한국항행학회 논문지 제11권 제1호 2007년 3월

안전한 무선 Multihop Ad hoc 네트워크를 위한 연구

Investigation of Secure Wireless Multihop Ad hoc Network

이 상 덕*, 박 종 안*, 한 승 조*, 변 재 영*

Sang-Duck Lee*, Jong-An Park*, Seung-Jo Han* and Jae-Young Pyun*

요 약

에드혹 네트웍은 동적으로 노드들을 조직화하고 네트워크 토폴로지를 사람들과 장치들 사이에 통신 인프라 없이 네트워킹이 가능하도록 하는 무선 모바일 시스템이다. 애드혹 네트워크 시스템이 매력적인 솔루션이지만 상업적으로 성장하는 것을 방해하는 결점들이 존재하며 이 결점들의 주된 문제는 보안에 관련된 것이다. 애드혹 네트워크 시스템은 평상 보안 공격에 취약하다고 알려져 있는데 이는 집중화된 키 분배센터와 노드들이 암호화 키와 디지털 증명서를 제공하기 위한 신뢰된 인증권한을 확립하기 어렵기 때문이다. 애드혹 라우팅 프로토콜 상에서 공격을 예방하기 위해 많은 알고리즘들이 사용되고 있으며, 본 논문에서 우리는 무선 멀티-홉 네트워크상에서 데이터를 안전하게 전송하는 시큐어 프레임워크에 대해 기술했고 기존의 존재하는 소스 라우팅 스키마와 제안된 스키마를 시뮬레이션 결과로 비교했다.

Abstract

An ad hoc network is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies allowing people and devices to internetwork without any preexisting communication infrastructure. Although ad hoc network is attractive solution, there are still some major flaws that prevent commercial growth. Security is one of these main barriers; ad hoc networks are known to be particularly vulnerable to security attack. It is difficult to establish a centralized key distribution center and a trusted certification authority to provide cryptographic keys and digital certificates to nodes. To prevent attacks in ad hoc routing protocols, many algorithms have been used. In this paper, we have depicted a secure framework for multipath routing in wireless multihop network, which is comprehensive solution for secure data forwarding in wireless multihop networks. With the simulation results, the proposed scheme is compared with existing source routing scheme.

Key words : hoc, wireless, Secure, opnet, certification

I. Introduction

A wireless multihop ad hoc network is emerging as an important area for new developments in the ubiquitous network. An ad hoc network is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies allowing people and devices to internetwork without any preexisting communication infrastructure. The mobile devices, for instance cell phones, laptops, palmtops

* 조선대학교 정보통신공학과(Dept. Information & Communication Eng. Chousn Univ.)
· 제1저자 : 이상덕(first author)
· 교신저자 : 변재영(corresponding author)
· 접수일자 : 2007년 1월 24일

remote systems, etc. carry out communication with other nodes that come in their radio range of connectivity. Each participating node provide services such as message forwarding, providing routing information, authentication, etc. to form a network with other nodes spread over an area. This requires routing mechanism on each mobile device in the ad hoc network. The earlier protocols like AODV (Ad-hoc On-demand Distance Vector) [1] and DSR (Dynamic Source Routing) [2] concentrated only on efficient routing.

Although the principle of wireless, structureless, dynamic networks is attractive, there are still some major flaws that prevent commercial growth. Security is one of these main barriers; wireless multihop networks are known to be particularly vulnerable to security attack. It is difficult to establish a centralized key distribution center and a trusted certification authority to provide cryptographic keys and digital certificates to nodes. In this paper we provide a framework which enables wireless multihop ad hoc network with end-to-end secure data transmission.

Ⅱ. Ad hoc Security Threats and Preventions

Mainly attacks targeting ad hoc routing protocols are eavesdropping, modification, fabrication, replay, impersonation/non-repudiation, dropping of packets and denial of service.

Eavesdropping - The only way by which the protocol can prevent attack is encryption of packets.

