International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

NEAR FIELD COMMUNICATION BASED SECURITY THROUGH CONDITIONAL PRIVACY SEQUENCE METHODOLOGY

D.Prabakaran, M. Indira Kumar
Department of Electronics and Communication Engineering,
Affiliated to Anna University
Chennai-25, India.
prabakaranirt.88@gmail.com indirakmar@gmail.com

ABSTRACT

In recent years, various mobile terminals equipped with NFC (Near Field Communication) have been released. The combination of NFC with smart devices has led to widening the utilization range of NFC. It is expected to replace credit cards in electronic payment, especially. In this regard, security issues need to be addressed to vitalize NFC electronic payment. The NFC security standards currently being applied require the use of user's public key at a fixed value in the process of key agreement. The relevance of the message occurs in the fixed elements such as the public key of NFC. An attacker can create a profile based on user's public key by collecting the associated messages. Through the created profile, users can be exposed and their privacy can be Compromised. In this paper, we propose conditional privacy protection methods based on pseudonyms to solve these problems. In addition, PDU (Protocol Data Unit) for conditional privacy is defined. Users can inform the other party that they will communicate according to the protocol proposed in this paper by sending the conditional privacy preserved PDU through NFC terminals. The proposed method succeeds in minimizing the update cost and computation overhead by taking advantage of the physical characteristics of NFC.

Keywords—NFC security; Pseudonym; Unlinkability; Conditional privacy protection

1. INTRODUCTION

NFC (Near field Communication) is a short-range wireless communication technology whose technology distance is around 4 inches, and it operates in the 13.56MHz frequency band at a speed of 106Kbps to 424Kbps. The combination of NFC with smart devices resulted in widening the range of NFC, which includes data exchange, service discovery, connection, e- payment, and ticketing. It is expected to replacecredit cards in electronic payment, especially. According to Gartner, a market research company, the number of NFC- 1 based payment services is expected to increase by 11.3 times from $316 million in 2010 to $3.572 billion in 2015 , and Juniper research predicted that the global NFC payment market size would be increased to $180 billion in 2017 . To use NFC in electronic payment, security is a prerequisite to be addressed. Presently, NFC security standards define data exchange format, tag types, and security protocols, centering on NFC forum. It is expressly stipulated in the NFC security standards that key agreement is required for secret communications between users . In the process of key agreement, both users should exchange their public keys. The public key is received from CA (Certificate Authority), and it uses a fixed value until reissued.

Malicious internal attackers can create profiles of users through the acquisition of public keys of other users in the process of key agreement. If NFC is used in e-payment in this way, the privacy of users can be infringed through profiles created by attackers. Suppose Alice purchases items such as cloths, food, and medicine several times at a supermarket, the supermarket can get information about her tastes, preferences, and health conditions. The collected information can help her to purchase products more efficiently, but it may contain information that nobody wants to announce to others such as his or her health conditions.

In this paper, we propose privacy protection methods based on pseudonyms to protect privacy of users. The proposed methods provide conditional privacy in which the identity of users can be verified by the TTP (Trusted Third Party) to resolve disputes when necessary. In addition, the PDU (Protocol Data Unit) for the conditional privacy is proposed in this paper. The data used to help a future purchase uses protected PDU of NFC-SEC, and data not wanted to

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

be recorded uses conditional privacy PDU selectively, which makes it possible to remove the connectivity with the existing messages. It covers background, security requirements, and differences between pseudonym-based method and the proposed method. According to survey conducted so far, this paper has its significance in the sense it is the first research on the conditional privacy protection of users in NFC.

I. NFC STANDARDS AND PRIVACY METHODS

In this section, the current NFC standards are introduced, and the pseudonyms are also introduced as conditional privacy protection methods. In the current NFC standards, a variety of Standards ranging from the basic interface protocols to testing and security methods are defined. This section also introduces NFCIP-1, the basic interface and NFC-SEC, the security method.

