune is able to compromise the past session, he/she somehow will not able to compromise the following session, since the established session is always fresh and will not correspond to any past or even future session.

- Light-weight cryptographic operation with sufficient-level security strength: RFID-Tate uses 128 bit security strength of ηT paring. This method is known as the most light-weight cryptographic operation, even it is feasible for the most constrained sensor node [169]. In addition, such security strength is about same as the 1024 bit of RSA method. Thus, it is adequate to protect the RFID system against various techniques of brute-force attacks.

5.4.4. Special Issue on Application Layer related to Privacy Threats

Providing a tracking service without implication on privacy issue is one of the biggest challenges in RFID applications. There are a lot of things that can be exploited by an adversary in order to reveal the users privacy. Take into consideration that the communication in RFID system is commonly not equipped with sufficient authentication and encryption methods, an adversary can arbitrary read the content of application in surreptitious way without leaving any tread. In addition, the privacy problem is even more complicated since most of RFID tags respond to request from any reader. This issue makes RFID system is highly susceptible from authorized reading and tracking that may reveal the user’s privacy.

By enforcing the about same features as provided in IMKA-Tate, the RFID-Tate also establishes mutual authentication protocol with cryptographic challenge-response verification. In this case, the legitimate RFID tags and readers perform challenge request mechanism to each other in mutual-way with fresh and random cryptographic values for each session. Thus, an adversary will not be able to answer the challenge by just using the rouge reader that has no valid cryptographic challenge and respond values. Thus, the legitimate party (e.g. the RFID tag) will discard the connection by aborting the request. In general, by performing challenge-response and mutual authentication mechanisms, a rouge reader will not be able to arbitrary interact and read the content of RFID tag.

5.4.5. Potential Drawbacks and Mitigation Strategy

Instead of proposing and negotiating mutual key agreement to generate the primary session key like in IMAKA-Tate, the RFID-Tate rules the tag to comply with the session key generated by the reader. This method enables efficient cryptographic computation since the tag does not have to calculate one more pairing function in order to generate the session key. Nevertheless, the elimination of mutual session key agreement sacrifices the risk on brute force guessing of the session key. In particular case, a recent work [185] reports that a massive number of processors (e.g. 2^{30} processors) need to take about one year to break the DLP of the Tate pairing. Although one year is extremely very long for the case of WIP where the session may change very fast (e.g. only in a couple of seconds), the security may be reduced in the foreseeable future. The risk may be higher when an adversary is able to physically compromise or steal the unsupervised reader or tag, and further elicit the sensitive security parameters stored in the devices' memory. In this case, the sensitive security parameters may help an adversary to speed up the brute force guessing of the generated session key.

There are no perfect cryptographic algorithms that each of them must have particular drawback. To mitigate this risk, the smart RFID environment should applying tight surveillance of the employed personal security guard, thus any suspicious activity in the WIP environment can be detected. In addition, all legitimate reader should also be well protected with advanced physical protection (e.g. with alarm). This method is applied to prevent the unsupervised reader from being physically compromised by an adversary. Thus, there is no chance for an adversary to elicit the security properties stored in device's memory. In addition, security and data protection policy, as well as performing risk assessment should be established and maintained continuously. Moreover, all clients should be continuously educated and trained in order to establish knowledge and awareness against policy and critical data protection.

5.5. Conclusion

Although we sacrifice one feature in mutual key agreement in order to achieve optimal computation efficiency, we prove that RFID-Tate can also be relied to mitigate various security and privacy threats in multi-layer problem. Such protocol even can provide the same security resistance as provided by IMAKA-Tate, reaching from the resistance from physical layer attacks (e.g. relay attacks), network and transport layer attacks (e.g. cloning, impersonation, spoofing, resource consumption attacks, and protocol attacks such as various technic of man-in-the-middle attacks), application layer attacks (e.g. unauthorized tracking and reading, etc.), to multi-layer attacks such as traffic analysis attacks, denial-of-service attacks, and replay attacks.

RFID-Tate provides identity protection and mutual authentication with highly efficient computation overhead. It is affordable for the constrained nature of active RFID system. We have analyzed that RFID-Tate computation is two time faster than the computation overhead of our previous solution in IMAKA-Tate. On the other hand, RFID-Tate provides the relatively same security and privacy features as it is provided by IMAKA-Tate. In this regards, the proposed solution performs encryption of the active RFID tag identity even before the mutual authentication is started. This method prevents the tag identity from being revealed by unauthorized party. Therefore, privacy preserving can be achieved well.

Chapter 6

Key Management System

6.1. Introduction

The emerging of WIP technology (i.e. smart RFID applications), which extend the capability of a RFID tag to sense the environment condition (e.g. temperature, pressure, light, humidity, elevation, etc.), has been seen as a prominent solution in various fields including industrial applications. Indeed, its integration with sensor node can significantly improve the services, reduce operational and labor cost, increase productivity, and preserve the quality standards. In addition, such pervasive computing technology introduces various advantages ranging from low cost, to its flexibility to be deployed in large-scale system.

Nevertheless, smart RFID system introduces tremendous security and privacy problems. One of them is the complex problem in large-scale Key Management System (KMS). On the other hand, the enforcement of common KMS solution like using Public Key Infrastructure (PKI) demands higher resources consumption, which is infeasible for smart RFID system that associates to limited resources (i.e. limited CPU power, limited memory, limited battery/power, and low bandwidth/data-rate). On the other hand, enforcing manual key management solution by recalling all the RFID tags in order to update the security property (e.g. update the new private key) is not feasible to be applied in large-scale and distributed system.

Furthermore, most of existing solutions in key management system for wireless communication are highly susceptible to various security and privacy threats. For instance, an adversary may have chance to perform various techniques of Man-in-the-Middle attacks to compromise the key management system. Moreover, an adversary may impersonate as legitimate third party server, in order to trick the legitimate RFID tag and RFID reader to reveal their sensitive information. In this case, an adversary may reveal the privacy ranging from the location information, data applications, to the most critical information like security properties (e.g. the private key).

Indeed, using traditional PKI for the KMS is definitely not feasible to be applied in the constrained nature of WIP system. The following list describes the disadvantages of traditional PKI system in the face of WIP requirements.

- Traditional PKI system requires higher bandwidth resources. Most of standard PKI system requires full-time connection to the third-party server each time the new session is established. This method is performed to manage, distribute and revoke digital certificates [195]. On the other words, the connection to the third-party server is always required for each encryption process. This method is definitely not suitable to the system's limited resources of WIP system such as limited bandwidth or data-rate availability.
- Require higher system's resources. Most of standard PKI systems [196-199] rely on upper layer method (i.e. SSL/TLS) to perform authentication and encryption process. These methods introduce higher communication overhead, since the number and size of packets exchanged during the authentication process are higher when comparing to the system relies on lower layer method. In addition, most of standard PKI systems rely on heavy-weight cryptographic processing such as RSA method [200-202]. This issue makes the use of traditional PKI technology is feasible to be applied to the authentication system, which its clients have limited CPU power. Furthermore, the requirement in higher computation and communication overhead impact on particular drawback (e.g. higher energy

consumption). On the other hand, most of WIP clients are equipped with small or limited battery power.

- The risks on privacy, trust and relationship. Traditional PKI system requires complex architecture particularly in large-scale scenario. This issue introduces major risk that the PKI system is highly susceptible to the risks related to trust and relationship. In particular, Ellison and Schneier [179] define ten the risks about PKI system, including the problem about how to ensure the authority of the CA and how to protect the private signing key. Furthermore, during the last decade various weaknesses as well as its mitigation about PKI system have been reported. For instance, Holz et al. [183] introduce a solution to mitigate the risk on privacy and man-in-the-middle attacks. In addition, Suga et al. [184] propose a strategic solution to mitigate renegotiation attacks. Nevertheless, most of the solutions introduce various drawbacks, reaching from the weaknesses in complexity, to the risks related to performance.

Furthermore, in term of updating the security properties, the smart RFID system requires more specific needs that differ from common KMS. The following list defines the specific conditions in the RFID system where the KMS should update the new security properties.

- Life time for the security properties expires. In order to improve the security strength and guarantee the freshness, the security properties should be updated periodically. This method can also mitigate the system from being compromised.

- The increase number of new RFID tag deployed in the existing system might affect the need to update the security properties.

- The malicious tag or reader is detected. In case an adversary is able to compromise one or more RFID tags or RFID readers, all critical security properties in the existing networked system must be updated.

In general, the KMS for smart RFID system should be able to satisfy the dynamic requirements in large-scale deployment without hampering the system’s limited resources.

In addition, the KMS mechanism and architecture should also fit to operate with our proposed protocols (e.g. IMAKA-Tate and RFID-Tate). In other words, the proposed KMS should not require additional security setup and configuration, particularly for the constrained resources of RFID tag.

This chapter introduces a novel key management system that complements our previous work in RFID-Tate [23]. It is a light-weight key management solution that enables identity protection and mutual authentication using Identity-based Encryption (IBE) method. In particular, it relies on cryptographic Tate (ηT) pairing over super singular elliptic curves, ternary field $F_{3^{509}}$ [168]. Furthermore, in order to prolong the RFID tag lifetime, we propose efficient communication overhead. In this regards, the key management scheme relies on link layer security method, particularly over IEEE 802.15.4 which is commonly used to deliver low-data rate in order to produce efficient processing as well as save the energy. Thus, it is affordable to be applied in the constrained nature of smart RFID environment.

6.1.1. Vulnerabilities

Smart RFID system introduces tremendous problem in security and privacy ranging from the vulnerabilities that arise from the nature of wireless communications, the threats arising from the vulnerable nature of Wireless Sensor Networks (WSN), to the vulnerabilities derived from the use of RFID technic itself. In our previous works [22-23], we already demonstrated that our solution is feasible to mitigate various security and privacy threats in smart RFID system.

In this paper we particularly focus on the threats derived from key management scheme in the constrained nature of smart RFID, which are listed as follow.

- An adversary can perform various technics of Man-in-the-Middle (MITM) attacks in order to hijack the session and intercept the key management system. The adversary may steal the critical security properties including the private key and can use it to perform further malicious activities (e.g. cloning, impersonation, data manipulation, replay attacks, Denial-of-Service (DoS), etc.).

- The smart RFID system is highly susceptible from physical attacks. In his case, the adversary may steal the legitimate RFID tag and subsequently copies all the security properties in order to plant their own RFID tag. The stolen security properties may be used also to perform impersonation or playing with various technics of MITM, in order to fool the KMS.

- An adversary may eavesdrop the KMS in order to elicit the privacy. In this regards, an adversary can find out the sensitive information reaching from the position of the RFID tag as well as carry out unauthorized tracking.

In addition, various threats and risks on the communication between the RFID tag and the reader in multi-layer vulnerabilities are also susceptible for the KMS.

6.1.2. Requirements

The following list outlines the important requirements that must be fulfilled in order to achieve the integrity protection in the constrained nature of smart RFID system.

- *Mutual authentication and Authorization*. First of all, all participants in the communication of RFID system must be mutually authenticated before revealing their sensitive information to each other. Thus, it ensures that only authorized RFID tag or reader can be involved in the communication system. This requirement is also important to protect the system from various other threats in multi-layer vulnerabilities.

- *Availability*. In the constrained nature with limited connection and data-rate, the key management solution must ensure that the service is available to the RFID system whenever needed.

- *Privacy*. It ensures the confidentiality of the key management system, which prevents the sensitive information from being eavesdropped or illegally revealed by unauthorized party.

- *Credibility*. It ensures that all messages transported during the key management process are not modified or transited by unauthorized party.