Modification- This can be prevented by generating a hash with a key shared with the destination and sending the hash along with the packet.

Fabrication - This can be prevented by signing the packet with the sender's secret key. Solution to modification also solves this problem because the attacker doesn't know the shared key and will not be able to generate the hash of the generated packet.

This can be easily prevented by putting sequence numbers in the packets and then hashing the packet.

Impersonation/Non-Repudiation - Since all the packets are hashed with the shared key and each pair of devices will have different shared key, impersonation is prevented.

Denial of Service - There can be two kinds of denial of service attacks. First one is that the attacker can change the secret key shared between the source and the destination without the knowledge of source and prevent source from communicating with the destination. This can be prevented if the protocol to change the secret key is robust enough and doesn't allow attacker to interrupt it. Second one is that the attacker can flood the network or one destination with a lot of packets to process and prevent all other nodes from communicating with a destination. This can be prevented by keeping track of number of packets coming from a node within some time period. If there is a sudden deviation, the packets can be ignored.

Dropping of Packets - There can be three kinds of attacks. a) The malicious node drops all the packets. This kind of attacks can easily be prevented by using watchdog mechanism described in [3]; b) The malicious node drops only data packets but not control packets; and c) The malicious node drops packets randomly. For b) and c), there is one robust solution as given in [4]. We can divide the packets sent to the destination in several fragments with some redundancy which will enable the destination to recreate the packet even though only part of the fragments is received. As the communication increases, the malicious nodes would be isolated and the good put will increase.

Ⅲ. Ad hoc Security Schemes

3-1 Secure routing

Routing of packets form a basis of the wireless multihop ad hoc network, where intermediate nodes route the data from the source to the destination.

Assumption is that encryption keys have already been established between the communicating nodes [5]. The efficient packet routing is one of the crucial functionalities required in the ad hoc network. It includes monitoring network traffic, prioritizing the sending of the data packets, authenticating the packets from legitimate nodes, and keeping track of updated routes [6].

There are many algorithms that provide security on top of two major routing protocols Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR) such as SAR [7], SRP[8], ARAN[9], ARIADNE[10], Protocol resilient to Byzantine failures [11], SEAD [12] and SAODV [13].

3-2 Secure data forwarding

Secure routing is the pre-requisite for implementing secure data forwarding [5]. The motivation is to securely forward data in wireless multihop ad hoc networks in the presence of malicious nodes after the route between the source and target is discovered. There are various schemes proposed for secure data forwarding such as data forwarding based on neighbor's rating, implementing currency system in network for packet exchange, and redundantly dividing and routing message over multiple network routes.

Secure Message Transmission (SMT) [4] is a secure data forwarding scheme in which first the active paths are discovered between two nodes using secure routing protocol.

IV. Related Works

Security issues in wireless multihop ad hoc networks have been studied [14] [15] and many protection schemes have been proposed. [3] [4]

In case of single path routing, various mechanisms to prevent attacks on routing and data transmission in ad hoc networks have been proposed. To detect and mitigate the routing misbehaviors in ad hoc networks, the authors have proposed a reputation-based scheme composed of two modules called watchdog and pathrater. [3] Two network-layer acknowledgement -based schemes, TWOACK and S-TWOACK, are proposed in [16] to detect the selfish nodes that refuse to forward data packets for others, and alleviate the problem using a reputation-based system.

In wireless ad hoc network, multiple paths have been utilized as a means to tolerate path breakages due to mobility. One such scheme proposes the use of diversity coding and provides an approximation for the probability of successful data transmission [17].

In case of multipath routing, several protocols using multiple paths between source and destination to provide secure data transmission in wireless ad hoc networks have been studied. Zhou and Haas [15] initially proposed using multiple routes between nodes to defend routing against denial-of-service (DOS) attacks.

Recently, several studies have been conducted on providing protection on data transmission by using multiple node-disjoint paths between the source and the destination. [4] [18]

Papadimitratos and Haas [4] have presented and evaluated the Secure Message Transmission (SMT) protocol, which fights against malicious behavior of intermediate nodes on data transmission in the network.