A. *NFCIP-1:Near Field Communication Interface and Protocol*

In NFC, the object of communication is divided into an initiator and a target. An initiator generates RF field (Radio Frequency field) and starts NFCIP-1. A target that receives signals from initiator responds to the initiator through the RF field. When target communicates using RF field of initiator, it is called passive communication mode, and using self generated RF field is referred to as active communication mode. Communication mode is determined according to applications when transaction starts. Once the transaction is started, the communication mode cannot be changed until the target becomes disabled or removed.

The major mechanism provided by NFCIP-1 is SDD (Single Device Detection) and RFCA (Radio Field Collision Avoidance) .The SDD is an algorithm for initiator to find a specific target among multiple targets in the RF field. In existing RFID system, collision problem may occur. The collision is referred to as a state in which more than two initiators or targets transmit data at the same time, and it is impossible to distinguish which data is real. The collision problem is solved by NFC standard using algorithm named RFCA. RFCA is an algorithm that detects other RF fields and prevents collision using carrier frequency. RFCA begins by confirming the presence of other RF fields. If other RF fields exist, the NFC does not generate its own RF field. Thanks to the SDD that finds specific target within the range and RFCA that does not permit 2 RF fields, the NFC can be safe from MITM (Man-In-The-Middle) attacks. The detailed information about this is discussed in section IV-D.

B. *NFC-SEC: NFCIP-1 Security Services and Protocol*

NFC-SEC defines SSE (Shared SEcret service) and SCH (Secure CHannel service) for NFCIP-1. SSE generates a secret key for secure communication between NFC devices and in this process, key agreement and key confirmation is performed. SCH service provides the communication between

NFC devices with confidentiality and integrity using a key generated through SSE service. Also NFC-SEC defines the procedures of key agreement using ECSDVP-DH (Elliptic Curve Secret Value Derivation Primitive, Diffie-Hellman version) for SCH between NFC terminals in SSE. To achieve the above, NFC terminal must have public key and private key based on Elliptic curve. SCH makes three keys hierarchically by using the key generated through SSE and provides confidentiality and integrity to the messages using generated keys. The three keys created in SCH are used to provide the confidentiality and integrity of the message. The key agreement and confirmation protocols are implemented as shown in Figure 2, and the notation follows Table I.

Table 1

Protocol Notations and descriptions		
Index	***Notation***	***Description***
1	$\|\|$	Concatenation symbol
2	N	Nonce of user X
3	IDX	Random ID of user X for the activation of transport protocols
4	QX, QX', QX	Compressed elliptic curve public key of user X
5	$QX, Q'X, Q''X$	Elliptic curve public key of user X
6	dX	Elliptic curve private key of user X
7	G	Elliptic curve base point
8	KDF	Key derivation function
9	$MacTagX$	Key verification tag received from X
10	MK	Shared secret key
11	z	Unsigned integer
12	rX	Random integer generated by user X
13	PN	Pseudonym set
14	$Enc(k, m)$	Encrypt m with k

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

Protocol Notations and descriptions		
Index	***Notation***	***Description***
15	*Sig*(*k*, *m*)	Signature on *m* with *k*

a.

