I-SEAD: A Secure Routing Protocol for Mobile Ad Hoc Networks

Wei-Shen Lai[1], Chu-Hsing Lin[2], Jung-Chun Liu[2], Yen-Lin Huang[2], Mei-Chun Chou[2]
[1]*Department of Information Management, Chienkuo Technology University, Taiwan*
[2]*Department of Computer Science and Information Engineering,*
Tunghai University, Taiwan
[1]*WeiShenLai@gmail.com*
[2] *{chlin, jcliu, g942803, g96350011}@thu.edu.tw*

Abstract

Ad hoc networks are highly dynamic routing networks cooperated by a collection of wireless mobile hosts without any assistance of a centralized access point. Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV). SEAD provides a robust protocol against attackers trying to create incorrect routing state in the other node. However, it does not provide a way to prevent an attacker from tampering the next hop or the destination field in route update. In this paper, we propose an I-SEAD protocol to solve the problem. A series of simulation experiments are conducted to evaluate the performance.

1. Introduction

Ad-hoc network is a computer network in which the communication links are wireless and the devices on it communicate directly with each other. This allows all wireless devices within range of each other to discover and communicate in a peer-to-peer fashion without involving central access points.

An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance degrades as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage.

To design an Ad hoc network routing protocol is challenging, and to design a secure one is even more difficult. There are many research focus on how to provide efficient [1, 2] and secure [3-6] communication in ad hoc networks.

The Secure Efficient Ad hoc Distance Vector (SEAD) [5] protocol uses one-way hash chains to prevent an attacker from forging better metrics or sequence numbers. But SEAD does not prevent an attacker from tampering other fields or from using the learned metric and sequence number to send new routing updates. In this paper, we proposed a new protocol to improve security of SEAD. We also conduct some simulation experiments to evaluate the performance of our proposed protocol.

2. Introduction of SEAD

2.1. Second-order headings

In order to understand the route information, we list the notations used as follows:

$H(\ )$	is an one way hash function.
ti	is the TESLA [7,8] time interval corresponding to the TESLA key that currently uses.

$K_{A_{ti}}$ is the TESLA key of node A corresponding to time interval *ti*.

$MAC_{K_{A_{ti}}}(M)$ is the computation of the message authentication code (MAC) of the message M with $K_{A_{ti}}$.

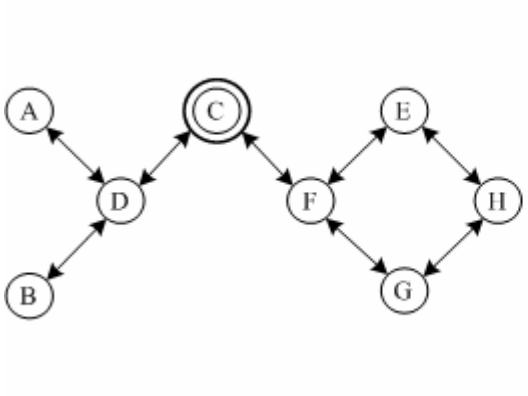
RReq indicates route request.

RRep indicates route reply.

2.2. The SEAD Protocol

Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of Destination Sequenced Distance Vector routing protocol (DSDV) [9]. Nodes maintain distances to destination and keep information about the next hop in the optimal path to a destination. SEAD routing tables maintain a hash value for each neighbor to prevent an attacker to forge better metrics or sequence numbers.

The characteristic of SEAD is that it uses a one way hash function. Each node computes a list of hash values h_1, … , h_n where $h_i = H(h_{i-1}), 0 < i \le n$, given an initial h_0. If a node knows H and a value h_n, then it can authenticate any other values of $h_i, 0 < i \le n$.



Dest.	N. hop	Metric	Seq. No.	Hash value
C	C	0	S406_C	83DF733A
A	D	2	S128_A	B938E96C
D	D	1	S564_D	F2002330
B	D	2	S710_B	JI1042OP
E	F	2	S392_E	IE34M930
F	F	1	S076_F	M93805I0
G	F	2	S128_G	38GD302P
H	F	3	S050_H	TEF153LK

Figure 1. Routing table of node C on SEAD protocol

The method used by SEAD for authenticating an entry in a routing update uses the sequence number in that node to determine a contiguous group of *m* elements from that destination node's hash chain, one element of which has to be used to authenticate that routing update. In Figure 1, the difference in the table of node C is the column of hash values. The particular hash value from this group of hash values that have to be used to authenticate the node is determined by the metric value being sent in that node.