Lou et al. [18] propose and investigate a scheme called SPREAD, which provides further protection to the existed data confidentiality service in an ad hoc network using multipath routing. It aims to protect secret message from being compromised. A secret message is transformed into multiple shares using the threshold secret sharing algorithm, are delivered via multiple node-disjoint paths to the destination. As the shares are delivered through multiple node-disjoint paths, the secret message as a whole is not compromised even if a small number of shares are compromised.

Ⅴ. Secure Framework for Multipath Multihop Network

Viewing at the attacks and their solutions in wireless multihop network, it can be seen that there must be at least a pair of key shared between the source and the destination to authenticate each other and to provide secure transmission. This gives the minimal requirement for the secure framework in the wireless multihop ad hoc network.

In this paper, we propose a secure framework for wireless multipath multihop ad hoc networkin order to protect the data transmission against misbehaving nodes.

5-1 Overviews

This proposed framework can be worked on any on demand protocols. In our case we have chosen a source routing protocol. The proposed framework has four operations: Route Discovery, Session Establishment, Data Forwarding and Route Maintenance.

5-2 Route Discovery

Route Discovery for multipath routing in wireless multihop ad hoc network is as follows: The route from source S to destination D will be obtained by flooding the network with RREQ packets. When a node receives an RREQ packet with source address S and destination address D, it looks at its Intermediate node table. Intermediate node table maintains the list of recent most RREQ received for any source destination pair and the intermediate nodes for the request. If the packet arrived has a list of intermediate nodes that is a superset of what is there in the routing table, the packet is discarded else the node adds its own entry into the packet and rebroadcasts it.

Suppose an intermediate node 3 receives the RREQ directly from 1. When the same RREQ packet with intermediate nodes {1,2} arrives from node 2, node 3 discards it because {1,2} is a superset of {1}.

An intermediate node 5 receives RREQ from neighboring nodes 2, 3, 4 and 6. For RREQ from nodes 2 and 3, since none of the intermediate node list is a subset of other, 5 broadcasts both RREQ and makes an entry in its intermediate node table for both the packets. Whereas for RREQ from nodes 4 and 6, node 5 discards both of them because route paths created by nodes 4 and 6 are supersets of those by nodes 2 and 3 respectively.

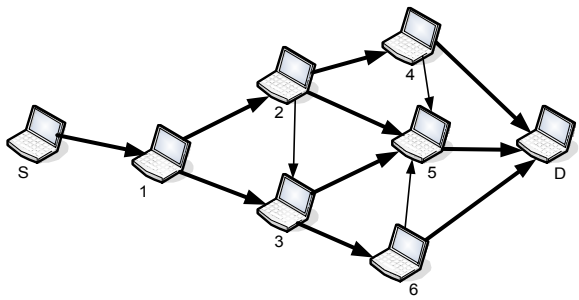

Fig. 1. Route Discovery

Now when D receives RREQ packets from its neighboring node, it sends RREP for each packet on the same path from which it has received RREQ. Thus S receives RREP packets in different route paths. In this case, 4 different route paths are created - {1,2,5}, {1,3,5}, {1,3,6} and {1,2,4} RREP comes very early and S can start communicating with D through that path. But as soon as the other RREP comes, S starts using that too for communication. Route discovery process is shown in Fig 1.

5-3 Session Establishment

The framework uses authentication scheme as stated in [19] to establish a session. Session establishment has two phases: registration, and authentication.

5-3-1 Registration phase

In registration phase, when S wants to communicate with D, it needs to provide a pair of Identity and password to the targeted D. This phase is carried out only once in the secure channel. S generates ID and PW and it calculates HPW = h(ID + PW). S sends ID, HPW to D which stores them in session table for future use.

S D : ID, HPW (in secure channel)

5-3-2 Authentication phase

In authentication phase, when S wants to communicate with D, the following steps will occur:

S generates a random number Rs and sends ID, Rs HPW, h(Rs) to D.