b. *IDx followsNFCID format.*

c. *NFCID generated dynamically and used in SDD and RFCA.*

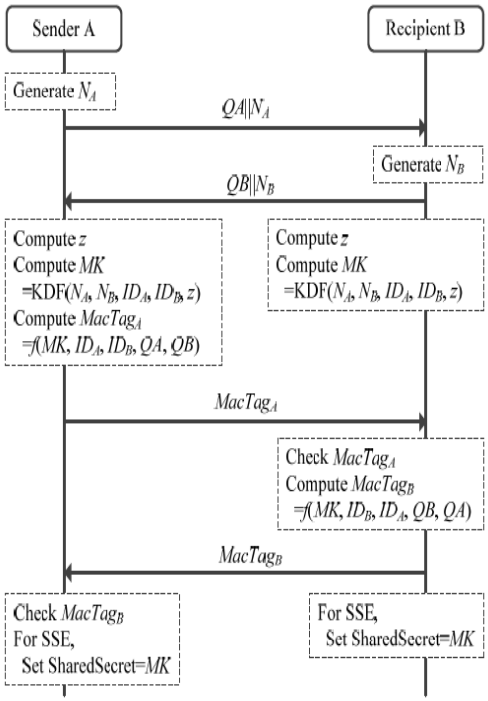


Figure. 1Key agreement and confirmation protocol for NFC-SEC

User *A* generates a random number *NA* before communication. When communication starts, user *A* sends compressed public key *QA* to user *B*. User *B* who receives the message creates a random number *NB* and sends it to user *A* along with the compressed public key *QB*. The two users get point *P* through multiplying the other party's public key by their private key. The *x* coordinate of the point *P* becomes secrete value *z* of two users. The two users who generate *z* obtain the secret key *MK* by using their ID, random numbers, and secrete value *z*. To verify that same *MK* is generated; they send *MacTag* reciprocally. Each user can generate their *MacTag* using *MK*, IDs, and public keys. The *IDX* used in NFC-SEC follows NFCID format. NFCID is dynamically generated in accordance with the application and used for SDD and RFCA. Accordingly, NFC can identify each other through the NFCID but they cannot figure out the definite identity. Since the NFCID is updated each time, the connectivity between messages is not provided. However, the public key *QX* used with *IDX* is a fixed value. Accordingly, if an attacker collects communication history based on the public key, an invasion of user's privacy breaks out due to the occurrence of the connectivity between messages.

C. Pseudonyms

Pseudonym represents ID that changes randomly, and it has widely been studied in VANET (Vehicle Adhoc NETwork) to remove the linkage between messages. The general pseudonym-based privacy protection method uses pseudonym set received from TTP . The pseudonyms are composed of public key, private key, and a certificate. Users can be assured of their anonymity through pseudonym and authenticated as normal users through a certificate. The TTP stores pseudonyms and actual ID of users to reveal the anonymity in case of a problem. However, the method using the pseudonym requires additional costs for storage and communication .Users should maintain data in devices for pseudonyms. In addition, when the pseudonym set owned by users is all used, additional communication needs to be done for reissuance. To improve this, recent studies have been conducted to generate pseudonyms without the help of TTP.

2. NFC ENVIRONMENT

In this section, NFC environment and features currently being applied are introduced. In particular, the suitability of applying pseudonym to NFC is demonstrated through comparison between NFC environment and VANET environment in which pseudonym has widely been studied.

TSM:

Trusted Service Manager TSM (Trusted Service Manager) is an institution that transfers mobile financial data of customers to financial institutions safely. The GSMA (Global System for Mobile Communications Association) proposed TSM to facilitate the provision of NFC services in 2007. TSM serves as CA (Certification Authority) and RA (Registration Authority) at the market of certification services. In this paper, the TSM is considered as TTP for mobile payment services, and the public key used in NFC devices is assumed to be issued from TSM.

SE: Secure Element

SE is a security area that can safely store important data such as financial information, authentication information, and service applications as a secure smart chip. In SE, the range of functions varies depending on the type of implementation, but

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

the storage features and secure domain is certainly included. The secure domain is a unique area separated to safety store important information such as service applications and access key, etc.

Since each secure domain exists independently, it cannot have access to the secure domain in which other services are installed. Users can be provided with payment services from various financial companies through a NFC device.

NFC Features

NFC provides TRH (Tamper Resistamt Hardware) called SE, along with TSM, the trusted third party, which is similar to the VANET environment. However, NFC is somehow different from VANET in communication environment. In the NFC, attacker's actions are further limited compared to VANET. Accordingly, the pseudonyms used in VANET are improved to meet the NFC features and the protection of user's privacy can be achieved at low cost. The NFC features noted in this paper are as follows.

