Performance Evaluation of Two Secure Communication Schemes on Vehicular Ad Hoc Networks

N.W. Lo[1], Chu-Hsiang Yang[2] and Kuo-Hui Yeh[3]
Department of Information Management,
National Taiwan University of Science and Technology
E-mail: nwlo@cs.ntust.edu.tw[1], {M9509104[2], D9409101[3]}@mail.ntust.edu.tw

Abstract *Along with the need of pervasive communication and intelligent decision support services for a modern citizen, vehicle communications technologies will be on demand and deployed in the near future. Because of the unique communication characteristics between vehicles such as self-organizing and decentralized topology, and high-speed movement, how to provide an efficient and secure communication scheme for VANETs (Vehicular Ad Hoc NETworks) has become an important issue in recent years. In this paper, we theoretically evaluate the performance efficiency of two recently published secure communication schemes proposed by Raya & Hubaux (2007) and Wang et al. (2008) on VANETs. From our investigation, we find that the selection of cryptographic module used in these two secure communication schemes should depend on the average number of hop counts between the source vehicle and the destination vehicle. In addition, our evaluation results can help secure communication schemes plot more efficient utilization policies on cryptographic modules to gain better performance in terms of the total transmission time for a message in VANETs.*

Keywords: VANET, performance evaluation, secure communication scheme.

1. Introduction

VANET is one of the most challenging instantiations of mobile ad hoc networks where every vehicle, denoted as a node, is equipped with powerful computing device and various sensors such as global positioning system and radar detector. As the DSRC (Dedicated Short Range Communications) and its wireless component, WAVE (Wireless Access in Vehicular Environments), provide an architecture to support the development of secure communication schemes on VANETs, vast literatures [1-2, 4-11] have investigated the security concern of VANETs and the future perspective of secure VANETs has become a center of attraction. A secure communication scheme on VANETs should guarantee message security and integrity for life-critical information, behavior non-repudiation and individual privacy preservation for each communicating vehicle. The security and privacy goals seem to be contradictory to each other and are worthy to be further studied.

In recent years much attention has focused on secure communication mechanism development on VANETs. In 2005, Dotzer et al. [5] developed a locally information exchanging mechanism and intelligently signal controlling method to reduce the car accidents at intersection. Laurendeau and Barbeau [6] proposed a secure anonymous WAVE-based broadcasting communication scheme, called SAB protocol, on VANETs. Based on the hybrid public key infrastructure and secure key management mechanism, the proposed SAB protocol can fulfill major security requirements such as data confidentiality, anonymity, behavior non-repudiation and mutual entity authentication. Next, Juhong et al. [10] developed a prototype to explore the feasibility of inter-vehicle secure communication scheme and conducted two concluding remarks. First, the performance of public key cryptographic operations and traffic congestion are main challenges on VANETs. Secondly, the encrypted wireless communications over the IEEE 802.11 channel are more effective in terms of delay and loss.

Recently, Raya and Hubaux [2, 4] proposed a secure communication scheme to eliminate the potential security threats during message transmission on VANETs. Their scheme focuses on the safety related application. The message transmitted for this type of applications is usually life-critical information and requires real-time delivery. Hence, information integrity is mandatory. In addition, Raya and Hubaux figured that safety related messages will not contain any sensitive information; therefore, confidentiality for

message content is not required. Furthermore, considering system efficiency and real-time constraint, safety related messages during transmission need only authentication but not encryption. Based on these analyses, Raya and Hubaux successfully developed a secure communication scheme to enhance security of messages transmitted via VANETs. Afterwards, Wang et al. [1] pointed out that Raya and Hubaux's scheme neglects security consideration of transmitted messages for non-safety related applications, and in turn, proposed a robust communication scheme which focuses on non-safety related messages and provides message confidentiality, entity authentication and behavior non-repudiation. Based on Diffie-and-Hellman's three way key exchanges [3], their scheme successfully enhances the security pitfalls of Raya and Hubaux's protocol. In this paper we aim to further analyze these two secure communication schemes proposed by Wang et al. and Raya et al. and make suggestions to improve their performance efficiency.