- *Security strength and resistance*. It ensures that the key management solution is strong enough to prevent various threats ranging from various techniques of brute-force attacks, resource consumption attacks, various techniques of MITM attacks, to the specific threats on RFID communications including cloning, tag emulating, spoofing and impersonation.

- *Communication overhead*. The key management solution should ensure that the size and the number of messages transported during the key management process are affordable for the limited resources (i.e. limited bandwidth or data-rate).

- *Computation overhead*. The key management solution should ensure that the limited resource of RFID tag is feasible to deal with the cryptographic processing.

- *Storage overhead and energy consumption*. The KMS should ensure the security update is feasible for the limited storage and battery.

In general, the key management system should satisfy the smart RFID system requirements, reaching from the requirements related to system's limited resources, to the requirements related to security and privacy.

6.1.3. Challenges

The following list describes the challenges in designing efficient key management solution to enforce security and privacy protection in large-scale smart RFID system.

- *Vulnerable nature of wireless communication*. The broadcast nature of wireless channel makes an adversary has good chances to perform active and passive Eavesdroppings including various technics of Man-in-the-Middle attacks.

- *Limited CPU power*. The sensor integration to the RFID tag can give benefit to the increase of processing power. Several standard sensor platform platforms have diverse options of core frequency (i.e. 104, 208, 312 and 416 MHz). Nevertheless, such CPU options are still not feasible for common solution in standard key management system such as TLS/SSL. Indeed, it introduces high computation overhead that overburdens the limited capabilities of CPU, particularly in large-scale system which the key management activities might be frequently required.

- *Limited battery*. Most of Standard solution like TLS/SSL introduces high communication overhead. This issue causes drainage of the battery energy affecting the lifetime of the RFID tag expires soon.

- *Limited memory storage*. Smart RFID system requires more storage to store various parameter including sensor application data and the security properties. On the other hand, most of standard RFID tag as well as sensor node have very limited memory storage.

- *Low data-rate*. Typically, tiny devices communicate over standard IEEE 802.15.4 which delivers low data-rate. Such standard wireless technology is chosen in order to save the battery energy as well as for efficient processing. Thus, the key management system must sustain this requirement by providing efficient communication that optimally minimizes the number and the length of packets that are transported during the security management process.

- *Large-scale system*. Taking into account the smart RFID tag deployed in large-scale scenario, this issue makes all aforementioned challenges as well as the security management are more complicated.

- *High risk on various security threats*. Most of RFID communication is not mutually authenticated. This issue introduces specific security and privacy problem. In this case, an adversary might perform malicious activities based on various technics of MITM, including cloning attacks, replay attacks, etc. Moreover, an adversary may also intercept the key management system or even revealing the privacy (e.g. tag location) based on the broadcasted MAC Address. Furthermore, the content of RFID tag can easily be read without authorization.

In general, the challenges in providing KMS for the smart RFID system, ranging from the challenge in the system's limited resources, the large scale management, to various security and privacy threats emerging from multi-layer vulnerabilities.

6.2. Key Management Scheme

This section structurally describes the proposed scheme of key management solution for large-scale smart RFID system.

6.2.1. Preliminaries

We apply ηT pairing with 128 bit extension field $F_{3^{509\,x\,6}}$. It is noticed as the fastest pairing method over super singular curve [166][181] with advanced level security strength. It provides cryptographic protection which is about same security level as 1024 bit of RSA method [170].

In the key management scheme, we initially assume that the reader and the RFID tag perform mutual authentication to each other like defined in RFID-Tate [23]. In this regards, they communicate over standard IEEE 802.15.4f, which defines standard wireless Physical (PHY) and Media access control (MAC) for active RFID. Furthermore, we assume that each smart RFID tag is complemented with co-processor, as it is integrated to standard platform like Imote2 that has various options of core frequency (i.e. 104, 208, 312 and 416 MHz).

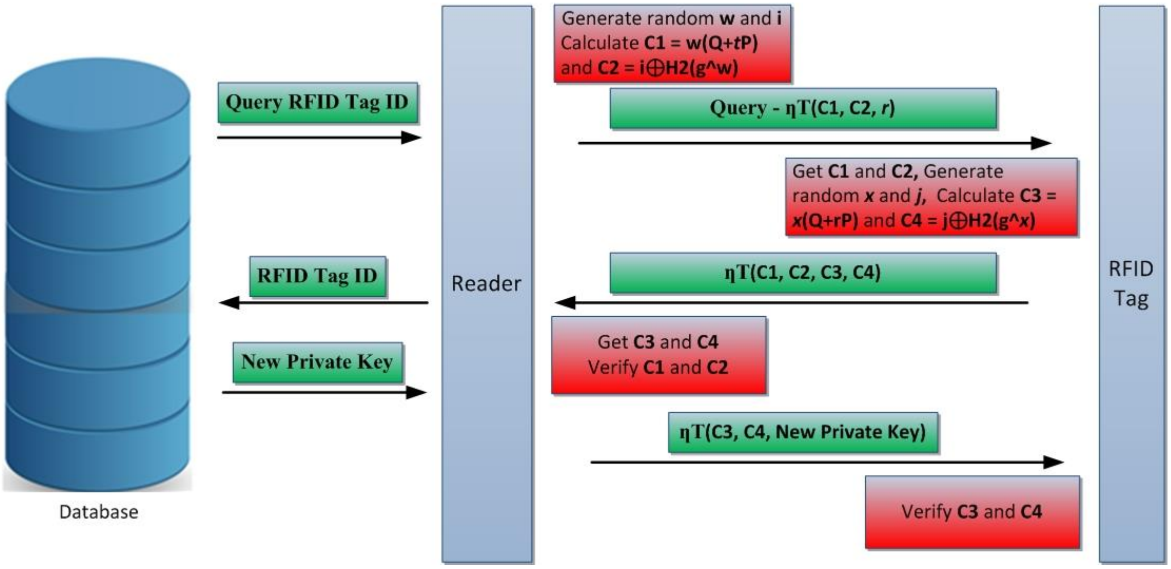


Figure 6.1. Three-way handshake of the key management scheme.

6.2.2. Authentication and Key Update

After the reader and the RFID tag have connected to each other according to the procedure defined in RFID-Tate [23], the database is now ready to carry out key update procedure. In this scenario, the reader acts as a pass-through device, while the RFID tag and the database act as client and server. Figure 1 illustrates the mutual authentication and key update by performing encrypted three-way handshake negotiation. The following list describes the three-way handshake procedure.

1. Initially, the database sends query message to the RFID tag through the reader, in order to inquiry the tag ID. In this case, The reader firstly calculates the tag public key as $t = H1(tag\ MAC\ address)$. Subsequently, the reader randomly generates two 128 bit integer i and w, where i is temporary session key.

2. The reader then generates two ciphertexts $C1 = w(Q + tP)$ and $C2 = i \oplus H2(g^w)$. The reader subsequently pass on the query message that is included in the two ciphertexts to the RFID tag. The reader also includes its MAC address $r = H1(reader\ MAC\ address)$ in the encrypted payload. This mechanism is conducted in order to protect its identity from being revealed by unauthorized party. In this case,

all contents in the message including the query message, the session key *i* and the reader MAC address are encrypted using the RFID tag public key. Thus, only the corresponded RFID tag can decrypt the message.

3. The tag receives and decrypts the messages using its private key *T*. The tag is able to elicit all contents of the message including the session key *i* by calculating $i = H2(e(T, C1)) \oplus C2$.

4. In the second message of the key management process, the tag generate *x* and *j* as two random 128 bit integers, where *j* is primary session key that is used in the rest of key management process including transporting the new private key for the RFID tag. The tag afterward generates and send two ciphertexts $C3 = x(Q + rP)$ and $C4 = j \oplus H2(g^x)$. The tag also attaches the chippertexts of *C1* and *C2* in the encrypted message to be verified by the reader.

5. The reader then proceeds the key management process by decrypting the message which contains the session key *j* using its private key *R*. It is carried out by computing $j = H2(e(R, C3)) \oplus C4$. The reader further verifies the value of *C1* and *C2*. The reader then pass on the tag ID to the database only if the two values are same as the two values of *C1* and *C2* generated by the reader on the first message. Otherwise, the reader discards the query.

6. The database then sends the new private key of the corresponding RFID tag through the reader. The reader then forwards the new private key to the corresponding tag and includes the value of *C3* and *C4* to be verified by the tag in the encrypted-payload. The tag accept the new private key if the received values of *C3* and *C4* are equal as the values generated by the tag on the second message. Otherwise, the reader sends failure notification to discard the key management process.

Up to this step, the RFID tag can use its new private key to perform further mutual authentication with the reader as well as securing the communication according to the RFID-Tate scheme.

TABLE 6.1. ESTIMATION OF KMS COMPUTATION AT 416 MHZ

Phase	Main Operations	Time Estimation
Mutual Authentication & Sharing the new Private Key	1 ηT Pairing	*22.79 ms*
	1 Exp. $F_{3^{509\,x\,6}}$	*0.577 ms*
	2 Multipl. $F_{3^{509\,x\,6}}$	*0.181 ms*
	Total	***23.54 ms***

TABLE 6.2. ESTIMATION OF KMS COMPUTATION AT 208 MHZ

Phase	Main Operations	Time Estimation
Mutual Authentication & Sharing the new Private Key	1 ηT Pairing	*34.34 ms*
	1 Exp. $F_{3^{509\,x\,6}}$	*1.144 ms*
	2 Multipl. $F_{3^{509\,x\,6}}$	*0.451 ms*
	Total	***35.93 ms***

TABLE 6.3. ESTIMATION OF KMS COMPUTATION AT 104 MHZ

Phase	Main Operations	Time Estimation
Mutual Authentication & Sharing the new Private Key	1 ηT Pairing	*54.54 ms*
	1 Exp. $F_{3^{509\,x\,6}}$	*2.129 ms*
	2 Multipl. $F_{3^{509\,x\,6}}$	*0.653 ms*
	Total	***57.32 ms***

6.3. Computation Overhead Analysis

Efficient computation overhead is a critical requirement for RFID system that associates with limited resources. In order to ensure that our key management solution is affordable for the smart RFID system, we conducted a benchmark test that iteratively calculate the time performance of IBE 128 bit ηT pairing over $F_{3^{509\,x\,6}}$. This benchmark test is written in C++ adapted from [2][5]. We executed the benchmark test in our platform under Windows 7 with 64-bit Intel 2 Cores at 1.8 GHz. In order to emulate the smart RFID system, we forced the CPU to run in a single core. In addition, we scaled down clock frequency according to the three options of Imote2 platform (i.e. 104 MHz, 208 MHz and 416 MHz).

Table 1, 2 and 3 summarize the 1000 iterations of computation performance calculated by each RFID tag at the three options of clock frequencies. On each key management process, each RFID tag computes several cryptographic parameters in order to perform mutual authentication. The parameters are two Multiplication over $F_{3^{509\,x\,6}}$ (Multipl. $F_{3^{509\,x\,6}}$), one Exponentiation over $F_{3^{509\,x\,6}}$ (Exp. $F_{3^{509\,x\,6}}$) and one ηT Pairing. According to the three tables, the computation performance is feasible for the smart RFID tag, even it is affordable for the lowest CPU option at 104 MHz which computes the mutual authentication only in 57 milliseconds. Moreover, the average performance is more than two times faster when the benchmark test was executed in the advanced clock frequency at 416 MHz. Indeed, the key management process was accomplished only in about 24 milliseconds. Thus, in extraordinary case where the RFID tag moves very fast from one point to other point, the KMS still works very well, since the processing time is much more faster than the computation time of the baseline defined in chapter 3 (i.e. 250 ms).