- *One-to-One communication*: In VANET, all vehicles within the range of RSU (Road-Side Unit) perform communication with one RSU. However, in case all vehicles are anonymized RSU cannot communicate with specific vehicles. Accordingly, if a certificate is not provided, an attacker can make an attack more easily by mingling. On the other hand, since only oneto- one communication is possible in case of NFC, it is easy to identify with whom you communicate.
- *Near field Communication:* VANET features communication between vehicles and RSU, and it is implemented during driving, which makes it difficult for users to check the contents of the communication. On the other hand, NFC is a near field communication, and communication is conducted with the target in front of our eyes. Two users can identify whether the communication is properly progressed through each other's device.
- *Sporadic Communication:* VANET performs communication consistently until users arrive at their destination, while updating pseudonym periodically. On the other hand, since NFC performs sporadic communication for payment, it is advantageous to use one-time ID such as pseudonym. In addition, it is not necessary to store a large amount of pseudonyms in advance due to plenty of time before next-payment.

3. SECURITY ISSUES IN NFC

Eavesdropping

Because NFC is a wireless communication interface it is obvious that eavesdropping is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can of course use an antenna to also receive the transmitted signals. Either by experimenting or by literature research the attacker can have the required knowledge on how to extract the transmitted data out of the received RF signal. Also the equipment required to receive the RF signal as well as the equipment to decode the RF signal must be assumed to be available to an attacker as there is no special equipment necessary.

The NFC communication is usually done between two devices in close proximity. This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more.

- RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)
- Characteristic of the attacker’s antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker’s receiver
- Quality of the attacker’s RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.

Additionally, it is of major importance in which mode the sender of the data is operating. This means whether the sender is generating it’s own RF field (active mode) or whether the sender is using the RF field generated by another device (passive mode). Both cases use a different way of transmitting the data and it is much harder to eavesdrop on devices sending data in passive mode.

In order to not leave the reader without any idea on how big the eavesdropping distances are, we give the following numbers, which as stated above are not valid in general at all, but can only serve to give a

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

rough idea about these distances. When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1 m.

Data Corruption

Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device.

Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.

Data Insertion

This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.

Man-in-the-Middle-Attack

MITM attack means an attacker's obtaining data between two users by spoofing. Suppose that Alice and Bob try to exchange their keys, and Carol is an attacker. Carol obtains key K_{AC} by performing key agreement after disguising her as Bob, and key *KBC* after disguising her as Alice. When user Alice sends data encrypted with *KAC* to Carol disguised as Bob, Carol can obtain data *m*. Carol transfer *m* encrypted with *KBC* to Bob. Attacker can modify data of the two users through MITM attack. However, it is known that the MITM attack is generally impossible in NFC [9] due to physical characteristics that protocols performs in close proximity as well as SDD and RFCA described in section II-A. To identify the impossibility of MITM attacks in NFC, let us suppose an environment in which NFC-SEC is not applied (attackers can perform eavesdropping).

In case Alice is in active communication mode, and Bob is in passive communication mode: Alice generates RF field and transfers data to Bob. Carol, an attacker, can prevent Bob from receiving data, while watching the data of Alice. In this case, Alice can detect an attack and stop key agreement. Though Alice cannot detect the attack, Carol needs to generate her own RF field to transfer data to Bob. However, since Alice and Bob are in communication with active-passive mode, Alice does not reap the RF field until NFC of Bob becomes disabled or removed. Since two RF fields cannot exist simultaneously according to RFCA, it is impossible for Carol to transfer data to Bob. Accordingly, a MITM attack is impossible.