S D : ID, Rs HPW, h(Rs)

D calculates RS by doing (Rs HPW) HPW because it already has HPW from registration sub-phase. It verifies RS with the received h(Rs). If it is true, it generates a random number Rd. It sends Rd HPW, h(Rs + Rd) to S. It also calculates AUTH'=h(HPW + Rs + Rd). If not verified, it just discards.

D S : Rd HPW, h(Rs + Rd)

Then S calculates Rd by conducting (Rd HPW) HPW. It verifies Rd with the received h(Rs + Rd). If it is verified, it calculates AUTH=h(HPW + Rs + Rd) and sends ID, AUTHto D. If not verified, it restarts the Authentication sub-phase.

S D : ID, AUTH

Finally D compares received AUTH with AUTH'generated before. If it is matched, the source is verified and the session is established. Otherwise, it just discards.

5-4 Data Forwarding

In data forwarding, source S and the destination D uses keys Rs and Rd respectively to encrypt and hash packets transmitted. Apart from doing encryption and hashing, the packets would be divided in n fragments that would be sent to the destination on ndifferent routes. This operation follows the approach explained in Secure Message Transmission [4]. The list of routes would be maintained in the routing table along with the path rating of each route. If the path rating falls below a threshold, the path is removed from the routing table.

To send message M to D, S carries out the following:

Divides the packet in a set of n fragments {g0, g1, ···., gn-1} with redundancy factor r. Thus the resultant length of each fragment would be

len(gi) = r len(M)/n 0 i < n

Encrypts each fragment with Rs i.e. it calculates encrypted fragment

Egi = E (gi + i + n + N, Rs) ; 0 i < n

It generates the hash of Egi + Rdand appends it with the packet i.e. it calculates h(Egi + Rd) and sends Egi + h(Egi + Rd) to D on path i.

S D : Egi + h(Egi + Rd)

After sending the packets, S starts a timer. If it doesn't receive any acknowledgement from D till the timer expires, it decreases the rating of the path equivalent to 1 failure and sends the packet again with new rating of routes. If S doesn't receive any acknowledgement from D for T retries, it restarts the route discovery.

If S receives an acknowledgement from D with some delivered and some lost fragments, it resends the fragment i that was lost on the path j that delivered the fragment j.

Routes that delivered fragments successfully will have their rating in the routing table incremented by Vsuccand the routes that failed will have their rating decremented by Vfail. If the rating falls below zero, the path would be discarded.

When D receives any packet from S from path i

D generates h(Egi + Rd) and compares it with the received. If they match, the packet must be from S and

not from any other node.

Decrypts packet i.e. it calculates gi + i + n + N = D(Egi, Rs).

Compares calculated N with the sequence number K of the last packet received from S stored in the routing table. If N = K+1, (re)starts a receiver timer otherwise it discards the packet and sends a negative acknowledgement for sequence number K+1 to the source. The value of the receiver timer is dependent on the value of TDmax for the source.

As soon as D receives P/n packets with sequence number N and different i's, it reconstructs M, discards all the fragments and starts processing M.

If D doesn't receive enough packets to reconstruct M till the receiver timer expires, it sends the acknowledgement of the received fragments to S.

5-5 Route maintenance

Since the route discovery and session establishment are independent of each other, if the routes break because of mobility of nodes, the routes can be reestablished without reestablishing the session. Whenever a route breaks because of mobility of a node, the neighbor of the node will send a route error to the source. The source will then discard that route from the routing table.

VI. Performance Evaluation

6-1 Scenerio

In order to evaluate the performance of the proposed framework in wireless ad hoc network, we have designed experimental model and simulated using OPNET Modeler. [20] We have modified DSR model to provide multipath routing protocols as per proposed framework.

Beyond the end-to-end security associations, additional trust assumptions have not been made. Each source is securely associated with one destination and sources transmit data to the same destination throughout the period.