Table 1. onception of hash chain in SEAD

	j=1	2	3	4	5
i=1	h_{15}	h_{16}	h_{17}	h_{18}	h_{19}
2	h_{10}	h_{11}	h_{12}	h_{13}	h_{14}
3	h_5	h_6	h_7	h_8	h_9
4	h_0	h_1	h_2	h_3	h_4

Let a node's hash chain be the sequence of values h_0, h_1, … , h_n where $h_i = H(h_{i-1})$ and n is divisible by m, then for a sequence number i in some routing update, and let $k = (n/m) - i$. An value from the group of hash values h_{km}, h_{km+1}, … , h_{km+m-1} is used to authenticate the node. The example in Table 1 has m = 5 and n = 20, in which i denotes the sequence number, j denotes metric, m denotes network diameter, and n denotes length of hash chain. In SEAD protocol, the received node can verify the metric according to the received hash value. Some malicious node can increase the metric and compute the corresponding hash value. In this case, a potential shortest route will not be used.

3. The Proposed Protocol

3.1. Some Problems Using the SEAD

SEAD provides a robust protocol against attackers trying to create incorrect routing state in other node by modifying the sequence number or the routing metric. But SEAD does not provide a way to prevent an attacker from tampering the next hop or the destination field in route update. Also, it can't prevent an attacker to use the same metric and the sequence number learned from some recent update message, to send a new routing update to a different destination.

3.2. Our Enhancement on SEAD

In SEAD, the nodes exchange their routing tables periodically and broadcast their hash value to their neighbors, so that the neighbors can verify the correctness of the value by one way hash function. Because of the periodic and triggered updating, SEAD increases the routing overhead significantly. And how do the nodes trust the correctness of the hash value that they have received? In our proposed protocol, called I-SEAD, it can let the neighbors check the correctness of the hash value and reduce the routing overhead.

We describe the procedure as follows. When the start node sends the route request, it randomly chooses a number as a seed. The start node computes the list of values with the seed. Before sending the route request, the start node computes its MAC value by its TESLA key to protect its hash value. Each node can verify the received value after a period of time. For example, given an authenticated h_i value, a node can authenticate h_{i-3} by computing $H(H(H(h_{i-3})))$ and verifying that the resulting value equals h_i as in the SEAD.

3.3. Secure Route Maintenance

In Figure 2, the node D computes a list of hash values h_0, h_1, … , h_n, and encrypts h_n by its TESLA key. So that, each node receives the hash value could verify the correctness of the message and could not modify it. Then, the intermediate node checks whether the hash value originated from the destination node. The nodes in the routing path update their routing tables including the start node and the end node.

Due to the feature of TESLA, the intermediate node can not verify the packet by the run, it just appends its information on RReq and forwards it to the next hop. After a period of time, then it is able to check the correctness of the RReq.

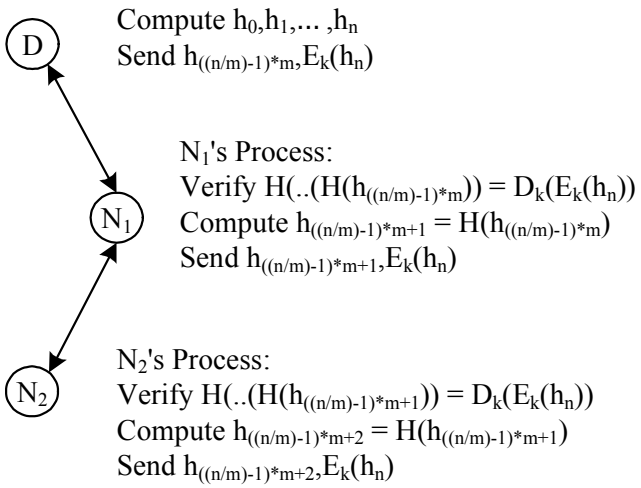


Figure 2. I-SEAD Protocol

4. Performance Evaluation

4.1. Simulation Setup

We conduct a series of simulations to evaluate the performance of I-SEAD, and compare with SEAD. We launch the simulation on NS2. NS2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. The project is funded by DARPA in collaboration with XEROX Palo Alto Research Center (PARC) and Lawrence Berkeley National Laboratory (LBNL).