2. Review of Two Secure Communication Schemes

In this section we review the secure communication schemes proposed by Raya & Hubaux and Wang et al. In these two protocols, each vehicle V has been preloaded a set of public/private key pair (PuK_V/PrK_V) with the certificate $Cert_V$ of PuK_V issued by CA under a PKI (Public Key Infrastructure) environment, where $Cert_V[PuK_V]=PuK_V|Sig_{PrKCA}[PuK_V|ID_{CA}]$. ID_{CA} and PrK_{CA} denote the identity and long-term private key value of CA. When two entities or one group intend to communicate with each other, the corresponding session key establishment process and message transmission procedure will be executed as follows.

Raya & Hubaux's communication scheme:

(1) Two communication entities:

A→B: (*request for communication*) M_1, $Sig_{PrKA}[M_1|T]$, $Cert_A$.
B→A: (*agree for communication*) M_2, $Sig_{PrKB}[M_2|T]$, $Cert_B$.
A→B: $\{B|SK|T\}_{PuKB}$, $Sig_{PrKA}[B|SK|T]$.
A→B: (*message transmission*) m, $HMAC_{SK}(m)$.

Entity A first signs the message M_1 and current timestamp T by utilizing its long-term private key PrK_A. Next, A sends M_1 and $Sig_{PrKA}[M_1|T]$ with its certificate $Cert_A$ as a communication request to entity B. When entity B receives this request message, B first utilizes $Cert_A$ to verify A's signature. If the signature is valid, B generates M_2 to represent its agreement for this communication request and sends it with B's signed message $Sig_{PrKB}[M_2|T]$ and certificate $Cert_B$ back to A. Once A obtains the responses, A adopts B's public key PuK_B to encrypt the generated session key SK, current timestamp T and B's identity ($\{B|SK|T\}_{PuKB}$). After that, A transmits $\{B|SK|T\}_{PuKB}$ and its corresponding signed message $Sig_{PrKA}[B|SK|T]$ to B. When B receives the $\{B|SK|T\}_{PuKB}$, B decrypts this ciphertext and retrieves the current session key SK. Furthermore, if the verification of $Sig_{PrKA}[B|SK|T]$ is passed at B end, B can ensure this session key SK is correctly shared with A. As mentioned before, safety related messages only require authentication, the message transmission phase can accordingly be completed by using Hashed Message Authentication Codes (*HMAC*) with current session key SK.

(2) Group communication (more than two communication entities):

L→i: H_i, $\{SK\}_{PuKi}$, Sig_{PrKL}[*the whole message*], where i indicates a message receiver.
L→i: (*message transmission*) m, $HMAC_{SK}(m)$.
L→j: (*new member*) $\{SK\}_{PuKj}$, $Sig_{PrKL}[\{SK\}_{PuKj}]$.

In a communication group on VANETs, the group leader L will be the communication center of the dynamically formed network cell, where there may be multiple such cells generated on the road. With periodic exchange of certified public keys, the group leader L will decide the session key SK on his own and encrypt it with the public key of targeted receiver i. Then L sends the encrypted session key along with H_i, the hashed public key value of receiver i, and signed message with group leader L's private key to each corresponding receiver i. Once a member i received the message issued by L, i first calculates the hash value of its own public key and compares it with the received value H_i. If two values are matched, i will utilize L's public key to verify the signed message Sig_{PrKL}[*the whole message*] and then decrypt the cipher $\{SK\}_{PuKi}$ to obtain the session key SK. Note that Raya and Hubaux's group communication scheme only considers security threats from external malicious attackers; L will send $\{SK\}_{PuKj}$ and $Sig_{PrKL}[\{SK\}_{PuKj}]$ to newly joined member j and do nothing regarding to any member left the current group.

Wang et al.'s communication scheme:

(1) Two communication entities:

A→B: M_1 (*request for communication with*

Diffie-Hellman parameters a, q, Y_A), $Sig_{PrKA}[M_1|T]$, $Cert_A$.

B→A: M_2 (*response with Diffie-Hellman parameter* Y_B), $Sig_{PrKB}[M_2|T]$, $Cert_B$, $HMAC_{SK}(M_2)$.

A→B: M_3 (*session key is built*), $HMAC_{SK}(M_3)$.