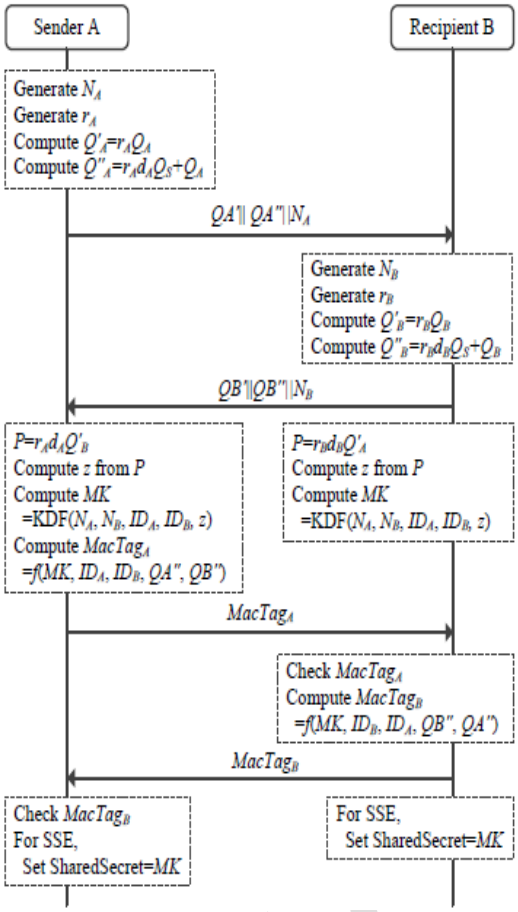
In case both Alice and Bob are in active communication modes: If Alice's data is blocked, Alice can detect attacks as in case of active-passive mode. If not, Alice comes to reap her own RF field to receive data from Bob, when Carol can generate her own RF field successfully and transfer data to Bob. However, Alice waiting for Bob's data can detect attacks after receiving Carol's data. Alice discontinues protocols after detecting attacks, and Carol's MITM attack fails.

4. SELF UPDATABLE PSEUDONYM METHOD

In this project the proposed method is self updatable pseudonym based security protocol that provides privacy between two NFC enabled devices. Some applications such as e-payment we need privacy between terminals. Pseudonym represents ID that changes randomly, and it has widely been studied in VANET (Vehicle Adhoc Network) to remove the linkage between messages. As mentioned in chapter 3 the self updatable pseudonym method provides privacy and reduces the communication as well as storage overhead because when compare to existing pseudonym protocol it can update pseudonym without the need to communicate with TSM or TTP.

The conditional privacy method has widely been studied in the light of pseudonyms when the privacy protection is required. In this paper, conditional privacy protection methods tailored to the NFC environment are proposed. Since the proposed method can reuse NFCIP-1 and NFC-SEC, the NFC standards. If we consider the NFC features in the protocol design process, the protocol can be configured so that it can update pseudonym without the need to communicate with TSM. The communication with the TSM can be used only to keep track of the message constructor. The proposed protocol is shown in Figure 3, and the notation follows Table 1

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349



Figue .2 Key agreement and confirmation protocol using self updatable pseudonym method.

The User B can obtain Q'A and Q″A by decompressing QA' and QA″. Q'A and Q″A are the points on the elliptic curve, and they are developed as in (1) and (2).

$$Q'_A=r_AQ_A=r_Ad_AG \quad (1)$$

$$Q''_A=r_Ad_AQ_s+Q_A=r_Ad_Ad_sG=d_AG \quad (2)$$

According to ECDLP (Elliptic Curve Discrete Logarithm Problem), user B cannot find that Q'A is QA which is the message made by same person, even if user B knows QA. Likewise, in Q″A, user B cannot find rAdAQS because user B does not know rAdA. Thus, user B cannot remove rAdAQS from Q″A, and cannot recognize that the message was constructing by user A. In contrast, the TSM can recognize who made of this message by (3).

$$Q''_A-d_sQ'_A=(r_Ad_A(d_sG))+Q_A-d_s(r_A(d_AG))=Q_A \quad (3)$$

Two users can obtain the common values by using the exchanged messages of Q'A and Q'B. To obtain the same value, multiply private key and the random value to Q'A and Q'B. The random value is the same number used when making Q″A and Q″B. Equation (4) expresses the process in which the two users get the same value.

$$P=r_Ad_AQ'_B=r_Ad_A(r_Bd_BG)=r_Ad_Ar_Bd_BG=r_Bd_B(r_Ad_AG)=r_Bd_BQ'_A \quad (4)$$

Two users can get a shared secret value z by taking x coordinate value at point P. When compared with the existing protocols based on the above process, Q'A and Q'B can replace QA and QB, the existing public keys. In other words, the anonymity of users can be guaranteed by replacing the public key alone, while retaining the existing protocols. This method cannot be used to specify the owner of the public key, but it can identify whether the public key is regularly generated or not. Therefore, it can be identified that the message is generated by using the public key received from TSM. In case the user's public key doesn't pass the verification, the NFC communication is discontinued. When the protocol is discontinued in the process of one-to-one short range communication, users suspect the involvement of attackers, and they can discontinue or restart the communication.

