ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India

An Enhancement of Security Standards Based On Pseudonyms in Near Field Communication

M. Isaivani[1], Mrs. T. Sivasankari M.E[2]

Embedded System Technologies, Department of Electronics and Communication Engineering, Anna University,

Raja College of Engineering and Technology, Madurai, India[1]

Department of Electronics and Communication Engineering, Anna University,

Raja College of Engineering and Technology, Madurai,, India[2]

ABSTRACT: Nowadays, numerous mobile terminals have been released into market with NFC which stands for Near Field Communication. The smart devices equipped with NFC have made to improve the effective utility range of NFC. Particularly, NFC electronic payment is expected to take place of credit cards in e-payment. Regarding that, it is necessary to direct the attention of security issues in NFC. At present, the security standards make use of user's public key at a fixed value in key agreement process. The message's relevancy can be obtained at the public key of NFC. Based on, malicious attacker can form a profile by collecting the required messages which leads to the infringement of privacy of user. The planned work presents conditional privacy protection method based on pseudonyms to overcome the problems mentioned earlier. Two users can communicate to each other based on some set of rules by sending the conditional privacy preserved Protocol Data Unit through NFC terminals. Additionally, the communicating party's identity can be computed to resolve problem if occurs. The proposal is implemented in hardware using ARM 7processor and NFC readers. It works well in decreasing the update cost and computation overhead by taking the merit of physical characteristics of NFC.

KEYWORDS*:* SE, Key Agreement, NFC

I. INTRODUCTION

NFC is a type of short-range wireless communication technology which has the coverage distance up to 4 inches and operates the speed range varies from 106kbps to 424kbps at 13.56 MHz operating frequency. The application of NFC together with smart devices includes access control, consumer electronics, health care, transport, data exchange, discovery, connection, e-payment and ticketing. NFC is one to one communication which lets to the ease of identification for the users. NFC is used in payment applications performs sporadic communication which is pseudonym used to advantageous of one time ID. Additionally, there is no need to store a large number of pseudonyms because so much of time before next payment. Also the users can check whether the communication is done properly via each other's device since communication is progressed with the target in front of our eyes. Presently, the NFC make use of public keys is exchanged for users for secret communications with key agreement processes. The public key uses a fixed value received from the Certificate Authority. Attacker can easily acquire the public key to creating the new profiles of users using key agreement process. M1TM attack, Eavesdropping and Data Modulation are the possible threats of NFC. For the purpose to apply the NFC in electronic payment, we have to address the security standard. The proposed work incorporates privacy protection method based on pseudonyms to protect the user's privacy. Conditional privacy is also provided to identify the users and can be checked by the TTP (Trusted Third Party) to solve problems if necessary. Conditional Privacy PDU (Protocol Data Unit) is also defined the users can make use of the protected PDU to receive the personalized services and use conditional privacy PDU conceal the needed information.

II. RELATED WORK

In e-ticketing, it is essential to provide a firm guarantee about the security and privacy of users. The system takes an account of these security requirements that includes exculpablity which means that both users and the service provider will never be accused wrongly to each other of misbehavior. It leads to a secure environment where either both of them got their corresponding data from other or neither they both do. The system also supports another vital phenomena called reusability in which the tickets can be used for a certain number of times that incorporates the same security as single tickets [1]. As vehicular ad-hoc networkers make the driving circumstance in a more safe and comfortable manner, it is being an important component of Intelligent Transportation Systems (ITS). Even though pseudonyms certificate and group-oriented signature are the mainly used privacy preserving technique in VANET, they lead to more efficiency flaws that affect their application. To overcome the above mentioned problems, the system incorporates privacy preserving authentication protocols based on self-certified signature and it has the advantages of short length of the signature and low computation [2]. For the electronic passports which are based on hardware based security, the system makes a security analysis of the ICAO first-generation e-passport as well as the EU's proposal which corresponds to a second-generation of e-passports. Also, the identification and authentication mechanisms are analyzed which make it possible to constitute a pseudonym system based on the security of retaining a high value secret which solves many security and privacy issues [3]. Nowadays, various on line services need user identification. Nevertheless, the possible potential risk is that loosing privacy when revealing messages about user's identity in an unregulated way. The Identity Management System is developed in order to favour users in managing and maintaining related identity data. The system which includes a frame work for identity and privacy management on mobile devices supports roaming users with privacy sensitive handling of a identification process in online transactions [4].