A→B: (*message transmission*)

1. $E_{SK}(m)$ or
2. $E_{SK}(m|Sig_{PrKA}[HMAC_{SK}(m)])$ or
3. $E_{SK}(m)$, $Sig_{PrKA}[HMAC_{SK}(E_{SK}(m))]$

Entity A first defines a primitive root a of a prime number q, and computes $Y_A=a^{X_A} \bmod q$ with a generated random number X_A. Then, A sends the request message containing parameters a, q and Y_A with its signature $Sig_{PrKA}[M_1|T]$ and certificate $Cert_A$ to B, where T denotes the current timestamp. Once receiving the message sent by A, B first verifies A's signature; if the message passed the verification, B selects a random number X_B, and computes $Y_B=a^{X_B} \bmod q$ and current shared session key $SK=(Y_A)^{X_B} \bmod q$. Furthermore, B can also calculate the $HMAC_{SK}(M_2)$ value by adopting hashed message authentication codes (*HMAC*) with this shared session key *SK*. Next, B responds message M_2 with its signature $Sig_{PrKB}[M_2|T]$, certificate $Cert_B$ and calculated value $HMAC_{SK}(M_2)$ to A. With these response messages, A can compute the shared session key $SK=(Y_B)^{X_A} \bmod q$ after the verification of B's signature $Sig_{PrKB}[M_2|T]$ and $HMAC_{SK}(M_2)$ are examined successfully. Finally, A transmits message M_3 and $HMAC_{SK}(M_3)$ to inform B that session key is successfully built. Furthermore, Wang et al. further developed three tailor-made message transmission mechanisms to achieve different security requirements such as message confidentiality, entity authentication and behavior non-repudiation. Note that $E_{SK}(m)$ means the symmetric encryption of message *m* with secret (session) key *SK*.

(2) Group communication (more than two communication entities):

L→*: H_A, $\{SK\}_{PuKA}$, H_B, $\{SK\}_{PuKB}$, H_C, $\{SK\}_{PuKC}$, Sig_{PrKL}[*the whole message*].

L→*: (*message transmission*)

1. $E_{SK}(m)$ or
2. $E_{SK}(m|Sig_{PrKA}[HMAC_{SK}(m)])$ or
3. $E_{SK}(m)$, $Sig_{PrKA}[HMAC_{SK}(E_{SK}(m))]$

The group communication scheme proposed by Wang et al. is almost the same as Raya and Hubaux's protocol except for the message transmission phase. Similarly, three tailor-made message transmission options are provided here to achieve different security demands.

3. Performance Evaluation

In this section, we theoretically evaluate the performance of the communication schemes proposed by Raya & Hubaux and Wang et al. The simulation environment and benchmark parameters are described as follows. We conduct the benchmark test on a HP laptop computer with the following specifications: Intel 1.73GHz processor, 504MB memory and Windows XP Professional service package 2. In addition, in our simulation all cryptographic algorithms are from Crypto++ 5.5.2 library [13] and complied with Microsoft Visual Studio .NET 2005.

Before introducing the performance evaluation of these two targeted communication schemes, the computation cost analysis of single cryptographic operation such as encryption/decryption, signature, and one way hash function is conducted first. We select RSA, ECC (both are asymmetric encryption methods) and AES (symmetric encryption method) [1, 13] as the analysis targets for encryption/decryption operation. The key size used during cost analysis for RSA, ECC and AES are 1024bits, 256bits and 128bits due to the similar security level as shown in Table 1 [12]. Secondly, the target signature schemes in our simulation only consider RSA and DSA [13]. The standard format of message digest, key size and certificate size are presented in Table 2 [1, 13-14], respectively. Based on our simulation result, signature generation and verification times of DSA and RSA are also presented in Table 2. Finally, we adopt SHA-1 as the target hash function (HMAC) due to its higher security level [13]. According to our simulation, the computation time of HMAC operation is almost negligible in comparison with the other cryptographic operations such as encryption/decryption and signature operation. This simulation result is similar to reports depicted in [6]. Note that the listed computation time of each cryptographic operation is the average value of ten experimental results.

In the following, we evaluate the security cost of communication schemes proposed by Raya & Hubaux and Wang et al. with different combination of cryptographic operations such as (RSA signature, AES encryption), (RSA signature, ECC encryption), and so on. The security cost consists of the extra data processing time involved with the cryptographic operations, encrypted message transmission time and encrypted message propagation time. Next, we assume that the nominal transmission rate is 11Mbps [10], the base rate in 802.11g standard, and the wireless

transmission distance of each node/vehicle is 250m. Multi-hops message transmission model is adopted in our performance evaluation. Since entity authentication is indispensable to both safety related applications and non-safety related applications, we assume all intermediate nodes/vehicles need to verify the signature of each incoming message to ensure the entity authentication before forwarding it during a multi-hops message transmission.