The traffic is of constant bit rate (CBR). Each flow does not change its source and destination for the lifetime of a simulation run. Each source node transmits data packet at four 512-byte data packets per second. The mobility model is with a pause time of 30 seconds. The network size and the respective network areas are shown in Table 2,The size and the area are selected so that the node density is approximately constant, which would properly reflect the scalability of routing protocols.

Table 2. Network sizes and network areas

Size	Area (m2)	Size	Area (m2)
100	1400 × 1400	800	4000 × 4000
200	2000 × 2000	1000	4500 × 4500
400	2800 × 2800	1200	4900 × 4900
600	3500 × 3500	1400	5300 × 5300

4.2. Comparison of I-SEAD and SEAD

First, we study the scalability of I-SEAD in networks with 100 to 1,400 nodes. Second, we study the performance of I-SEAD with the pause time from 0 to 100 seconds. The number of CBR flows is 20 in both simulation sets. Finally, we analyze the performance of I-SEAD when the number of flows increased from 20 to 60 in networks with 400 nodes. In the

simulations, we collect data for three metrics, namely, the control overhead, the packets delivery ratio, and the end-to-end delay. Each data point in the graphs is averaged over 10 simulation runs, each with a different seed. Each simulation lasts for 600 seconds.

4.2.1. Scalability

In this series of simulation, we analyze the performance of I-SEAD when the network size varies from 100 nodes to 1,400 nodes. The main purpose of source on-demand routing in MANETs is to reduce the routing overhead. It shows that control overhead in I-SEAD reduces significantly in Figure 3 because of the decreasing period updating packets. In Figure 4, we observe that I-SEAD shows lower packets delivery ratio than SEAD because of periodic updates, SEAD has the latest route information. In Figure 5, I-SEAD does not reduce the end-to-end delay. In order to reduce the control overhead, it costs a little time for initiating a new route.

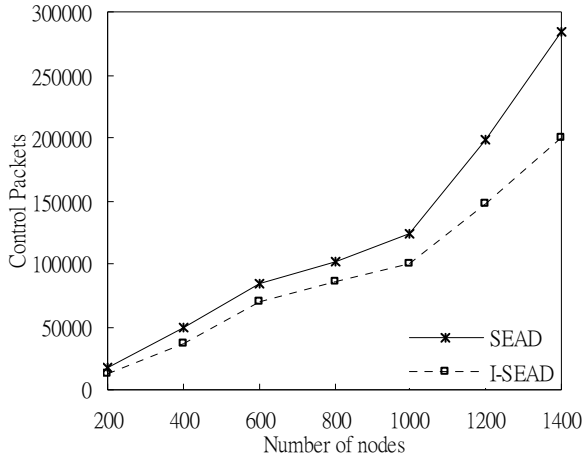


Figure 3. Control Overhead on I-SEAD and SEAD (Scalability)

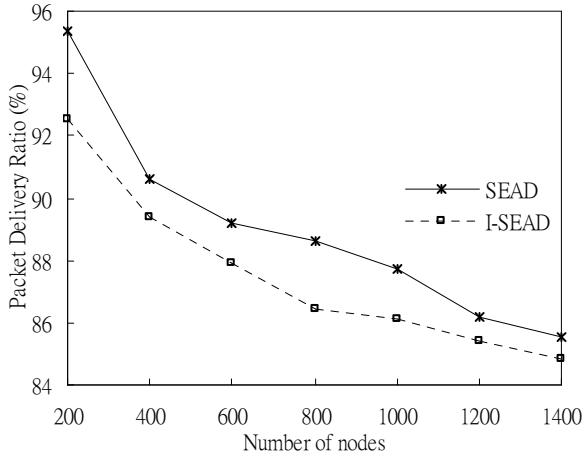


Figure 4. Packets Delivery Ratio on I-SEAD and SEAD (Scalability)