III. Proposed Work

A. TSM, SE, Pseudonym

The more efficient production in the implementation and chip design sector is possible to reusing NFCIP -1 and NFC-SEC. We assume that a user stores the long term public key received from TSM in SE. TSM is an organization which transfers customer's mobile financial data to financial institutions in a safe manner and it is considered to TTP for mobile payment services. SE stands for Secure Element, is a security area which is used to store vital data such as financial information, authentication information and service applications as a secure smart chip safely. Pseudonym is a randomly changing ID and it is considered to be received from TTP & they are composed of public keys, private key and a certificate. In case, any problem arises, TTP always stores pseudonyms and actual ID of users to reveal the anonymity. The Planned work proposes privacy protection methods based on pseudonyms to protect privacy of users are shown in figure 1.

B. UPM: Updateable pseudonym based method

Without any communication with the Trusted Service Manager, the pseudonym can be updated in the process of protocol design in NFC. But to keep track of the message constructor, there is a need to communicate with the TSM.

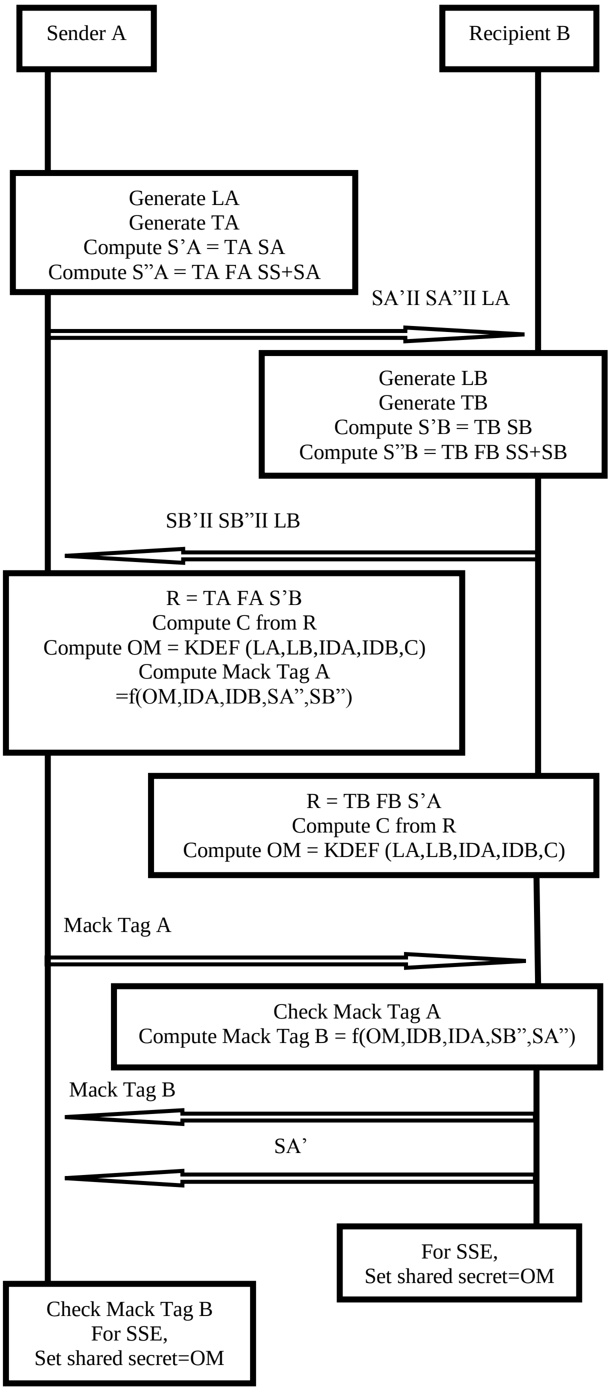


Fig. 1 Updatable Pseudonym Based Method

TABLE – I
NOTATIONS IN UPDATABLE PSEUDONYM BASED METHOD

II	Concatenation symbol
Lx	Nonce of user x
Idx	Random id of user x for the activation of transport protocol
Sx, Sx', Sx''	Compressed elliptic curve public key of
Sx, S'x, S"x	user
Fx	Elliptic curve public key of user
I	Elliptic curve private key of user
KDEF	Elliptic curve base point
Mack tag x	Key derivation function
OM	Key verification tag received from x
C	Shared secret key
Tx	Unsigned integer
	Random integer generated by user x