Table 4 shows an example of evaluating the performance of Wang et al.'s communication scheme with (DSA signature, AES encryption) cryptographic operations. The length of each transmitted message in step 1 is 2088 (=40+1024+1024) bytes; and the corresponding transmission time of this message is 1.5185 (=2088*8/(11*10^6)*10^3) ms for each immediate node. Note that we assume the number of nodes along this transmission route is *n*. i.e., there are *n-1* hops between source node and destination node. The propagation time is 250/(3*$10^{8)}$ (the velocity of electromagnetic wave) seconds. Next, the data processing time is composed of one signature generation time and *n-1* signature verification time in which the multi-hops transmission scenario is considered. The calculation of computation cost in step 2 is similar to step 1 except the addition of message digest of $HMAC_{sk}(M_2)$, which is 20 bytes long [14]. In step 3, the cost of $HMAC_{sk}(M_3)$ is very little and negligible. Therefore, the data processing time is set to 0. In step 4, we adopt the expensive and robust message style ($E_{SK}(m)$, $Sig_{PrKA}[HMAC_{SK}(E_{SK}(m))]$) in Wang et al.'s scheme. The length of each transmitted message is 1080(=1040+40) bytes whereas the length of ciphertext after executing AES encryption is 1040 bytes; and its corresponding transmission time at each intermediate node is 0.785ms. The data processing time in step 4 consists of one AES encryption time (0.6354ms), one AES decryption time (1.8411ms), one DSA signature generation time (11.8868ms) and *n-1* DSA signature verification time (8.096*(n-1) ms). In brief, we can utilize the function 29.54**n*+8.6 to represent the performance measurement of Wang et al's communication scheme with (DSA signature, AES encryption) cryptographic operations. In Table 5 & 6, the performance measurements of communication schemes proposed by Wang et al. and Raya & Hubaux with different cryptographic operation combinations are listed.

Table 1. The minimum key sizes of target encryption/decryption algorithms [12]

Algorithm security	AES	ECC	RSA
Present-2010	128/192/256 bits	160 bits	1024 bits
Present-2030	128/192/256 bits	224 bits	2048 bits
Beyond 2030	128/192/256 bits	256 bits	3072 bits

Table 2. Target signature operations with corresponding message format, key size and computation time

	DSA	RSA
Message size	1024 bytes	1024 bytes
Message digest	40 bytes	128 bytes
Certificate size (at least)	1024 bytes	1024 bytes
Public key size	128 bytes	128 bytes
Signature generation time	11.8868 ms	39.1353 ms
Signature verification time	8.096 ms	3.7196 ms

Table 3. Target encryption/decryption algorithm and its corresponding message format and computation time

	ECC	RSA	AES
Plaintext	1024 bytes	86 bytes * 11 + 78 bytes	1024 bytes
Ciphertext	1110 bytes	256 bytes*12	1040 bytes
Key size	32 bytes	128 bytes	16 bytes
Encryption time	90.3593ms	124.1057ms	0.6354 ms
Decryption time	58.7596ms	199.0496 ms	1.8411 ms

Table 4. An example of performance evaluation on Wang et al's communication scheme with (DSA signature, AES encryption) cryptographic operations

Wang et al's communication scheme			
	Message transmission time (ms)	Message propagation time (ms)	Data processing time involved with the cryptographic operations (ms)
Step1:A→B	1.5185*(*n*-1)	0.0008*(*n*-1)	11.88676+8.096* (*n*-1)
Step2:B→A	2.1876*(*n*-1)	0.0008*(*n*-1)	11.88676+8.096 *(*n*-1)
Step3:A→B	0.7592*(*n*-1)	0.0008*(*n*-1)	0
Step4:A→B	0.785*(*n*-1)	0.0008*(*n*-1)	14.3632+8.096*(*n*-1)
(security cost) Total computation time=29.54**n*+8.6 (ms)			

Table 5. The performance measurement of Wang et al.'s communication scheme

Combination of different cryptographic operations	Time (ms)
(RSA signature, AES encryption)	15.95**n*+103.932 ms
(DSA signature, AES encryption)	29.54**n*+8.6 ms