6.4. The Fulfilled Security Requirements

This section discusses the security requirements that have described in the first section. The following list outlines such requirements that are fulfilled by our key management solution.

- *Mutual authentication and authorization*. Our key management solution provides such feature, in order to prevent various threats on impersonation, fraudulence and various techniques of MITM (e.g. intercept the key management system, DoS, replay attack, etc.). In this case, the tag and the reader exchange the challenge in mutual way. Particularly, they exchange and verify the random value of (*C1*, *C2*) and (*C3*, *C4*) that are generated for each other. Indeed, if the exchanged two values cannot be verified, the key management process is aborted. Thus, it ensures that only authorized party can get access to the security service.
- *Availability*. Our solution ensures that the key management system is always available every time the RFID tag finds the located reader. In this regards, the RFID

reader is always connected to the RFID database. In other word, it arguably ensures that the service is available whenever needed.

- *Privacy*. The identity is included in the encrypted payload (i.e. *ηT(C1, C2)* and *ηT(C3, C4)*), thus only corresponding recipient can find out the correct source or destination address. In addition, the protection is layered by firstly hashing the identity (i.e. *t = H1(tag MAC address)* and *r = H1(reader MAC address)*) before attaching it in the encrypted message.

- *Credibility*. It was proved on the previous section that our solution can ensure that all communication payloads are not being altered or transited, since only authorized party can get access to the system. In this regards, we proved that even an adversary who is able to get the security parameter (e.g. by performing physical attack to unsupervised RFID tag), he or she somehow will not be able to compromise the RFID communications.

- *Security strength and resistance*. Our solution relies on 128 bit security strength of *ηT* paring, which is about same as the 1024 bit of RSA method. Thus, it is strong enough to prevent the key management solution from various techniques of brute-force attacks. Furthermore, it was demonstrated in previous section that the key management system can mitigate various security and privacy threats on smart RFID system, including cloning attacks, impersonation, resources consumption attacks as well as various technic of MITM attacks.

- *Communication overhead*. As described in section III, the key management systems only need to exchange the mutual authentication message in three-way handshake. The first message is 48 byte in length including 128 bit *C1*, 128 bit *C2* and 128 bit public key of the reader *r* (see figure 1). The second message is 64 Byte in length, including the four ciphertexts (i.e. *C1*, *C2*, *C3* and *C4*). Indeed, the maximum size of the authentication message that is required to be transported is only 160 Bytes in length. It is the third messages in the mutual authentication process, which includes

128 byte of the new private key and the two values of *C3* and *C4* with 128 bit each. Thus, it is doable to be transmitted in one frame of standard IEEE 802.15.4.

- *Computation overhead*. Our experiment demonstrated that the performance of our key management solution is affordable for the limited CPU options. It is even feasible for the lower option of clock frequencies at 104 MHz, which is done only in 0.057 sec.
- *Storage overhead*. The security properties that are stored in the RFID tag memory are *E* (1 Byte), *P* (128 Bytes), *Q* (128 Bytes), *g* (768 Bytes) and one private key *T* (128 Byte). In overall, the RFID tag requires a storage space less than 2KB.

In general, the proposed KMS for smart RFID system satisfies the requirements in multi-aspects, ranging from the challenge in the system's limited resources, the large scale management, to various security and privacy threats emerging from multi-layer vulnerabilities.

6.5. Conclusion

Providing key management solution in the system's limited resources such as RFID system is a complex challenges. However, we proved that our solution suits to the security requirements in the constrained nature of smart RFID system. It is affordable for the RFID tag that associates with limited resources (i.e. limited data-rate, limited CPU power, limited battery and memory storage). Furthermore, the analysis results presented that the key management solution can mitigate various threats including various technics of MITM attacks as well as various threats raised from the use of RFID technic itself (i.e. cloning attacks, unauthorized tracking, impersonation, etc.). In addition, both the RFID tag and the reader identities are protected in double-layered way. It is conducted by firstly hashing it in 128 bit integer and sequentially attaching it in to the encrypted payload. Thus, the privacy can be preserved and all possible threats arising from the revealed identity can be mitigated as well.

Chapter 7

Conclusion and Future Works

In this thesis, we have presented a novel security and privacy protection tailored to mitigate broader security and privacy problem in the constrained nature of wireless indoor positioning system. We demonstrated on security analysis that our solution can mitigate various aspects of multi-layer problem reaching from privacy preserving, mitigating some of physical threats, network and transport layer vulnerabilities, the application layer, to the threats raised from the exploitation several layer vulnerabilities. The main keys of our solution are the identity protection, mutual authentication and verification methods that fully rely on data-link layer. In this regards, the elimination of using upper-layer method is an effective way to provide efficient security and privacy protection with feasible computation and communication overhead. Thus, it is applicable for the constrained nature of wireless indoor positioning system.

Furthermore, we conducted extensive evaluation including the computation analysis and security and privacy analysis in several aspects of WIP systems including WIP based on WLAN and WPAN technologies, WIP based on RFID system and the corresponding key management system. Compared to the common security solution in WIP system, our approach can mitigate various risks more comprehensive in multi-layer problem and even it is suitable to be applied in broader application of wireless communication systems.

7.1. Contribution

This thesis comprises five main contributions that aim at mitigating specific security and privacy challenges in the constrained nature of WIP system, which are listed as follow.

- We investigated the possible threats and risks on security and privacy problem in WIP system. In this work, comprehensive problem in various aspects is presented, reaching from physical layer, network and transport layer, application layer, to the problem derived from combination of multi-layer vulnerabilities. In addition, we outline also various state of the art solution that focus on solving particular problem in a specific aspect. The lesson learned from this work is that the security and privacy problem in WIP system cannot be solved by just focusing on particular aspect of the problem.
- We propose a light-weight security and privacy protection tailored to the constrained nature of WIP system. The security and privacy protection relies on link layer method in order to provide efficient method with minimum computation and communication overhead. The light-weight method enables mutual authentication, verification and identity protection method to protect various threats in broader scope of WIP system.
- We design key management system as complementary service to our proposed mutual authentication protocol. The key management system provides light-weight security system update including mechanism to update the private key. Such key management system is designed with minimum bandwidth requirement in order to satisfy the need in system's limited resources of WIP applications. Thus, the system update is always available and possible to be done whenever the security properties are required to be renewed.
- We analyze the security and privacy protection of our proposed solution in several fields of WIP systems including WIP based on WLAN and WPAN technologies, RFID based system and the corresponding key management system. We demonstrated that our solution can be relied to mitigate various threats in multi aspects of WIP problem. It ranges from privacy problem, physical layer threats such as relay attacks, network and

transport based attacks (e.g. impersonation, spoofing, cloning attack, resource consumption attacks, network protocol attack such as various technics of man-in-the-middle attacks, etc.), application layer attack (e.g. unauthorized tag reading, unauthorized tracking, and tag modification), to the multi-layer problem such as replay attacks, traffic analysis and denial-of-services.

- We evaluate the performance of our proposed solution in various field of WIP system (i.e. WIP based on WLAN, WPAN, RFID system, and the corresponding KMS). The evaluation covers various aspects including the communication complexity, storage requirement and the processing overhead. For the communication complexity we analyze our solution according to the number and size of messages exchanged during the mutual authentication on the designed protocol. The analysis of storage requirement is defined based on the size of key and other security parameters that must be stored in the node or RFID tag's memory, while the processing overhead is defined by emulating the computation performance of cryptographic algorithm used in our proposed protocol. All results of this evaluation demonstrated that the proposed methods are feasible to be implemented in the constrained nature of WIP system.

7.2. Future Works

Although we have proved that our proposed solution can mitigate various threats in broader aspects of security and privacy in WIP system, nevertheless providing an integrity protection that covers the entire aspects is unrealistic goal. Thus, we left several aspects that can be used as direction for further works.

7.2.1. Cryptographic Algorithm Refinements

While focusing our work in security and privacy in the constrained nature of WIP system, we left few aspects of optimizations and refinements of cryptographic algorithm used in our proposed solution. Although it is claimed that elliptic curves $F_{3^{509x6}}$ is about same security strange with 1024 bit RSA modulus [170], surprisingly a recent work report that such 128 bit security level of cryptographic Tate pairing over $F_{3^{509x6}}$ is less resistant to attacks on the elliptic curve Discrete Logarithm Problem (DLP), Gora Adj et al. [185]. In particular, the authors estimate that the logarithms can be computed in $2^{81.7}$ time unit, by using combination algorithms introduced by Joux [186] and Barbulescu et al. [187]. Although computing $2^{81.7}$ is obviously a very hard challenge, the authors argue that it might be possible in the foreseeable future for a very well-funded adversary or at least for the one who has access to a massive number of processors (e.g. 2^{30} processors), to execute the computing challenges within one year.

Although we can also argue that spending one year will not give any particular gain to an adversary since the proposed solution generate random cryptographic value for every session. In such mobile environment which the parameter and the session are changed very fast (e.g. just in a couple of seconds or minutes), breaking the communication in one week is even not useful. Furthermore, not only the session and the security parameters, the light-weight Key Management System defined in chapter 6 also enables to update the security properties (e.g. the private key) within particular period of time. Thus, in case an adversary can break the system in shorter period of time, he will not be able to use the old properties to get access to the system. In general, an adversary will not be able to compromise the WIP system by just using the session key that was generated in previous year. Nevertheless, such reported research work somehow should be noted as potential drawback for our proposed solution. Thus, the refinements of cryptographic algorithm should be marked as one of directions for the future works.

7.2.2. Protocol Refinements Tailored to new Cryptographic Algorithm

Other option to improve the security protection in term of the vulnerability on DLP is by using other pairing based cryptosystems. In this regard, a new protocol must be redesign in order to match with the chosen cryptographic algorithm. One promising solution is the one based on Barreto-Naerig curves [188], which use larger primes number such as a prime of 256 bit length for a 128bit security. Several options of the curve implementation can be used for efficient protocol design such as Devegili et al. [189], Shirase et al. [190], and Beuchat et al. [191].

Nevertheless, when addressing the protocol refinement for the vulnerability in term of DLP, the proposed solution must also consider the characteristic of WIP system that have been satisfied in this thesis, reaching from the system's constrained resources (i.e. limited memory storage, processing power, battery/power supply, and limited access and data-rate), the privacy preserving aspects, to the security resistant that cover various aspect in multi-layer vulnerabilities.

7.2.3. Security Threats on Physical Radio Channel

When focusing our work on multi-aspect security and privacy problem in the WIP system, we left few aspects of security protection particularly related to wireless radio channel security, such as radio jamming and various technics of relay attacks for denial of service purpose. We have proved that our proposed solution can mitigate the relay attacks in the purpose of revealing the privacy, particularly the attacks that target particular victim in the density environment. Nevertheless, an adversary still have chance to randomly perform such attacks targeting to random authorized users in order to perform denial-of-service. In this case, a transponder can be used to intercept and alter the radio signal, so that either a legitimate client or its peer discards the communication due to the suspicious contents. Various solutions have been provided for this specific problem such as Distance Bounding protocol and its variants [43-56]. Nevertheless, this method aims at detecting the relay attacks rather than preventing the attacks to be launched.

Another problem that always becomes a specter in common wireless communication is a radio jamming. Although this problem is not particularly raised from the case of WIP system, we should somehow consider this problem in order to achieve the integrity protection. It is to be noted that the proposed physical layer solution that will be introduced in the future work must not conflict and hamper the performance of security and privacy solution tailored to mitigate various threats in the upper-layer.