User A generates nonce, random number and calculates SA', SA" as shown in fig.1 and it sends the concatenation SA' II SA" II LA to user B. User B decompresses SA' and SA" and thus it gets SA' and SA" which are the points on the elliptic curve.

SA' = TA SA = TA FA I
SA" = TA FA SS + SA = TA FA FS I + FA I

Based on ECDLP (Elliptic Curve Discrete Logarithm Problem) Algorithm, user B never find that S'A is SA, that is the message from the same person, though user B knows SA. In the same manner, in S"A user B will not find TA FA SS. The reason is that user B does not know TA FA. Thus, it is guaranteed that user B never remove TA FA SS from S"A and also it could not trace that the message was made by user A. But the TSM should always recognize the message originator to result disputes if any problem occurs. This is done by the following expression.

S"A-FS SA = (TA FA (FS I)) + SA – FS (TA(FA I)) =SA

Both users get the common values by using the above exchanged messages of S'A and S' B. Private key and random value are multiplied with S'A & S'B for the purpose of getting the same value. The random number should not be varied from the one which is used when making S"A and S"B

R =TA FA S'B = TA FA (TB FB I) = TA FA TB FB I =TB FB (TA FA I) = TB FB SA
User A and user B compute a shared secret value C, just by taking x coordinate value at point R. Thus, it is strongly guaranteed that users anonymity can be achieved by replacing the public key alone involved in the existing protocols.

The NFC communication will be discontinued if the users public key doesn't pass the verification. It makes user to suspect the involvement of attackers and based on that, they can either discontinue or restart the communication.

C. Advantages

There is no chance of hacking using public keys, since the system involves pseudonyms. Legal users only identify and communicate to each other. Though hackers can get the data, they cannot know how to decrypt it.

IV. SIMULATION RESULT

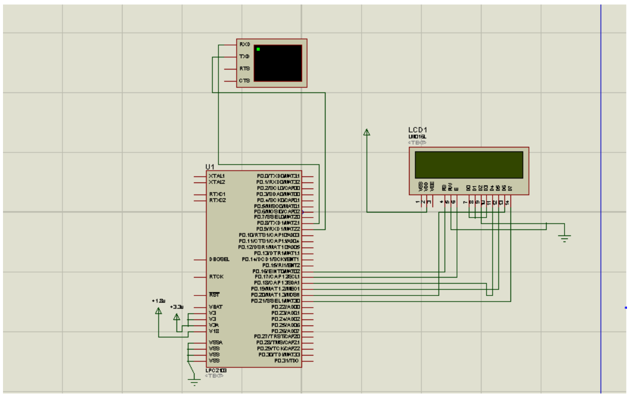
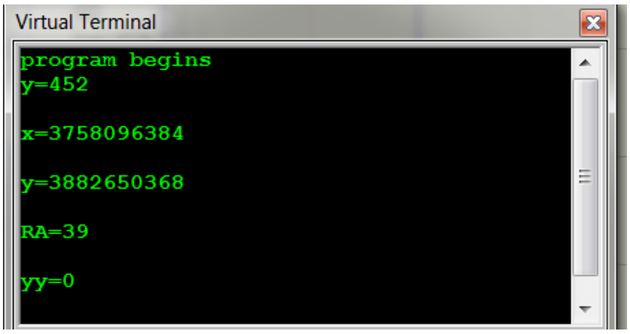