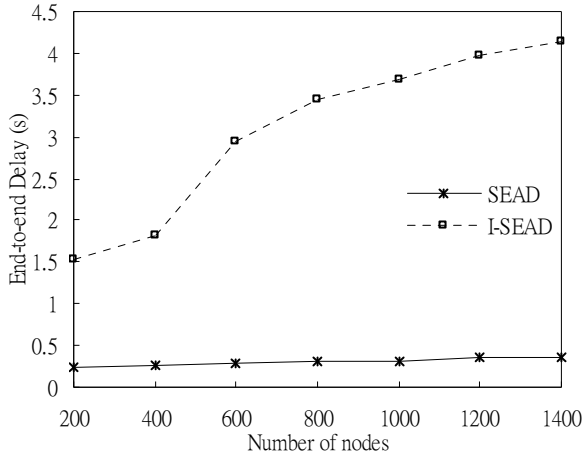


Figure 5. End-to end Delay on I-SEAD and SEAD (Scalability)

4.2.2. Mobility

In this series of simulation, the simulations are run on networks with 100 nodes in the area of 1,400 × 1,400 m^2 and with pause time varying from 0 to 180 seconds. In Figure 6-8, we observe that the more frequent nodes move the more control overhead SEAD has. In SEAD, periodic updating packets are needed. The SEAD and I-SEAD have similar packet delivery ratio. If the nodes do not move very frequently, I-SEAD has higher packet delivery ratio with pause time above 35 seconds. In order to reduce the control overhead, I-SEAD costs more time for initiating a new route in ad hoc networks, so the end-to-end delay time is longer than SEAD.

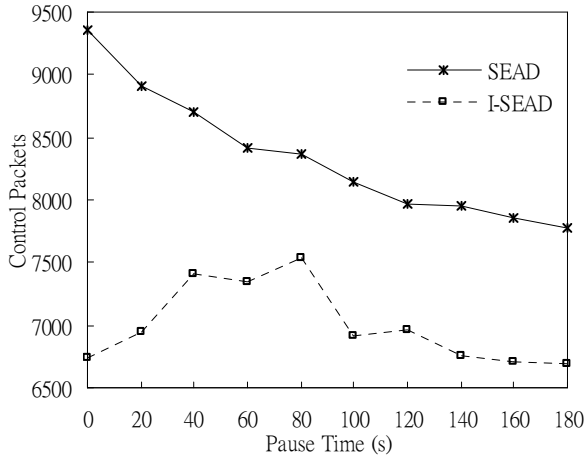


Figure 6. Control Overhead on I-SEAD and SEAD (Mobility)

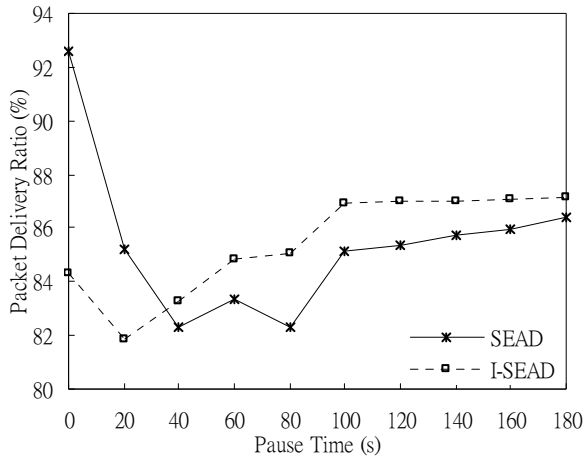


Figure 7. Packets Delivery Ratio on I-SEAD and SEAD (Mobility)

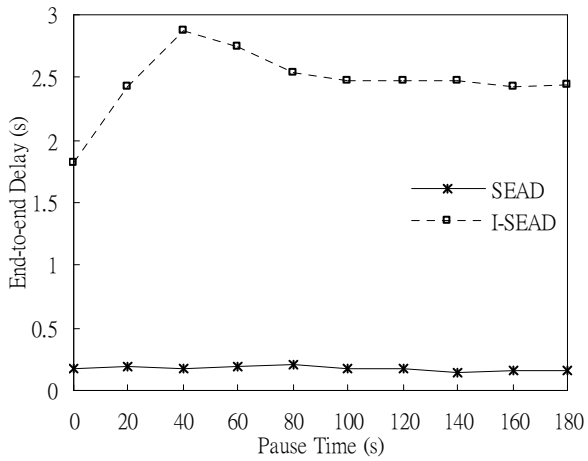


Figure 8. End-to-end Delay on I-SEAD and SEAD (Mobility)

4.2.3. Capability

This series of simulations analyze the performance of I-SEAD when the number of CBR flow increases. The simulations are run on networks with 400 nodes in the area of 2,800 × 2,800 m^2. The number of CBR flow increases from 20 to 60.