7.2.4. Security for covert channel and side channel attacks

Covert channel and side channel attacks are basically not common threats in WIP system. These types of attacks cannot be launched remotely like common attacks in network or transport layers, means that the attacks are impossible to be done without physically comprising or stealing the victim's devices. Nevertheless, take into account that some of WIP applications may deploy in uncontrolled environment, this situation may introduce a chance for an adversary to launch these attacks. On the other hand, Various research works have introduced in these fields [152-156], nevertheless most of them introduce major drawback that increase the power consumption and manufacturing cost. Therefore, a suitable solution that tailored to the constrained nature of WIP system should be developed in the future.

7.2.5. Security Policy, Database and Middleware Architecture

When addressing our work for multi-aspect of security and privacy in the WIP applications, we left several aspects of security optimization related to policy, database and middleware architecture. Various vulnerabilities may arise from inappropriate development of such aspects. One example is various threats on middleware attacks. Although our proposed solution provides access control that prevents an adversary to launch middleware attack such as SQL injection, nevertheless such attacks can be launched by insider that already has access to the communication system. Even an adversary has possible chance to launch the attack, if he is able to steal the legitimate node (i.e. unsupervised node). Thus, an appropriate policy, database and middleware security should be the further research to combat and cope with the threats.

7.2.6. Other Methods of WIP Systems

Wireless indoor positioning system is a very broad application that uses various methods to define the client's position. During the last decade, various promising WIP methods have been introduced including the one using infrared technology, ultrasound, magnetic signals, vision analysis and audible sound. Furthermore, WIP system based on various contexts of cellular network technologies including UMTS, GSM, GPRS, LTE, CDMA and HSPA expand the scope of WIP method.

All aforementioned WIP methods also introduce specific security and privacy challenges, particularly the requirements related to architecture and characteristic of the used technology. Thus, the security and privacy method tailored to the aforementioned technologies should be considered as future work.

7.3. Conclusion Remarks

This thesis has shown that wireless indoor positioning system introduces complex challenges in term of security and privacy preserving particularly in large-scale scenario. Indeed, WIP system is highly susceptible from tremendous security and privacy threats in multi-aspects vulnerabilities. On the other hand, enforcing common security method is not affordable to be applied in the system's limited resources of the WIP system. Therefore, WIP system introduces the need on a novel system's protection that covers broader aspects of security and privacy problem.

We have presented our proposed solution that is suitable to combat the security and privacy threats in the constrained nature of WIP system. Our solution cover several aspect of WIP system including for WIP based on WLAN/WPAN, RFID system and the complementary key management system. Compared to state of the art solution in WIP system, the security analyses have shown that our method is effective to combat various threats in broader aspects of security and privacy issues. The key factors of our methods are by protecting the identity and enforcing the security procedure in the lowest possible layer of wireless communication (i.e. data-link layer). In addition, the proposed solution enables access control, which fully relied on link layer method complemented with authentication, key agreement and verification in mutual way. Thus, most of the security and privacy threats based on inherent vulnerabilities in lower and the upper layer can be mitigated.

In cryptographic protection point of view, our solutions provide advance protection methods, which establish two-tier identity protection since in the beginning of authentication process. In this regards, the client identity (i.e. a binary MAC address) is firstly hashed into 128 bit integer and then the hashed value is included in the encrypted payload of the established session. Thus, an adversary must firstly break the session key and then break the hash function in order to reveal the identity. In general, by protecting the identity various risks related to privacy can be mitigated. In addition, this method is also effective to strengthen the security since most of state-of-the art attacks cannot be launched without revealing the identity.

Furthermore, our proposed solution that protect the identity on the lowest possible layer (i.e. MAC Address) can mitigate the threats based on physical layer such as various technic of relay attacks. Although an adversary is still able to relay the encrypted messages as well as observe its inherent meta-data (e.g. time of arrival), the adversary will not be able to find the node identity (i.e. the MAC address). In this regards, the adversary may be able to reveal the location information of the particular node based on meta-data in physical layer such as the time of arrival. Nevertheless, he will not be able to recognize the node identity which is included in the encrypted payload. In other word, an adversary may still be able to launch the relay attacks, however he will not be able to gain significant benefit since there is no chance for the adversary to identify the node, particularly in density environments. In general, eliciting the position information without revealing the identity is considered as useless information.

Moreover, the identity protection is also effective as complementary method to strengthen the security procedure, since most of attacks that exploit various problems reaching from the vulnerabilities of data link layer, network and transport layer, application layer, to multi-layer problems cannot be conducted without revealing the identity of the possible victims. We can learn from one example of attack such as various technics of resource consumption attacks. This attack is type of denial of service attacks that aims at draining the battery and wasting the bandwidth by repeatedly sending amount of packets to the node/victim. Nevertheless, an adversary will not be able to send the malicious packets to the node without firstly finding the identity of the destination address (i.e. node's identity).

Not only preserving the privacy and securing the threats in lower and upper layer, protecting the identity but also can mitigate various threats raised from multi-layer vulnerabilities such as traffic analysis attacks. In this case, an adversary will not be able to particularly infer the traffic pattern since he will not be able to decrypt the encrypted identity that is used as source and destination address of the traffic. In other world, an adversary may be able to intercept and learn the encrypted messages, however he will not be able to answer particular questions such as who changes to medium to medium which indicates the movement profile, who talks to whom which can indicate the relationship among the clients, or who moves when which may indicate the position, duty or values of the clients or commodities.

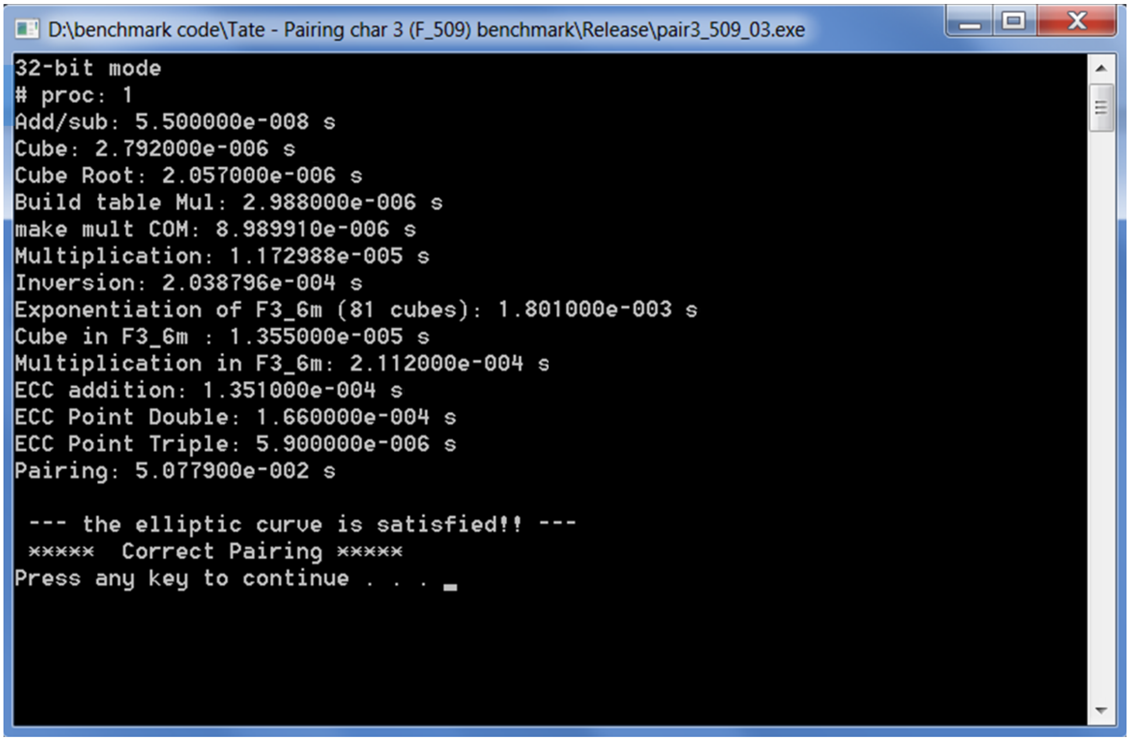
In addition, the proposed solution enables feasible challenge-respond verification as additional feature to provide access control and mitigating impersonation. This issue can provide resistance from various threats, such as replay attacks that exploit the vulnerabilities of multi-layer problem. For instance, an adversary can relay and copy the encrypted authentication message and later broadcast the message in order to impersonate as legitimate party. By reusing the relayed message an adversary can impersonate either as legitimate node or peer. Thus, the legitimate parties (i.e. the node and its peer) will grant access since they are fooled to think that they communicate in proper way. Nevertheless in our method, the legitimate node and its peer perform challenge-respond mechanism to each other in mutual-way with fresh and random cryptographic values for each session. Therefore, an adversary will not be able to answer the challenge by just replaying the old message, which is intercepted during the previous session.

In general, a light-weight mutual authentication and verification that is affordable to be applied in the constrained nature of WIP system is a key feature to protect the system from various threats in broader scope of security problem. Particularly, this method can provide access control that only authorized party can connect to the communication system. Indeed, such features as well as the combination with the identity protection can mitigate most of known attacks reaching from the physical layer (e.g. relay attacks), network and transport layer attacks (e.g. cloning, impersonation, spoofing, resource consumption attacks, and protocol attacks such as various technic of man-in-the-middle attacks), application layer attacks (e.g. unauthorized tracking, etc.), to multi-layer attacks such as traffic analysis attacks, denial-of-service attacks, and replay attacks.

As final conclusion, this thesis has introduced a novel security and privacy protection that cover various aspects of WIP system including WLAN/WPAN based WIP system, RFID system and the key management system as complementary component to strengthen the security and privacy enforcement. Indeed, compared to state of the art solutions, our proposed solution covers broader scope of security and privacy problem that can mitigate various risks in multi-layer problem.

Appendix

Sample of 128 bit Tate Paring $F_{3^{509\,x\,6}}$


D:\benchmark code\Tate - Pairing char 3 (F_509) benchmark\Release\pair3_509_03.exe

```
32-bit mode
# proc: 1
Add/sub: 5.500000e-008 s
Cube: 2.792000e-006 s
Cube Root: 2.057000e-006 s
Build table Mul: 2.988000e-006 s
make mult COM: 8.989910e-006 s
Multiplication: 1.172988e-005 s
Inversion: 2.038796e-004 s
Exponentiation of F3_6m (81 cubes): 1.801000e-003 s
Cube in F3_6m : 1.355000e-005 s
Multiplication in F3_6m: 2.112000e-004 s
ECC addition: 1.351000e-004 s
ECC Point Double: 1.660000e-004 s
ECC Point Triple: 5.900000e-006 s
Pairing: 5.077900e-002 s

 --- the elliptic curve is satisfied!! ---
 *****  Correct Pairing *****
Press any key to continue . . .
```

Figure A.1. 128 bit Tate pairing $F_{3^{509\,x\,6}}$ benchmark test at 104 MHz.

In this section we show a sample of benchmark test of the Tate pairing cryptographic processing adapted from [181]. The benchmark test estimated the time consuming for the cryptographic method. It is a benchmark test of all parameters that are needed to construct 128 bit ηT pairing over $F_{3^{509\,x\,6}}$. The code of such benchmark test is written in C++ adapted from [168]. The benchmark tests were executed in our platform under Windows 7 with 64-

bit Intel i5 4 Cores at 1.8 GHz. In order to emulate the WIP end-device, we forced our platform to run into a single core processor and scaled down the CPU according to an example standard sensor platform (i.e. 104 MHz). According to the two benchmark test implied in figure A.1., the pairing function was executed in 50.77 milliseconds, while the Exponentiation over $F_{3^{509} x 6}$ was executed in 1.8 milliseconds.