Fig 2. Simulation Output Setup

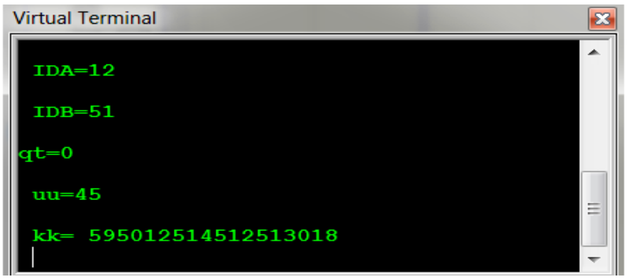
LPC 2103 Processor, virtual terminal, Liquid Crystal Display are interconnected as shown in fig.2. LPC 2103 is a 32 bit ARM 7 processor. It has 48 input-output pins, 32 kb flash memory for program storage and 8kb SRAM for data storage. The process status results are displayed in Liquid Crystal display. To view them in a enlarged and clear manner, virtual terminal has been provided.



```
program begins
y=452

x=3758096384

y=3882650368

RA=39

yy=0
```

Fig 3. Generation of Initial Values at Transmitter

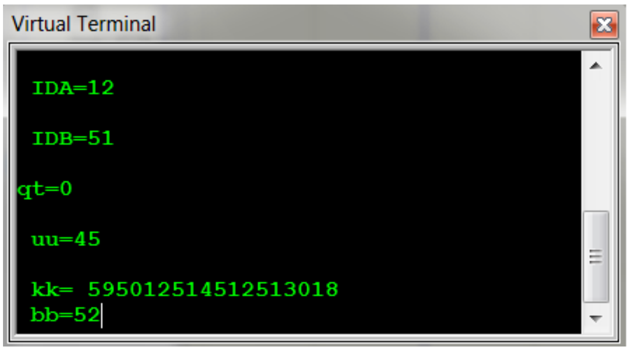
At first, some initial values such as x, y, random numbers are displayed in virtual terminal as per the program when it is run.



```
 IDA=12

 IDB=51

qt=0

 uu=45

 kk= 595012514512513018
```

Fig 4. Generation of Pseudonym MACTAG A at Transmitter

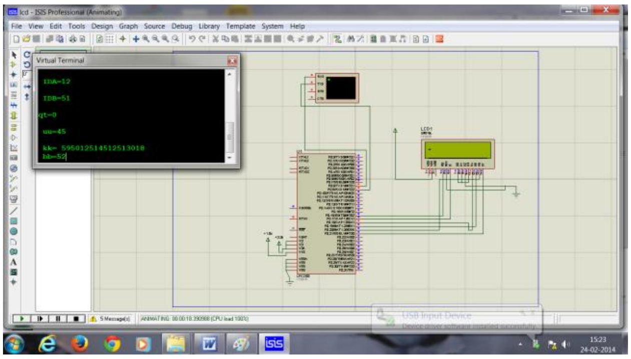
The key pressing in PC is taken as the UART (Universal Asynchronous Receiver Transmitter). When entering the first and second key generates elliptic curve public key, random numbers respectively. When the third key is pressed, the MACTAG A Value is calculated and it is displayed at the virtual terminal.



```
 IDA=12

 IDB=51

qt=0

 uu=45

 kk= 595012514512513018
 bb=52
```

Fig 5. Reception of Pseudonym MACTAG B at Transmitter

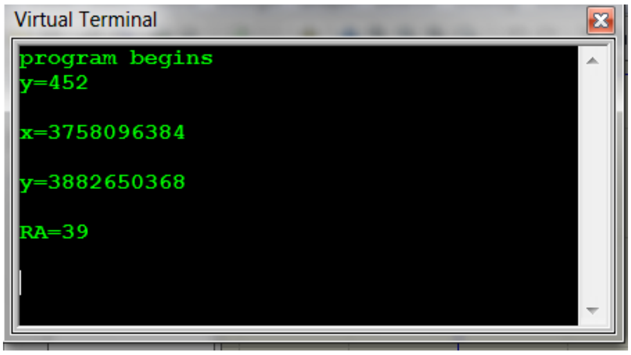
The recipient Pseudonym MACTAG B value is received and is shown at the virtual terminal immediately after the fourth key is being entered.



```
 IDA=12

 IDB=51

qt=0

 uu=45

 kk= 595012514512513018
 bb=52
```