Table 6. The performance measurement of Raya & Hubaux's communication scheme

Combination of different cryptographic operations	Time (ms)
(RSA signature, RSA encryption)	17.41**n* +423.1538 ms
(RSA signature, ECC encryption)	15.98**n*+250.543 ms
(DSA signature, RSA encryption)	30.35**n*+328.4681 ms
(DSA signature, ECC encryption)	28.92**n*+97.0996 ms

Based on the performance measurements presented in Table 4-6, we analyze the effect of security cost of these two schemes while the number of nodes passed in a message transmission route changes. Figure 1 shows that the cryptographic operation combination (DSA signature, AES encryption) requires less time to complete a secure communication session and is more suitable to Wang et al's scheme when the number of nodes *n* is no more than 7. As the value of *n* is greater than 7, the combination (RSA signature, AES encryption) is better. In addition, this figure indicates non-secure communication scheme requires much less communication time. Obviously, the adoption of cryptographic operations will dramatically increase total communication time when the number of nodes passed becomes larger. In Figure 2, as *n* is less than 11, the cryptographic operation combination (DSA signature, ECC encryption) is the best candidate to implement Raya & Hubaux's communication scheme. However, the combination (RSA signature, ECC encryption) becomes a better choice once *n* is more than 11. Note that the combination (RSA signature, RSA encryption) is better than (DSA signature, ECC encryption) after *n* is greater than 28. From these results, we can conclude that ECC is a very efficient asymmetric encryption algorithm and suitable to be utilized by a secure communication scheme on VANETs. On the other hand, DSA and RSA signature can be adopted respectively depending on the number of nodes involved on VANETs.

Figure 3 indicates that different message sizes will not affect security cost significantly when implementing Wang et al.'s scheme with AES symmetric encryption. Note that in Wang et al.'s scheme only symmetric encryptions are required. Wang et al. [1] had shown that AES is one of the most promising symmetric encryption algorithms for VANETs. Hence, we choose AES as the targeted symmetric encryption operation in our simulation. From Figure 3, we can find that DSA, RSA and AES are non-sensitive to message size variation. In Figure 4 and 5, we present experimental results of the Raya & Hubaux's scheme based on RSA and DSA signature with various message sizes. We observe that ECC encryption operation will be affected significantly by message size variation while RSA encryption operation is non-sensitive to this factor.

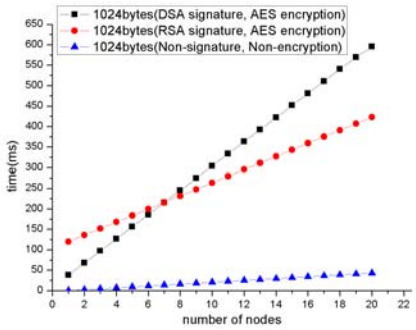

Figure 1. The security cost of Wang et al.'s communication scheme based on different combinations of cryptographic operations.

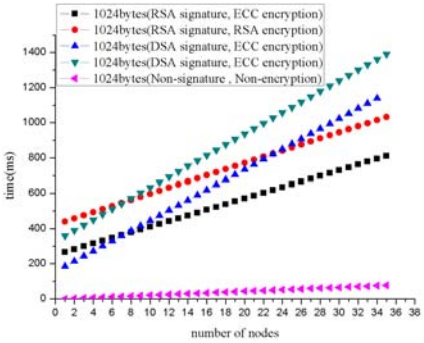

Figure 2. The security cost of Raya & Hubaux's communication scheme based on different combinations of cryptographic operations.

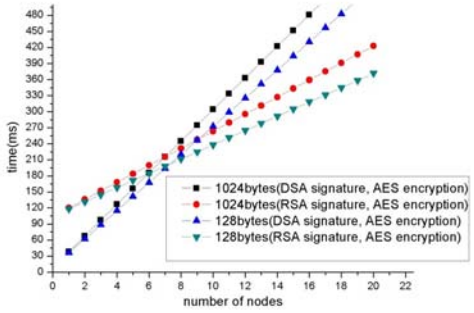

Figure 3. The security cost of Wang et al.'s communication scheme based on different combinations of cryptographic operations and various message sizes.