Glossary

AOA angle-of-arrival

CDMA code division multiple access

CPU central processing unit

DBP distance bounding protocol

DLP discrete logarithm problem

DoS denial-of-service

DPA Differential Power Analysis

DSR dynamic source routing protocol

ECC elliptic curve cryptography

EPC electronic product code

ESS extended service set

GPRS general packet radio service

GPS global positioning system

GSM groupe spécial mobile (global system for mobile communications)

HSPA high speed packet access

IDS intrusion detection system

IBE identity-based encryption

KMS key management system

LTE long-term evolution

MAC media access control

MAC message authentication codes

MITM man-in-the-middle

NFC near field communication

PBC pairing-based cryptography

PDA personal digital assistant

PKC public-key cryptography

PKI public key infrastructure

PKG private-key generator

PPS public parameter server

RF radio frequency

RFID radio-frequency identification

RTT round trip time

SPA simple power analysis

SSL secure sockets layer

TDOA time-difference-of-arrival

TLS transport layer security

TOA time-of-arrival

TOF time-of-flight

UMTS universal mobile telecommunications system

WBAN wireless body area network

WIP wireless indoor positioning

WLAN wireless local area network

WPAN wireless personal area network

WSN wireless sensor network

List of Figures

List of Tables

Bibliography

[1] Y. Lee, L. Batina, and I. Verbauwhede, “Untraceable RFID authentication protocols: revision of EC-RAC,” In IEEE International Conference on RFID, pages 178–185, 2009.

[2] Y. Lee, L. Batina, D. Singel´ee, and I. Verbauwhede, “Low-cost untraceable authentication protocols for RFID,” In ACM Conference on Wireless Nnetwork Security (WiSec), pages 55–64, 2010.

[3] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and implementation of PUFbased “unclonable” RFID ICs for anti-counterfeiting and security applications,” In Proceedings of the 2008 IEEE international conference on RFID, 16–17 April 2008 (pp. 58–64). Las Vegas: IEEE Computer Society.

[4] Ari Juels, “Strengthening EPC tags against cloning,” In M. Jakobsson & R. Povendran (Eds.), Proceedings of ACM workshop on wireless security (WiSec’05) (pp. 67–76). New York: ACM.

[5] P. Tuyls, and L. Batina, “RFID tags for anti-counterfeiting. In D. Pointcheval (Ed.),” Topics in cryptology – CTRSA 2006, proceedings of the cryptographer’s track at the RSA conference 2006, San Jose, CA, USA, February 13–17, 2006. Lecture notes in computer science, security and cryptology (Vol. 3860, pp. 115–131). Berlin: Springer. doi:10.1007/11605805.

[6] L. Mirowski, and J. Hartnett, “Deckard: A system to detect change of RFID tag ownership,” International Journal of Computer Science and Network Security, 7(7), 89–98.

[7] J. Halamka, A. Juels, A. Stubblefield, and J. Westhues, “The security implications of VeriChip cloning,” Journal of American Medical Informatics Association, 13(6), 601–607.

[8] Eun Young Choia, Dong Hoon Leeb, and Jong In Lim, “Anti-cloning protocol suitable to EPCglobal Class-1 Generation-2 RFID systems,” Computer Standards & Interfaces. Volume 31, Issue 6, November 2009, Pages 1124–1130.

[9] Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede, “EC-RAC (ECDLP based Randomized Access Control): provably secure RFID authentication protocol,” In IEEE International Conference on RFID, pages 97–104, 2008.

[10] Julien Bringer, Hervé Chabanne, and Thomas Icart, “Cryptanalysis of EC-RAC, a RFID identification protocol,” In Cryptology and Network Security (CANS), pages 149–161. Springer-Verlag LNCS 5339, 2008.

[11] Ton van Deursen and Saša Radomirović, “EC-RAC: enriching a capacious RFID attack collection,” In Radio Frequency Identification: Security and Privacy Issues (RFIDSec), pages 75–90. Springer-Verlag LNCS 6370, 2010.

[12] Junfeng Fan, Jens Hermans, and Frederik Vercauteren, “On the claimed privacy of EC-RAC III,” In Radio Frequency Identification: Security and Privacy Issues (RFIDSec), pages 66–74. Springer-Verlag LNCS 6370, 2010.

[13] Gildas Avoine and Philippe Oechslin, “A scalable and provably secure hash-based RFID protocol,” Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on , vol., no., pp.110,114, 8-12 March 2005. doi: 10.1109/PERCOMW.2005.12

[14] Ari Juels, “Minimalist cryptography for low-cost RFID tags,” In The Fourth International Conference on Security in Communication Networks – SCN 2004, LNCS, Springer, 2004.

[15] Naveen Sastry, Umesh Shankar and David Wagner, “Secure verification of Location Claims,” In Proceedings of the 2nd ACM workshop on Wireless security, WiSe 2003.

[16] Marco Gruteser and Dirk Grunwald, “Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking,” In Proceedings of the 1st

international conference on Mobile systems, applications and services, MobiSys 2003.

[17] Jason I. Hong, James A. Landay, “An architecture for privacy-sensitive ubiquitous computing,” In Proceedings of the 2nd international conference on Mobile systems, applications, and services, MobiSys 2004.

[18] Ari Juels, Ronald L Rivest and Michael Szydlo, “The blocker tag: Selective blocking of RFID tags for consumer privacy,” Proceedings of the 10th ACM conference on Computer and communications Security – CCS, ACM Press, 2003.

[19] Ari Juels and John Brainard, “Soft blocking: Flexible blocker tags on the cheap,” In Sabrina De Capitani di Vimercati and Paul Syverson, editors, Workshop on Privacy in the Electronic Society – WPES, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.

[20] Günter Karjoth , and Paul A. Moskowitz, “Disabling RFID tags with visible confirmation: clipped tags are silenced,” Proceedings of the 2005 ACM workshop on Privacy in the electronic society, November 07-07, 2005, Alexandria, VA, USA.

[21] Mohammad Fal Sadikin, Marcel Kyas, “IMAKA-Tate: Secure and Efficient Privacy Preserving for Indoor Positioning Applications,” In Proceedings of the 5th International Conference on Smart Communications in Network Technologies (SaCoNet), June 2014, Vilanova i la Geltrú, Spain.

[22] Mohammad Fal Sadikin, Marcel Kyas, “Security and Privacy Protocol for Emerging Smart RFID Applications,” In Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), July 2014, Las Vegas, Nevada, USA.

[23] Mohammad Fal Sadikin, Marcel Kyas, “RFID-tate: Efficient security and privacy protection for active RFID over IEEE 802.15.4,” In Proceedings of the 5th International Conference on Information, Intelligence, Systems and Applications (IISA), July 2014, Chania, Crete, Greece.

[24] Mohammad Fal Sadikin, Marcel Kyas, “Efficient Key Management System for Large-scale Smart RFID Applications,” In Proceedings of the 1st International

Conference on Industrial Networks and Intelligent Systems (INISCom), March 2015, Tokyo, Japan.

[25] Mohammad Fal Sadikin, Marcel Kyas, “Efficient Security and Privacy Protection for Emerging Smart RFID Communications,” The International Journal of Networked and Distributed Computing (IJNDC), volume-issue: 2-3, pages: 156 – 165, ISSN: 2211-7946, Atlantis Press Paris, July 2014.

[26] Mohammad Fal Sadikin and Marcel Kyas, “Light-weight Key Management Scheme for Active RFID Applications”, EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, ISSN: 2410-0218, Volume: 2, Issue: 5, 2015. DOI: 10.4108/eai.17-9-2015.150286.

[27] Athanasios T. Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips, “Guidelines for securing radio frequency identification (RFID) systems: Recommendations of the national institute of standards and technology,” NIST Special publication 800–98, national institute of standards and technology, technology administration U.S. Department of Commerce. 2007.

[28] Guevara Noubir and Guolong Lin, “Low-power DoS attacks in data wireless LANs and countermeasures,” ACM SIGMOBILE Mobile Computing and Communications Review, Volume 7 Issue 3, Pages 29 - 30, 2003.

[29] Anthony D. Wood, John A. Stankovic, and Sang H. Son, “Denial of service in sensor networks,” IEEE Computer, 35(10):54–62, October 2002.

[30] Anthony D. Wood, John A. Stankovic, and Sang H. Son, “JAM: A jammed-area mapping service for sensor networks,” In 24th IEEE Real-Time Systems Symposium, pages 286 – 297, 2003.

[31] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc '05), Pages 46 – 57, 2005.

[32] Yee Wei Law, Pieter Hartel, Jerry den Hartog and Paul Havinga, “Link-layer jamming attacks on S-MAC” in 2nd European Workshop on Wireless Sensor

Networks (EWSN 2005). IEEE, pp. 217-225, 2005. [Online]. Available: http://ieeexplore.ieee.org/iel5/9875/31391/01462013.pdf

[33] Yee Wei Law, Lodewijk van Hoesel, Jeroen Doumen, Pieter Hartel and Paul Havinga, “Energy Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols”, in The Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), ACM Press, 2005.

[34] Ziv Kfir and Avishai Wool, “Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems,” Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM '05), Pages 47-58, 2005.

[35] Gerhard P. Hancke, “Practical Attacks on Proximity Identification Systems,” available at: http://www.library.ca.gov/crb/rfidap/docs/Hancke-practicalattacksonproximityIDsystems.pdf. Accessed February 2015.

[36] Gerhard P. Hancke, “A Practical Relay Attack on ISO 14443 Proximity Cards,” available at: http://www.rfidblog.org.uk/hancke-rfidrelay.pdf. Accessed February 2015.

[37] P. Thevenon, O. Savry, and S. Tedjini, “On the weakness of contactless systems under relay attacks,” In Proceeding of the 19th international conference on software, telecommunications and computer networks (SoftCOM 2011), Split, Croatia (pp. 1–5). 2011.

[38] Aurelien Francillon, Boris Danev, and Srdjan Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” In Proceedings of the 18th annual network and distributed system security symposium (NDSS 2011), San Diego. USA: California. 2011.

[39] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis, “Practical NFC peer-to-peer relay attack using mobile phones,” In S. B. Ors Yalcin (Ed.), LNCS: Vol. 6370. Radio frequency identification: security and privacy issues (RFIDSec 2010) (pp. 35–49). Heidelberg: Springer. 2010.

[40] Kin Seong Leong, Mun Leng Ng and Peter H. Cole, “Positioning Analysis of Multiple Antennas in a Dense RFID Reader Environment,” International

Symposium on Applications and the Internet Workshops, 2006. SAINT Workshops 2006., vol., no., pp.4 pp.,59, 23-27 Jan. 2006. doi: 10.1109/SAINT-W.2006.32.

[41] Hsi-Tseng Chou, Chien-Te Yu, Kai-Te Wang, and Paolo Nepa, "A Simple Design of Patch Antenna Array With an Optimized Field Distribution in the Near-Zone for RFID Applications," Antennas and Wireless Propagation Letters, IEEE , vol.13, no., pp.257,260, 2014. doi: 10.1109/LAWP.2014.2303159.

[42] Renato Ferrero, Filippo Gandino, Bartolomeo Montrucchio, Mauruzio Rebaudengo, "A Fair and High Throughput Reader-to-Reader Anticollision Protocol in Dense RFID Networks," IEEE Transactions on Industrial Informatics, vol.8, no.3, pp.697,706, Aug. 2012. doi: 10.1109/TII.2011.2176742.

[43] G. P. Hancke, and M. Kuhn, "An RFID distance bounding protocol," In Proceedings of the 1st international conference on security and privacy for emergent areas in communications networks (SecureComm 2005), Athens, Greece (pp. 67–73). 2005.

[44] G. Avoine, M. A. Bingöl, S. Karda¸s, C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," Journal of Computer Security Special Issue on RFID Security (RFIDSec 2010), 19(2), 289–317. doi:10.3233/JCS-2010-0408. 2010.