Fig 6. Transmitter output

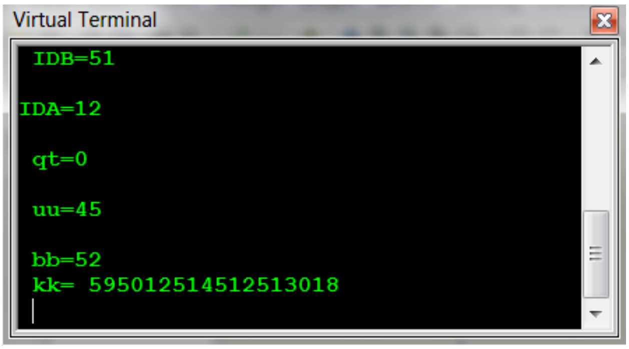
Fig.6 shows the overall view of the output from the transmitter. It displays the final transmitter output which results from the step by step process from fig. 3 to fig.5.



```
program begins
y=452

x=3758096384

y=3882650368

RA=39
```

Fig 7. Generation of Initial values at Receiver

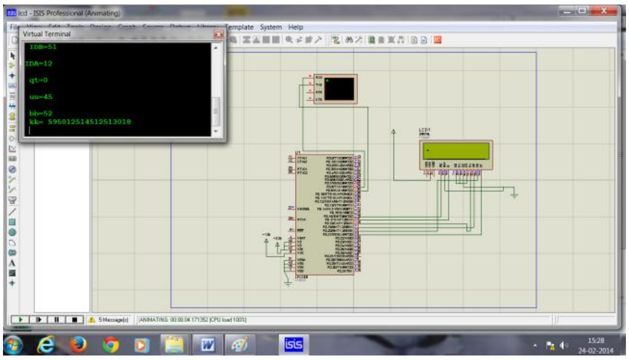
In receiver side, some initial values such as x, y, random numbers are shown in virtual terminal as per the program when it is run.



```
 IDB=51

IDA=12

 qt=0

 uu=45

 bb=52
 kk= 595012514512513018
```

Fig 8. Generation and Reception of Pseudonyms MACTAG B, MAGTAG A

As same as in transmitter, the key pressing in PC is taken as UART (Universal Asynchronous Receiver Transmitter). Entering the first, second and third keys generate elliptic curve public key, random number, ID respectively. When entering the fourth recipient Pseudonym value is calculated and sender's Pseudonym value is received and both are displaced at the virtual terminal.


lcd - ISIS Professional (Animating)
Template
System
Help
Virtual Terminal
LCD1
U1
5 Message(s)
ANIMATING: 00:00:04.171352 (CPU load 100%)
15:28
24-02-2014

```
 IDB=51

IDA=12

 qt=0

 uu=45

 bb=52
 kk= 595012514512513018
```

Fig 9. Receiver Output

Fig. 9 shows the overall view of the receiver output. If same keys are entered both in transmitters and receiver then the pseudonyms are matched and thus authentication is done. That is the sender finds the authenticated receiver and the receiver finds the appropriate sender and secure connection is made.

V. Comparison

MUPM which stands for Multiple Pseudonym Based Method needs additional storage to maintain the pseudonyms and it involves the overhead of managing revocation list and communication cost for pseudonyms issuance. But the updatable pseudonym based method does not involve any communication cost for the issuance of pseudonyms. But it has additional computation time and transfer time.

A. Need of extra storage for the maintenance of pseudonyms

A single pseudonym is consisted of public key, private key which is encrypted with long-term key of user, ID of TSM and signature on the message. The size of a single pseudonym is computed as 1200 bits. If more number of pseudonyms is used, such as 1000, it requires more space i.e. 146.484K bytes. Though the compensation of NFC with mobile device makes it possible, there is a limit on account of the billing charges of mobile device.