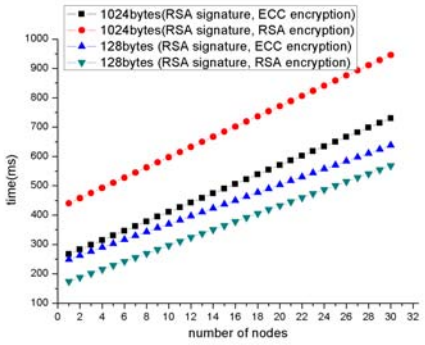

Figure 4. The security cost of Raya & Hubaux's communication scheme based on RSA signature with various message sizes.

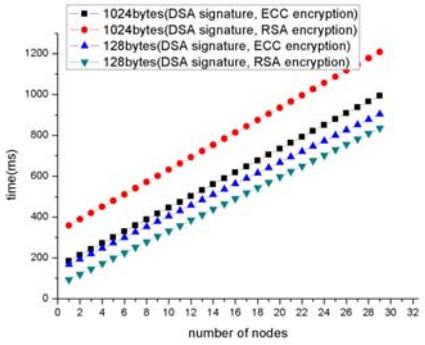

Figure 5. The security cost of Raya & Hubaux's communication scheme based on DSA signature with various message sizes.

4. Conclusion

In this paper, we have demonstrated the performance evaluation of two secure communication schemes proposed by Raya & Hubaux and Wang et al. on VANETs. According to our evaluation results, we find that two combinations of cryptographic operations, (DSA signature, AES encryption) and (RSA signature, AES encryption), are more suitable to be implemented on Wang et al's scheme along with a dividing point of hop counts n=7, respectively. On the other hand, the operation combinations (DSA signature, ECC encryption) and (RSA signature, ECC encryption) are the best candidates to practice Raya & Hubaux's communication scheme along with a splitting value of hop counts n=11, respectively.

5. Acknowledgments

The authors gratefully acknowledge the support from TWISC projects sponsored by the National Science Council, Taiwan, under the Grants No NSC 96-2219-E-001-001 and NSC 96-2219-E-011-008.

6. References

[1] Neng-Wen Wang, Yueh-Min Huang, Wei-Ming Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer Communications*, Available online, 2008.

[2] M. Raya, J.P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, Vol. 15, Pages: 39-68, 2007.

[3] W. Diffie, M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, 1976.

[4] M. Raya, J.P. Hubaux, "The security of vehicular ad hoc networks," *In Proceedings of SASN'05*, pages: 11-21, 2005.

[5] F. Dotzer, F. Kohlmayer, T. Kosch, M. Strassberger, "Secure Communication for Intersection Assistance," *In proceedings of the 2nd International Workshop on Intelligent Transportation*, 2005.

[6] C. Laurendeau and M. Barbeau, "Secure Anoymous Broadcasting in Vehicular Networks," *IEEE Conference on Local Computer Networks*, 2007.

[7] C. Laurendeau and M. Barbeau, "Threats to Security in DSRC/WAVE," *In Proceedings of the 5th International Conference on Ad Hoc Networks and Wireless*. Vol. 4104 of LNCS, 2006.

[8] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles," *In Proceedings of 4th Workshop on Embedded Security in Cars*, 2006.

[9] C. Adler and M. Strassberger, "Putting Together the Pieces- A Comprehensive View on Cooperative Local Danger Warning," *In Proceedings the 13th ITS World Congress and Exhibition on Intelligent Transport Systems and Services*, 2006.

[10] M. Juhong, H Jihun, Y Sangki, K Lnhye,K Hyogon," Secure Vehicular Communication for Safety Applications - A Measurement Study," *In Proceeding of the IEEE Vehicular Technology Conferenc*e, 2008.

[11] JT Isaac, JS Camara, S Zeadally, and JT Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," *Computer Communications*, 2008.

[12] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management – Part 1: General (Revised) NIST Special Publication 800-57", May, 2006

[13] Wei Dai, "Crypto++ Library 5.5.2." online available: http://www.cryptopp.com/

[14] FIPS PUB 186-2, "Digital Signature Standard (DSS)," National Institute for Standards and Technology, 2000.

[15] Ren Wei Kim, Yooh wan Jo, Ju-Yeon Yang, Mei Jiang and Ying tao, "dsRF: ID-based Secure Routing Framework for Wireless Ad-Hoc Networks," *In Proceeding of 4th International Conference on Information Technology*, Pages: 102-110, 2007.