[45] G. P. Hancke, "Design of a secure distance-bounding channel for RFID," Journal of Network and Computer Applications, 34(3), 877–887, 2011.

[46] G. Avoine, and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement," In P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna (Eds.), LNCS: Vol. 5735. Information security (ISC 2009) (pp. 250–261). Heidelberg: Springer. 2009.

[47] D. H. Yum, J. S. Kim, S. J. Hong, and P. J. Lee, "Distance bounding protocol with adjustable false acceptance rate," IEEE Communications Letters, 15(4), 434–436.

[48] C. H. Kim, G. Avoine, "RFID distance bounding protocols with mixed challenges," IEEE Transactions on Wireless Communications, 10(5), 1618–1626, 2011.

[49] H. Jannati, and A. Falahati, "Mutual implementation of predefined and random challenges over RFID distance bounding protocol," In Proceedings of the 9th

international conference on information security and cryptology (ISCISC 2012), Tabriz, Iran (pp. 43–47), 2012.

[50] Lee, S., Kim, J. S., Hong, S. J., & Kim, J. (2012). Distance bounding with delayed responses. IEEE Communications Letters, 16(9), 1478–1481.

[51] Kardas, S., Kiraz, M. S., Bingöl, M. A., & Demirci, H. (2012). A novel RFID distance bounding protocol based on physically unclonable functions. In A. Jules & C. Paar (Eds.), LNCS: Vol. 7055. RFID security and privacy (RFIDsec 2012) (pp. 78–93). Heiledberg: Springer.

[52] Kim, J. S., Cho, K., Yum, D. H., Hong, S. J., & Lee, P. J. (2012). Lightweight distance bounding protocol against relay attacks. IEIEC Transactions on Information and Systems, E95-D(4), 1155–1158, doi:10.1587/transinf.E95.D.1155.

[53] Gürel, A. Ö., Arslan, A., & Akgün, M. (2011). Non-uniform stepping approach to RFID distance bounding problem. In J. Garcia-Alfaro, G. Navarro-Arribas, A. Cavalli, & J. Leneutre (Eds.), LNCS: Vol. 6514. Data privacy management and autonomous spontaneous security (DPM 2011) (pp. 64–78). New York: Springer.

[54] Capkun, S., Buttyán, L., & Hubaux, J. P. (2003). SECTOR: Secure tracking of node encounters in multi-hop wireless networks. In Proceedings of the 1th ACM workshop on security of ad hoc and sensor networks, Fairfax, Virginia, USA (pp. 21–32).

[55] Yum, D. H., Kim, J. S., Hong, S. J., & Lee, P. J. (2011). Distance bounding protocol for mutual authentication. IEEE Transactions on Wireless Communications, 10(2), 592–601.

[56] Avoine, G., & Kim, C. H. (2013). Mutual distance bounding protocols. IEEE Transactions on Mobile Computing, 12(5), 830–839.

[57] Cremers, C., Rasmussen, K. B., & Capkun, S. (2012). Distance hijacking attacks on distance bounding protocols. In Proceedings of IEEE symposium on security and privacy (SP 2012), Can Francisco, CA, USA (pp. 113–127).

[58] Desmedt, Y. (2006). Major security problems with the “unforgeable” (Feige-)Fiat-Shamir proofs for identity and how to overcome them. In Proceedings of the 6th

worldwide congress on computer and communications security and protection (Securicomm’88), March 1988 (pp. 141–159). Paris, France.

[59] Reid, J., Gonzalez Nieto, J. M., Tang, T., & Senadji, B. (2007). Detecting relay attacks with timing-based protocols. In Proceedings of the 2nd ASIAN symposium on information, computer and communications security, Singapore (pp. 204–213). New York: ACM.

[60] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, “JAID: An Algorithm for Data Fusion and Jamming Avoidance on Distributed Sensor Networks”, Pervasive and Mobile Computing, in press.

[61] Rajani Muraleedharan and Lisa Osadciw, “Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System”, 2006 SPIE Symposium on Defense and Security, Orlando, FL, April, 2006.

[62] W. Xu, K. Ma, W. Trappe, Y. Zhang, “Jamming sensor networks: attack and defense strategies”, IEEE Network Magazine, vol. 20, pp. 41-47, 2006.

[63] W. Xu, T. Wood, W. Trappe, and Y. Zhang.“Channel surfing and spatial retreats: defenses against wireless denial of service”, in WiSe ’04: Proc. 2004 ACM workshop on Wireless security, NY, USA, pp. 80-89, 2004.

[64] W. Xu, W. Trappe, Y. Zhang, T. Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, in Proc. 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57, 2005.

[65] Mingyan Li; Koutsopoulos, I.; Poovendran, R., “Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks”, INFOCOM 2007. 26th IEEE International Conference on Computer Communications, pp.1307-1315, 6-12 May 2007.

[66] A. Mpitziopoulos, D. Gavalas, G. Pantziou and C. Konstantopoulos, “Defending Wireless Sensor Networks From Jamming Attacks”, in Proc. 18th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’2007), September 2007.

[67] Swaminathan Sankararaman, Karim Abu-Affash, Alon Efrat, Sylvester David Eriksson-Bique, Valentin Polishchuk, Srinivasan Ramasubramanian and Michael

Segal, Optimization schemes for protective jamming, Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '12), Pages 65-74, 2012.

[68] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service, Proceedings of the 2004 ACM workshop on Wireless security (WiSe ’04), pages 80–89, 2004.

[69] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In 7th ACM Symposium on Information, Computer, and Communications Security (AsiaCCS), May 2012.

[70] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin. Wireless secrecy regions with friendly jamming. Information Forensics and Security, IEEE Transactions on, 6(2):256–266, June 2011.

[71] European Digital Rights (EDRI-gram) (2006). Cloning an electronic passport. EDRI-gram, digital civil rights in Europe. http://history.edri.org/edrigram/number4.16/epassport. Accessed February 2015.

[72] Juels, A.; Molnar, D.; Wagner, D., "Security and Privacy Issues in E-passports," Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on , vol., no., pp.74,88, 05-09 Sept. 2005. doi: 10.1109/SECURECOMM.2005.59

[73] Luca Calderoni, Dario Maio, Cloning and tampering threats in e-Passports, Expert systems with applications Volume 41, Issue 11, 1 September 2014, Pages 5066–5070, doi:10.1016/j.eswa.2014.02.044

[74] Laurie, A. (2007). Practical attacks against RFID. Network Security, 9, 4–7.

[75] Auletta, V., Blundo, C., Caro, A. D., Cristofaro, E. D., Persiano, G., & Visconti, I. (2010). Increasing privacy threats in the cyberspace: The case of italian e-passports. In R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, & K. Sako, et al. (Eds.), Financial cryptography workshops. Lecture notes in computer science (Vol. 6054, pp. 94–104). Springer.

[76] Avoine, G., Kalach, K., & Quisquater, J.-J. (2008). ePassport: Securing international contacts with contactless chips. In G. Tsudik (Ed.), Financial

cryptography. Lecture notes in computer science (Vol. 5143, pp. 141–155). Springer.

[77] Chothia, T., & Smirnov, V. (2010). A traceability attack against e-passports. In R. Sion (Ed.), Financial cryptography. Lecture notes in computer science (Vol. 6054, pp. 20–34). Springer.

[78] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical One-Way Functions, Science Vol. 297, (2002), 2026-2030.

[79] R. Pappu, Physical One-Way Functions, Ph.D. thesis, MIT 2001.

[80] Pim Tuyls, Boris Škorić, "Secret key generation from classical physics, Physical Uncloneable Functions," AmIware Hardware Technology Drivers of Ambient Intelligence, Philips Research Volume 5, 2006, pp 421-447.

[81] Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum, "Classifying RFID attacks and defenses," Information Systems Frontiers, November 2010, Volume 12, Issue 5, pp 491-505.

[82] P. Tuyls, B. Skoric, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information theoretical security analysis of physical unclonable functions. In A.S. Patrick and M. Yung, editors, Proceedings of 9th Financial Cryptography and Data Security Conference, volume 3570 of Lecture Notes in Computer Science, pages 141–155. Springer-Verlag, 2005.

[83] B. Skoric, P. Tuyls, and W. Ophey. Robust key extraction from physical unclonable functions. In J. Ionnidis, A.D. Keromytis, and M. Yung, editors, Proceedings of the Applied Cryptography and Network Security Conference 2005, volume 3531 of Lecture Notes in Computer Science, pages 407–422. Springer-Verlag, 2005.

[84] Quan, C. H., Hong, W. K., & Kim, H. C. (2006). Performance analysis of tag anti-collision algorithms for RFID systems. In Emerging directions in embedded and ubiquitous computing, proceedings of EUC 2006 workshops: NCUS, SecUbiq, USN, TRUST, ESO, and MSA, Seoul, Korea, August 1–4 , 2006. Lecture notes in computer science, information systems and applications, incl. Internet/Web, andHCI (Vol. 4097, pp. 382–391). Berlin: Springer. doi:10.1007/11807964.

[85] Weis, S. A. (2003) Security and privacy in radio-frequency identification devices. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

[86] Weis, S., Sarma, S., Rivest, R., & Engels, D. (2003). Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan,&M.Ullmann (Eds.), Security in pervasive computing, proceedings of the 1st international conference in security in pervasive computing, boppard, Germany, March 12–14, 2003. Lecture notes in computer science (Vol. 2802, pp. 201–212). Berlin: Springer. doi:10.1007/b95124.

[87] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, Cryptographic approach to "privacyfriendly" tags. RFID Privacy Workshop, MIT, MA, USA, November 2003.

[88] E. Biham, R. Chen, Near collision for SHA-0, Advances in Cryptology, Crypto'04, 2004, LNCS 3152, pp. 290-305.

[89] F. Chabaud, A. Joux. Differential collisions in SHA-0, Advances in Cryptology, Crypto'98 Proceedings, Springer-Verlag, 1998.

[90] A. Joux. Collisions for SHA-0, rump session of Crypto'04, 2004.

[91] Wang X Y, Yu H B. How to break MD5 and other hash functions, Advances in Cryptology, EUROCRYPT 2005, LNCS 3494. Berlin: SpringerVerlag, 2005: 19-35.

[92] R.L. Rivest. The MD4 message digest algorithm, Advances in Cryptology, Crypto'90, Springer-Verlag, 1991, 303-311.

[93] Y.L. Zheng, J. Pieprzyk, J. Seberry. HAVAL–A one-way hashing algorithm with variable length of output, Advances in Cryptology, Auscrypt'92 Proceedings, Springer-Verlag.

[94] RIPE. Integrity Primitives for Secure Information Systems. Final Report of RACE Integrity Primitives Evaluation (RIPE-RACE 1040), LNCS 1007, Springer-Verlag, 1995.

[95] Wang X Y, Lai X J, Feng D G, et al. Cryptanalysis of the hash functions MD4 and RIPEMD, Advances in Cryptology, EUROCRYPT 2005, LNCS 3494. Berlin: Springer-Verlag, 2005: 1-18.

[96] Wang X Y, Feng D G, Yu X Y. An attack on hash function HAVAL-128, Science in China Series F: Information Sciences, 2005, 48(5): 545-556.

[97] Wang X Y, Yu H B, Yin Y Q L. Efficient collision search attacks on SHA-0, Advances in Cryptology, CRYPTO 2005, LNCS 3621. Berlin: Springer-Verlag, 2005: 1-16.

[98] Wang X Y, Yin Y Q, Yu H B. Finding collisions in the full SHA-1, Advances in Cryptology, CRYPTO 2005, LNCS 3621. Berlin: Springer-Verlag, 2005: 17-36.