B. More Computation Time

TABLE II
COMPUTATION TIME

Mathematical Operation	**Formula**	**Time**
Doubling	ti (2b1)	2MUL+ 2SQU+ INV
Addition	ti (b1 + b2)	2MUL+SQU+ INV

MUL, SQU, INV notates the multiplication, square and inverse operations respectively. (b3=b1+b2) is computed for the time taken to add two points and (b2=2b1) is calculated for computation time required for doubling. The number of doubling operations needed for every users to do the operation is calculated as

$$\log_2 \text{Tx Fx} = \log_2 2^{96} + \log_2 2^{192} = 288$$

It is 96 times increased when compared to NFC - SEC

C. *Extra Transference Time*

Based on the lowest 106kbps NFC, the standard method needs just 2.727ns and the proposed method requires 4.569ns. When compared with NFC - SEC, it is increased 7.680003628ms in order to provide conditional anonymity for each user.

VI CONCLUSION

Since the combination of NFC with various smart devices, e-payment market using NFC is expected to be emerged with proper security constraints. In that case, the users privacy should not be compromised by disclosing their transaction information. The proposed privacy protection method solves the above mentioned issues. It involves updatable pseudonyms and the update is based on the long-term public key which is issued from Trusted Service Manager. Moreover the long-term public is stored in secure element and thus the safe management can be achieved.

VII FUTURE WORK

In future, the communicating party's identity will be identified to resolve if any problem occurs and this entire system will be implemented in hardware using ARM 2103 processor, two NFC Readers. And also, the conditional privacy PDU will be proposed in order to hide any information based on users choice and protected PDU will be processed if the users want to receive personalized services.

REFERENCES

[1] Arnau VIVES-GUASCH, Magdalena PAYERAS - CAPELLA, Macia MUT-PUIGSERVER, Jordi CASTELLA - ROCA and Joseph LLUIS FERRER - GOMILA "A secure e-ticketing scheme for mobile devices with Near Field Communication (NFC) that includes exculpability and reusability" *IEICE TRANS. FUNDAMENTALS,* Vol - E93-A, No.1 January, 2010.

[2] Jianhong Zhang, Yuanbo Cui, Zhipengchen, "SPA : Self - Certified PKC - based Privacy preserving Authentication protocol vehicular ad-hoc networks" College of Science, North China University of Technology, Beijing 100144, P.R. China.

[3] Vijayakrishnan Pasupathinathan "Hardware Based Identification and Authentication Systems" The Degree of Philosophy Thesis, Macquarie University, Department of Computing, December, 2009.

[4] Christian Hansen "A Framework for Identity and Privacy Management on Mobile Devices" University of Agder, Grimstad, Norway, August, 2010.

[5] 1. S. John Moses, 2,P. Anitha Christy Angelin "Enhancing the Privacy through Pseudonymous Authentication and Conditional Communication in Vanets" *Research Inventy: International Journal Of Engineering And Science* Issn: 2278-4721, Vol. 2, Issue 7(March 2013), Pp 45- 49

[6]. Gauthier Van Damme and Karel Wouters "Practical Experiences with NFC Security on Mobile Phones" *Katholieke Universities Leuven Dept. Electrical Engineering-ESAT/SCD/IBBT-COSIC Kasteelpark Arenberg 10,* 3001 Heverlee-Leuven

[7]. Uwe Trottmann Betreuer: "NFC - Possibilities and Risks" Matthias Wachs Seminar Future Internet WS2012 Lehrstuhl Netzarchitekturen und Netzdienste Fakultät für Informatik, Technische Universität München

[8]. ECMA International 2013 Standard ECMA-385 3rd edition/June 2013 NFC-SEC:NFCIP1 Security Services & Protocol

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

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

[11] ISO/IEC 15946-1:2008, "Information technology – Security methods – Cryptographic methods based on elliptic curves – Part 1: General," Apr.2008.

[12]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.

[13]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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.