5. CONCLUSION

The proposed method uses random public key like pseudonyms. Since the public key is updated, fewer burdens are imposed on the administration. NFC is a short range one-to-one communication technology, and it has the robust characteristics to MITM (Man In The Middle) attack. Due to its design based on NFC features, the proposed method can provide conditional privacy with less overhead. The proposed methods follows standard systems additionally can hide user's identity, and if necessary, the user's identity can be confirmed by the TSM. Also the user can get personalized services by the selective use of our proposed method. In conclusion, it is expected that the proposed method will help users to protect their privacy and use personalized services. It will contribute to the promotion of mobile payment services through NFC. The self updatable pseudonym based method has the capability to provide privacy. The Anonymity of the user is guaranteed, but it does not provide the authentication mechanism. In case of any problem it is not possible to identify the users. So the future enhancement should be the secure authentication mechanism.

International Journal of Computing Communication and Information System(IJCCIS)
Vol 6. No.1 – Jan-March 2014 Pp. 40-46
©gopalax Journals, Singapore
available at : www.ijcns.com
ISSN: 0976–1349

REFERENCES

[1] A.Chandrasekar,V.R.Rajasekar,andV.Vaasudevan,Improved authentication and key agreement protocol using elliptic curvecryptography," International Journal of Computer Science and Security(IJCSS), Vol. 3, Issue 4, pp. 325-333, Oct. 2009.

[2] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC 2010), pp. 174-181, Dec. 2010.

[3] D. Huang, S. Misra, M. Verma, and G.Xue, "PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs," IEEE Transactions on Intelligent Transportation Systems, Vol. 12, No. 3, pp. 736-746, Sept. 2011.

[4] E. Haselsteiner and K. Breitfuß, "Security in Near field Communication (NFC) – Strengths and Weaknesses –," RFIDSec 2006, Jul. 2006.

[5] Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.

[6] G. Calandriello, P. Papadimitratos, J.P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET," Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (VANET 2007), pp. 19-28, 2007.

[7] GSMA, "Mobile NFC Technical Guidelines Version 1.0," Apr. 2007.

[8] GSMA, "Pay-Buy-Mobile Business Opportunity Analysis – Public White Paper Version 1.0," Nov. 2007.

[9] H. Eun, H. Lee, J. Son, S. Kim, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-381, Jan. 2012.

[10] ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.

[11] ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[12] ISO/IEC 18092:2004, "Information technology – Telecommunications and information exchange between systems – Near field Communication – Interface and Protocol (NFCIP-1)," ISO/IEC, Apr. 2004.

[13] J.C.M. Teo, L.H. Ngoh, and H. Guo, "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks," Proceedings of the 2009 International Conference on Advanced Information Networking and Applications (AINA 2009), pp. 675-682, May 2009.

[14]] J.-H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," Mathematical and Computer Modelling, vol. 55, No. 1, pp. 170-187, Jan. 2012.

[15] Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.

[16] J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.

[17] R.-J. Hwang, Y.-K. Hsiao, and Y.-F. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proceedings of the 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS 2011), pp. 654-659, Dec. 2011

[18] R. Lu, X. Lin, H. Zhu, P.H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Proceedings of The27th Conference on Computer Communications (INFOCOM 2008), pp. 1229-1237, Apr. 2008.

[19] R.-J. Hwang, Y.-K. Hsiao, and Y.-F. Liu, "Secure Communication Scheme of VANET with Privacy Preserving," Proceedings of the 2011 IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS 2011), pp. 654-659, Dec. 2011.