[99] Van ROMPAY B, Biryukov A, Preneel B, Cryptanalysis of 3-pass HAVAL, Advances in Cryptology, ASIACRYPT 2003, LNCS 2894. Berlin: Springer-Verlag, 2003: 228-245.

[100] Yu H B, Wang X Y, Yun A, et al. Cryptanalysis of the full HAVAL with 4 and 5 passes, Fast Software Encryption 2006, LNCS 4047. Berlin: Springer-Verlag, 2006: 89-110.

[101] Suzuki K, Kurosawa K. How to find many collisions of 3-pass haval, Second International Workshop on Security, IWSEC 2007, LNCS 4752. Berlin: Springer-Verlag, 2007: 428-443.

[102] Yu H B, Wang X Y. Multi-collision attack on the compression functions of MD4 and 3-pass HAVAL, Information Security and Cryptology, ICISC 2007, LNCS 4817. Berlin: Springer-Verlag, 2007: 206-226.

[103] Lee E, Chang D, Kim J, et al. Second preimage attack on 3-pass HAVAL and partial key recovery attacks on HMAC/NMAC-3-pass HAVAL, Fast Software Encryption 2008, LNCS 5086. Berlin: Springer-Verlag, 2008: 189-206.

[104] Yu H B, Wang G L, Zhang G Y, et al. The second preimage attack on MD4, Cryptology and Network Security (CANS) 2005, LNCS 3810. Berlin: Springer-Verlag, 2005: 1-12.

[105] Wang G L, Wang S H. Second preimage attack on 5-pass HAVAL and partial key-recovery attack on HMAC/NMAC-5-pass HAVAL, Progress in Cryptology, AFRICACRYPT 2009, LNCS 5580. Berlin: Springer-Verlag, 2009: 1-13.

[106] Aoki K, Guo J, Matusiewicz K, et al. Preimages for step-reduced SHA-2, Advances in Cryptology, ASIACRYPT 2009, LNCS 5912. Berlin: SpringerVerlag, 2009: 578-597.

[107] Sasaki Y, Aoki K. Finding preimages in full MD5 faster than exhaustive search, Advances in Cryptology, EUROCRYPT 2009, LNCS 5479. Berlin: Springer-Verlag, 2009: 134-152.

[108] Leurent G. MD4 is not one-way, Fast Software Encryption 2008, LNCS 5086. Berlin: Springer-Verlag, 2008: 412-428.

[109] Sasaki Y. Meet-in-the-middle attacks using output truncation in 3-pass HAVAL, Information Security (ISC) 2009, LNCS 5735. Berlin: Springer-Verlag, 2009: 79-94.

[110] Aumasson J P, Meier W, Mendel F. Preimage attacks on 3-pass HAVAL and step-reduced MD5, Selected Areas in Cryptography 2008, LNCS 5381. Berlin: Springer-Verlag, 2009: 120-135.

[111] Sasaki Y, Aoki K. Preimage attacks on 3, 4, and 5-pass HAVAL, Advances in Cryptology, ASIACRYPT 2008, LNCS 5350. Berlin: SpringerVerlag, 2008: 253-271.

[112] Isobe T, Shibutani K. Preimage attacks on reduced tiger and SHA-2, Fast Software Encryption 2009, LNCS 5665. Berlin: Springer-Verlag, 2009: 139-155.

[113] Aoki K, Sasaki Y. Meet-in-the-middle preimage attacks against reduced SHA-0 and SHA-1, Advances in Cryptology, CRYPTO 2009, LNCS 5677. Berlin: Springer-Verlag, 2009: 70-89.

[114] Guo J, Ling S, Rechberger C, et al. Advanced meet-in-the-middle preimage attacks: First results on full tiger, and improved results on MD4 and SHA-2, Advances in Cryptology, ASIACRYPT 2010, LNCS 6477. Berlin: Springer-Verlag, 2010: 56-75.

[115] Zhong J M, Lai X J. Improved preimage attack on one-block md4 [EB/OL]. (2011-07-01). http://eprint.iacr.org/2010/583.pdf.

[116] Aoki K, Sasaki Y. Preimage attacks on one-block MD4, 63-step MD5 and more, Selected Areas in Cryptography 2008, LNCS 5381. Berlin: SpringerVerlag, 2009: 103-119.

[117] Juha Kortelainen, Kimmo Halunen and Tuomas Kortelainen, Multicollision attacks and generalized iterated hash functions, Journal: Journal of Mathematical Cryptology, 2010, Volume 4, Number 3. DOI: 10.1515/jmc.2010.010

[118] Lei WANG, Kazuo OHTA, Yu SASAKI, Kazuo SAKIYAMA and Noboru KUNIHIRO, Cryptanalysis of Two MD5-Based Authentication Protocols: APOP and NMAC, Journal: IEICE Transactions on Information and Systems, 2010, Volume E93-D, Number 5, Page 1087. DOI: 10.1587/transinf.E93.D.1087

[119] Jin-min Zhong, Xue-jia Lai and Ming Duan, Improved preimage attack on 3-pass HAVAL, Journal: Journal of Shanghai Jiaotong University (Science), 2011, Volume 16, Number 6, Page 713. DOI: 10.1007/s12204-011-1215-3.

[120] Antoine Joux, Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions, Advances in Cryptology – CRYPTO 2004, Lecture Notes in Computer Science Volume 3152, 2004, pp 306-316.

[121] Jie Liang, Xue-Jia Lai, Improved Collision Attack on Hash Function MD5, Journal of Computer Science and Technology, January 2007, Volume 22, Issue 1, pp 79-87.

[122] Jonathan J. Hoch, Adi Shamir, Breaking the ICE – Finding Multicollisions in Iterated Concatenated and Expanded (ICE) Hash Functions, Fast Software Encryption, Lecture Notes in Computer Science Volume 4047, 2006, pp 179-194.

[123] Ioanna Stamouli, Patroklos G. Argyroudis, Hitesh Tewari, "Real-time intrusion detection for ad hoc networks," Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. , vol., no., pp.374,380, 13-16 June 2005. doi: 10.1109/WOWMOM.2005.85

[124] Yih-Chun Hu, Adrian Perrig and David B. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, Journal of Wireless Networks, Volume 11 Issue 1-2, January 2005, Pages 21-38, Kluwer Academic Publishers Hingham, MA, USA.

[125] Sencun Zhu, Shouhuai Xu, Sanjeev Setia and Sushil Jajodia, "LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks," In proceeding of the 23rd International Conference on Distributed Computing Systems Workshops, 2003. Vol., no., pp.749,755, 19-22 May 2003. doi: 10.1109/ICDCSW.2003.1203642.

[126] Gildas Avoine, Privacy issues in RFID banknote protection schemes. Smart Card Research and Advanced Applications VI, IFIP International Federation for Information Processing Volume 153, 2004, pp 33-48.

[127] Ari Juels and Ravikanth Pappu, Squealing euros: Privacy protection in RFID-enabled banknotes. In Financial Cryptography – FC'03, LNCS, Springer, 2003.

[128] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael Wiener, editor, Advances in Cryptology – CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 537–554, Santa Barbara, California, USA, August 1999. IACR, Springer-Verlag.

[129] David Molnar and David Wagner, Privacy and security in library RFID: Issues, practices, and architectures. Proceedings of the 11th ACM conference on Computer and Communications Security – CCS, ACM Press, 2004.

[130] Gildas Avoine and Philippe Oechslin, RFID traceability: A multilayer problem. Financial Cryptography and Data Security, Lecture Notes in Computer Science Volume 3570, 2005, pp 125-140.

[131] Meg McGinity, RFID: Is This Game of Tag Fair Play?, Communications of the ACM, Vol. 47 No. 1, Pages 15-18, 2004.

[132] Roy Want, RFID: A key to automating everything, Scientific American, 290 (1), 56-65, 2004.

[133] Aaron Weiss, Me and My Shadow, ACM netWorker, 7(3):24-30, 2003.

[134] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "RFID malware: truth vs. myth," Security & Privacy, IEEE , vol.4, no.4, pp.70,72, July-Aug. 2006. doi: 10.1109/MSP.2006.102

[135] Melanie R. Rieback, Patrick N.D. Simpsona, Bruno Crispoa, Andrew S. Tanenbauma, "RFID malware: Design principles and examples Pervasive and

Mobile Computing," Volume 2, Issue 4, November 2006, Pages 405–426, Special Issue on PerCom 2006.

[136] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," Fourth Annual IEEE International Conference on Pervasive Computing and Communications, 2006. PerCom 2006., vol., no., pp.10 pp.,179, 13-17 March 2006. doi: 10.1109/PERCOM.2006.32.

[137] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "RFID Guardian: A battery-powered mobile device for RFID privacy management," In C. Boyd, N. González, & M. Juan (Eds.), Information security and privacy, proceedings of the 10th Australasian conference on information security and privacy (ACISP '05), Brisbane, Australia, July 4–6, 2005. Lecture notes in computer science, security and cryptology (Vol. 3574, pp. 184–194). Berlin: Springer.

[138] Ari Juels, Paul Syverson, and Dan Bailey, "High-power proxies for enhancing RFID privacy and utility," Privacy Enhancing Technologies, Lecture Notes in Computer Science Volume 3856, 2006, pp 210-226, 2005.

[139] Ari Juels, "RFID Security and Privacy: A Research Survey," Selected Areas in Communications, IEEE Journal on , vol.24, no.2, pp.381,394, Feb. 2006. doi: 10.1109/JSAC.2005.861395.

[140] Kinoshita, Shingo, Fumitaka Hoshino, Tomoyuki Komuro, Akiko Fujimura, and Miyako Ohkubo. "Low-cost RFID privacy protection scheme." IPS Journal Transactions of information processing society of Japan 45, no. 8 (2004): 2007-2021.

[141] Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," In M. Joye & J.-J. Quisquater (Eds.), Cryptographic hardware and embedded systems - CHES 2004. Proceedings of the 6th international workshop on cryptographic hardware and embedded systems (CHES'04). Lecture notes in computer science (Vol. 3156, pp. 357–370). Berlin: Springer. doi:10.1007/b99451.

[142] Tassos Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks," In Proceedings of the 1st international conference on security and

privacy for emerging areas in communication networks (SecureComm’05) (pp. 59–66). Las Vegas: IEEE Computer Society.

[143] Sebastian Zander, Grenville Armitage, Philip Branch, “A survey of covert channels and countermeasures in computer network protocols,” Communications Surveys & Tutorials, IEEE , vol.9, no.3, pp.44,57, Third Quarter 2007, doi: 10.1109/COMST.2007.4317620.

[144] Daniel V. Bailey, Dan Boneh and Eu-Jin Goh, and Ari Juels, “Covert Channels in Privacy-Preserving Identification Systems,” Proceedings of the 14th ACM conference on Computer and communications security, Pages 297-306, CCS '07.

[145] T. Scott Saponas, Jonathan Lester, Carl Hartung, Tadayoshi Kohno, “Devices that tell on you: The Nike+iPod sport kit,” Technical Report 2006-12-06, University of Washington, 2006.

[146] Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs, “Dismantling MIFARE classic,” In Proceedings of the 13th European symposium on research in computer security, Malaga, Spain. Lecture notes in computer science (Vol. 5283, pp. 97–114). Berlin: Springer.

[147] C. H. Gebotys, C. C. Tiu, and X. Chen, “A countermeasure for EM attack of a wireless PDA,” In ITCC ’05: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC’05) - Volume I, pages 544–549, Washington, DC, USA, 2005, IEEE Computer Society.