In Figure 9, we observe that I-SEAD saves more control packets per flow compared to SEAD. This is mainly because I-SEAD does not have periodic route information. In Figure 10, the SEAD and I-SEAD have similar packet delivery ratio. That shows that SEAD and I-SEAD have similar latest route information. I-SEAD does not have the latest route information and it needs to compute the hash value for authentication. In Figure 11, I-SEAD costs more time than SEAD.

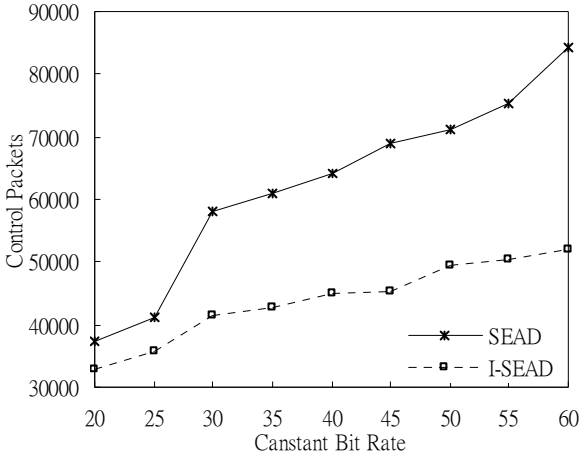


Figure 9. Control Overhead on I-SEAD and SEAD (Capability)

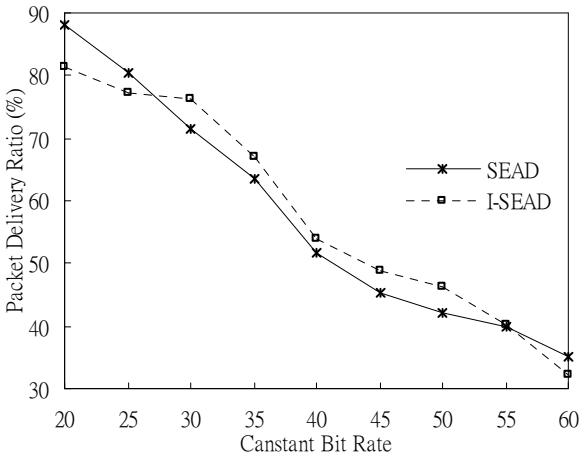


Figure 10. Packets Delivery Ratio on I-SEAD and SEAD (Capability)

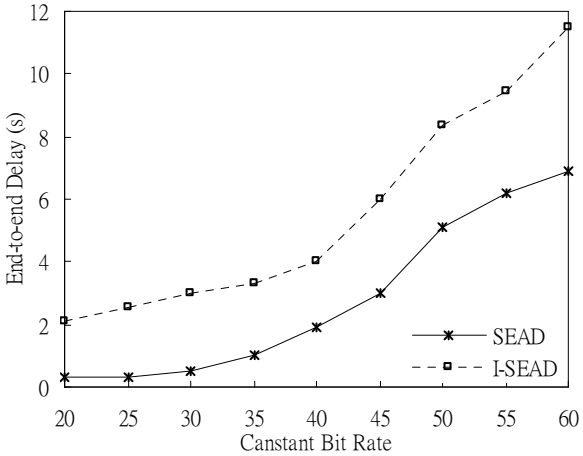


Figure 11. End-to-end Delay on I-SEAD and SEAD (Capability)

5. Conclusions

This paper has presented the design and evaluation of I-SEAD. Our routing protocol is based on the SEAD to provide security and bring more benefit. I-SEAD provides the authentication mechanism to prevent the malicious node from tampering the next hop or destination field in route update.

We compare I-SEAD to SEAD and evaluate the effect of them. We find that the I-SEAD in scalability, mobility or capability, has better performance but it costs some time to keep the secure route. We analyze the results of the evaluations, and we think the time cost is worthwhile.