[148] Katsuyuki Okeya and Tetsu Iwata, “Side Channel Attacks on Message Authentication Codes,” In the Proceedings of the Second European conference on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS'05), Pages 205-217.

[149] A. Berendschot, B. den Boer, J. P. Boly, A. Bosselaers, J. Brandt, D. Chaum, I. Damg˚ard, M. Dichtl, W. Fumy, M. van der Ham, C. J. A. Jansen, P. Landrock, B. Preneel, G. Roelofsen, P. de Rooij, and J. Vandewalle. “Final Report of RACE Integrity Primitives. ” LNCS 1007, 1995.

[150] Tetsu Iwata and Kaoru Kurosawa, “OMAC: One-Key CBC MAC,” FSE 2003, LNCS 2887, pp. 129–153, 2003.

[151] J. Black and P. Rogaway, “A Block-Cipher Mode of Operation for Parallelizable Message Authentication,” EUROCRYPT 2002, LNCS 2332, pp. 384–397.

[152] Kanthakumar Pongaliur, Zubin Abraham, Alex X. Liu, Li Xiao, and Leo Kempel, “Securing Sensor Nodes Against Side Channel Attacks,” High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE , vol., no., pp.353,361, 3-5 Dec. 2008.

[153] Zoya Dyka and Peter Langendörfer, “Improving the Security of Wireless Sensor Networks by Protecting the Sensor Nodes against Side Channel Attacks,” Wireless Networks and Security Signals and Communication Technology 2013, pp 303-328.

[154] Yuval Ishai, Amit Sahai, and David Wagner, “Private circuits: Securing hardware against probing attacks,” In Proceedings of CRYPTO, pages 463–481, 2003.

[155] Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner, “Private circuits 2: Keeping secrets in tamperable circuits,” In Proceedings of Eurocrypt, pages 308–327, May 2006.

[156] Benoit Chevallier-Mames, Mathieu Ciet, and Marc Joye, “Low-cost solutions for preventing simple side-channel analysis: Sidechannel atomicity,” volume 53, pages 760–768, Los Alamitos, CA, USA, 2004. IEEE Computer Society.

[157] Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang, “An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks,” IEEE Global Telecommunications Conference (GLOBECOM '07), 2007, vol., no., pp.986,990, 26-30 Nov, 2007. doi: 10.1109/GLOCOM.2007.190.

[158] Lingxuan Hu and David Evans, “Secure Aggregation for Wireless Networks,” In Proceeding of SAINT-W '03 Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops).

[159] Chris Karlof, Naveen Sastry, and David Wagner, TinySec: a link layer security architecture for wireless sensor networks, In the Proceedings of the 2nd international conference on Embedded networked sensor systems (SenSys '04), 2004.

[160] Azzedine Boukerche, Horacio A. B. F. Oliveira, Eduardo F. Nakamura, and Antonio A. F. Loureiro, Secure Localization Algorithms for Wireless Sensor

Networks, IEEE Communications Magazine, vol.46, no.4, pp.96,101, April 2008. doi: 10.1109/MCOM.2008.4481347.

[161] Yanfei Fan, Yixin Jiang, Haojin Zhu, Jiming Chen, and Xuemin (Sherman) Shen, “Network Coding Based Privacy Preservation against Traffic Analysis in Multi-hop Wireless Networks,” IEEE Transactions on Wireless Communications, vol.10, no.3, pp.834,843, March 2011. doi: 10.1109/TWC.2011.122010.100087.

[162] Jing Deng, Richard Han, and Shivakant Mishra, “Decorrelating Wireless Sensor Network Traffic To Inhibit Traffic Analysis Attacks,” Elsevier Pervasive and Mobile Computing Journal, Special Issue on Security in Wireless Mobile Computing Systems, vol 2, issue 2, April 2006, pp. 159-186.

[163] Jing Deng, Richard Han, and Shivakant Mishra, “Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks,” In Proceedings of the 2004 International Conference on Dependable Systems and Networks (DSN '04).

[164] Adi Shamir, “Identity based cryptosystems and signatures. In Proceedings of Cryptology (Berlin, Germany, 1984),” Springer-Verlag, pp. 47-53.

[165] G. Frey, M. Muller, and H. Rück, “The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems”, IEEE Transactions on Information Theory 45(5) (1999), pp. 1717–1719.

[166] X. Xiong, D. Wong, X. Deng, “Tinypairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks,” IEEE Wireless Communications and Networking Conference (WCNC), 2010, pp. 1–6.

[167] Martijn Maas, “Pairing-Based Cryptography,” Master Thesis, Technische Universiteit Eindhoven, 2004.

[168] J.-L. Beuchat, E. Lpez-Trejo, L. Martnez-Ramos, S. Mitsunari, F. Rodrguez-Henrquez, “Multi-core implementation of the tate pairing over supersingular elliptic curves,” Proceedings of the 8th International Conference in Cryptology and Network Security, 12-14 December, 2009.

[169] P. Szczechowiak, M. Collier, Tinyibe: Identity-based encryption for heterogeneous sensor networks, in: 5th International Conference on Intelligent Sensors, Sensor Networks, and Information Processing (ISSNIP), 2009, pp. 319–354.

[170] Christof Paar and Jan Pelzl, Understanding Cryptography A Textbook for Students and Practitioners, Springer, 2010. ISBN: 978-3-642-44649-8.

[171] V. Kolesnikov, G.S. Sundaram, “IBAKE: Identity-Based Authenticated Key Exchange Protocol, IACR Cryptology ePrint Archive,” 2011.

[172] Vladimir Kolesnikov and Charles Rackoff, Key exchange using passwords and long keys. In Theory of Cryptography, TCC 2006, volume 3876 of LNCS, pages 100-119. Springer, 2006.

[173] Vladimir Kolesnikov and Charles Rackoff. Password mistyping in two-factor-authenticated key exchange. In ICALP (2), pages 702-714, 2008.

[174] V. Cakulev, G. Sundaram, and I. Broustis, “IBAKE: Identity-Based Authenticated Key Exchange,” RFC 6539, March 2012.

[175] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.

[176] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," In Proc. of EUROCRYPT 04, LNCS 3027, pp. 223-238, 2004.

[177] V. Cakulev and I. Broustis, “An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange,” draft-cakulev-emu-eap-ibake-03.txt, August 2012, work in progress.

[178] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, “Extensible Authentication Protocol (EAP),” Request for Comments: 3748, June 2004.

[179] C. Ellison, and B. Schneier, “Ten risks of PKI: what you're not being told about public key infrastructure,” Computer Security Journal, v 16, n 1, 2000, pp. 1-7.

[180] E. Rescorla, M. Ray, S. Dispensa, N. Oskov, “Transport layer security (TLS) renegotiation indication extension,” RFC 5746. 2010.

[181] C. Mulkey, D. Kar, A. Katangur, “Towards an Efficient Protocol for Privacy and Authentication in Wireless Networks,” The 12th International Conference on Security and Management (SAM'13), July 2013.

[182] Carl Ellison and Bruce Schneier, “Ten risks of PKI: What you’re not being told about public key infrastructure,” Computer Security Journal, 16(1):1–7, 2000.

[183] R. Holz, T. Riedmaier, N. Kammenhuber, and G. Carle, "X.509 forensics: detecting and localising the SSL/TLS men-in-the-middle," In Proc. 17th ESORICS 2012, volume 7459/2012 of LNCS, pages 217-234, Pisa, Italy, September 2012. Springer Verlag.

[184] Y. Suga, "Countermeasures and tactics for transitioning against the SSL/TLS renegotiation vulnerability," In Proc. 6th IMIS, 2012, vol., no., pp.656-659, 4-6 July 2012.

[185] Gora Adj, Alfred Menezes, Thomaz Oliveira, Francisco Rodríguez-Henríquez, "Weakness of $F_{3^{509.6}}$ for Discrete Logarithm Cryptography," Pairing-Based Cryptography – Pairing 2013. Lecture Notes in Computer Science Volume 8365, 2014, pp 20-44.

[186] Antoine Joux, "A new index calculus algorithm with complexity L(1/4 + o(1)) in small characteristic," In T. Lange, K. Lauter, and P. Lisonek, editors, Proceedings of SAC '13, LNCS, pages 355–379. Springer, 2013.

[187] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, Emmanuel Thomé, "A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic: Improvements over FFS in small to medium characteristic," Advances in Cryptology – EUROCRYPT 2014, LNCS 8441 (2014), 1–16.

[188] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-friendly elliptic curves of prime order. In B. Preneel and S. Tavares, editors, SAC 2005, number 3897 in Lecture Notes in Computer Science, pages 319–331, Berlin Heidelberg, 2006. Springer-Verlag.

[189] Augusto Jun Devegili, Michael Scott, Ricardo Dahab, "Implementing Cryptographic Pairings over Barreto-Naehrig Curves," Pairing-Based Cryptography, Pairing 2007, Lecture Notes in Computer Science Volume 4575, 2007, pp 197-207.

[190] Masaaki Shirase, "Barreto-Naehrig Curve With Fixed Coefficient - Efficiently Constructing Pairing-Friendly Curves," Cryptology ePrint Archive, Report 2010/134.

[191] Jean-Luc Beuchat, Jorge E. González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, Tadanori Teruya, "High-Speed Software Implementation of the Optimal Ate Pairing over Barreto–Naehrig Curves," Pairing-Based Cryptography - Pairing 2010, Lecture Notes in Computer Science Volume 6487, 2010, pp 21-39.

[192] Mohammad Fal Sadikin and Marcel Kyas, "IMAKA-Tate: Secure and Efficient Privacy Preserving for Indoor Positioning Applications", International Journal of Parallel Emergent and Distributed Systems," ISSN: 1744-5760, Taylor & Francis, 2015. (http://dx.doi.org/10.1080/17445760.2015.1058939).

[193] Hai Liu, Miodrag Bolic, Amiya Nayak and Ivan Stojmenovi, "Integration of RFID and wireless sensor networks," In Proceedings of Sense ID 2007 Worksop at ACN SenSys, Sydney, Australia, November 6–9, 2007.

[194] Xiaoyong Su, B.S. Prabhu and Rajit Gadh, "RFID Based General Wireless Sensor Inferface," Technical Report, UCLA (2003).

[195] William Stallings, "Cryptography and Network Security Principles and Practices," 4th edition, Prentice Hall, 2006.

[196] N. Goffee, S. Kim, S.W. Smith, P. Taylor, M. Zhao, and J. Marchesini, "Greenpass: Decentralized, PKI-based Authorization for Wireless LANs," In 3rd Annual PKI Research and Development Workshop, pages 26–41. NIST, April 2004.

[197] R. Oppliger, R. Hauser, and D. Basin, "SSL/TLS session-aware user authentication—OR how to effectively thwart the man-in-the-middle," Comput. Commun., vol. 29, no. 12, pp. 2238–2246, Aug. 2006.

[198] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based Authentication for Secure WLAN-3G Interworking," Proc. IEE Communications, Vol.151, No.5, October 2004, pp. 501- 506.

[199] M. Thompson, A. Essiari, S. Mudumbai, Certificate-based authorization policy in a PKI environment, ACM Trans. Inform. Syst. Secur. 6 (4) (November 2003) 566–588.

[200] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs." Boston, Massachusetts: 6th

International Workshop on Cryptographic Hardware and Embedded Systems, August 2004.

[201] N. Jansma and B. Arredondo. Performance comparison of elliptic curve and rsa digital signatures. Technical report, University of Michigan College of Engineering, April 2004.

[202] Arvinderpal S. Wander, Nils Gura, Hans Eberle, Vipul Gupta and Sheueling Chang Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," PerCom '05: Proc. 3rd IEEE International Conference on Pervasive Computing and Commun., Mar. 2005.