Achieving a secure routing protocol is an important task that is being challenged by the unique characteristics of the ad-hoc network. Our next research interest is to propose a secure routing protocol with the least time cost.

6. Acknowledgement

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under grants NSC-95-2218-E-001-001, NSC-95-2218-E-011-015, iCAST NSC96-3114-P-001-002-Y, NSC95-2221-E-029-020-MY3, and NSC 97-2221-E-029 -023.

7. References

[1]A. Perrigy, R. Canetti, D. Song, and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proceedings of Network and Distributed System Security Symposium, NDSS 2001, February 2001.
[2]Y. C. Hu, A. Perrig, and D. B. Johnson, "Efficient Security Mechanisms for Routing Protocols," *Proceedings of the Tenth Annual Network and Distributed System Security Symposium, NDSS 2003*.
[3]Y. C. Hu, A. Perrig, and D. B. Johnson, "ARIADNE: A Secure OnDemand Routing Protocol for Ad Hoc Networks," *MobiCom'02*, Atlanta, Georgia, USA, September 23-26, 2002.
[4]Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *IEEE Infocom 2003*.
[5]Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Ad Hoc Networks Journal*, 1, 2003, pp.175-192.
[6]Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," *ACM Workshop on Wireless Security (WiSe 2003)*.
[7]Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," *Network and Distributed System Security Symposium*, NDSS '01, February 2001, pp.35–46.
[8]Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," *IEEE Symposium on Security and Privacy*, May 2000, pp.56–73.
[9]C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," *SIGCOMM Conference on Communications Architectures, Protocols and Applications*, Aug. 1994, pp. 234-244.

Authors

Wei-Shen Lai received his B.S. and M.S. degrees in computer science and information engineering from Feng Chia University and National Chiao Tung University, respectively. In 2002, he received his Ph.D. degree in computer science and information engineering from National Chiao Tung University, Taiwan. In 2004, he has been a faculty of the Department of Information Management, Chienkuo Technology

University. His current research interests include network security and cryptography.

Chu-Hsing Lin received both of his B.S. and M.S. degrees in applied mathematics from National Tsing Hua University and National Chung Hsing University, respectively. In 1991, he received his Ph.D. degree in computer sciences from National Tsing Hua University, Taiwan. Since then he has been a faculty of the Department of Computer Science and Information Engineering, Tunghai University. Dr. Lin is currently a professor and the chair of the CSIE department of Tunghai University. From 1995 to 1999, he has ever been the Director of the Computer Center of Tunghai. He has also been one of the Board Directors of the Chinese Information Security Association (CCISA) from 2001 till now. Dr. Lin has published over 50 papers in academic journals and international conferences. He has received over twenty project grants from government departments and private companies in recent years. In 2006, he was awarded the Outstanding Instructor Award of Master & Ph.D. Thesis by the IICM (Institute of Information & Computing Machinery). He was the winner of the 1991 Acer Long-Term Award for Ph.D. Dissertation. His current research interests include multimedia information security, wireless ad hoc networks, embedded systems applications.

Jung-Chun Liu received his B.S. degree in electrical engineering from National Taiwan University in 1990. He received M.S. and Ph.D. degrees from the Electrical and Computer Science Engineering Department at University of Texas at Austin, in 1996 and 2004, respectively. He is an assistant professor in the Computer Science Department at the Tunghai University, Taiwan. His research interests include digital signal processing, VLSI design, RF and microwave engineering, watermarking, embedded systems, and computer networks.

Yen-Lin Huang received both of her B.S. and M.S. degrees in computer science and information engineering from Tunghai University in 2005 and 2007, respectively. Under the instruction of her adviser Professor Chu-Hsing Lin, she has published two international conference papers. The topics of her research interests include security of firewall, mobile networks, routing protocols, digital signature, key agreement, and secure routes. Her current research focus on the analysis and improvement of the routing protocols for wireless ad hoc networks.

Mei-Chun Chou received her B.S. degrees in computer science and information management from Providence University in 2006. She is pursuing M.S. degrees in computer science and information engineering at Tunghai University. Under the guidance of Professor Chu-Hsing Lin, she has already published two international conference papers. The topics of her current research interests include ad hoc network routing and secure routing protocol.