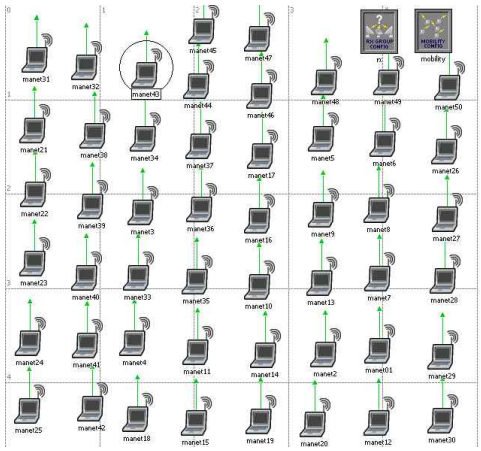

Fig. 2. Simulati1on Model

Fig. 2 shows the simulation model of the proposed framework in wireless as hoc network. In the simulation, the network coverage area is a 1000m x 1000m square with 50 mobile nodes, each having radio power range of 300m. The channel capacity is 2 Mbps. The IEEE 802.11 Distributed Coordination Function (DCF) is used as the MAC layer protocol. The nodes are initially uniformly distributed throughout the network area and their movement is determined by the random waypoint mobility model. The node speed is uniformly distributed between 0m/s and 20m/s, and the pause time is varied from 0 second to 300 seconds. 10 constant-bit-rate (CBR) sources generate 4 messages per second with data packet size of 64 bytes. The sources and destinations are chosen randomly with uniform probabilities. Each run executes 300 seconds of simulation time.

6-2 Assumptions

For the simulation, two scenarios have been designed in wireless ad hoc environment. First one is under normal condition, ie there is no misbehaving nodes, whereas second is under adverse environment, theremay be individual misbehaving node along the data forwarding path that drops all received data

packets instead of forwarding.

For the experimental evaluation, we have assumed the performance metrics in order to analyze the effect of proposed framework with single path DSR.

We have considered packet delivery rate metric to evaluate the performance of proposed framework with single path DSR under normal condition. Packet delivery rate is the total number of packets all nodes received normalized by the total number of packets they sent.

And under adverse environment, the performance metric evaluated is the data receive rate, which is the total number of data packets all nodes received normalized by the total number of data packets they sent.

6-3 Results and Analysis

In the simulation, we have examined the performance of the proposed scheme under normal and adverse environments.

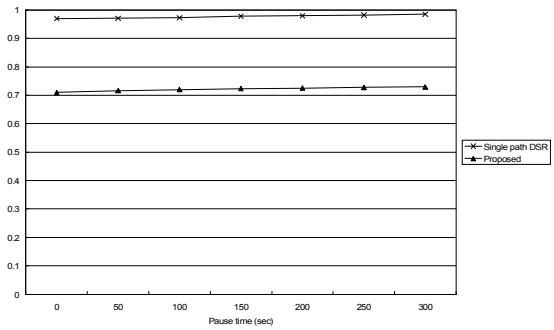

Fig. 3. Packet delivery rate

Under normal condition, the single path DSR and the proposed scheme are compared. Fig 3 shows the packet delivery rate plotted against pause time for the single path DSR and the proposed framework. It can be seen that the packet delivery rate of the proposed scheme is less than that of the single path DSR.

Hence, the proposed scheme is chosen to compare with the single path DSR under some adverse environment such as dropping data.

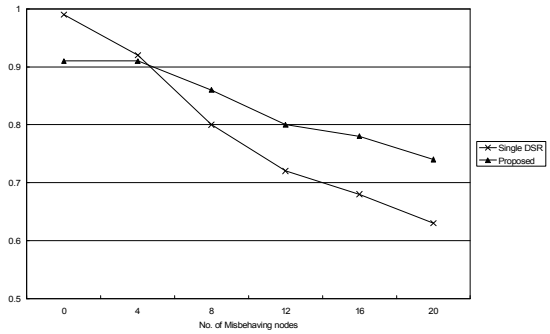

Fig. 4. Data receive rate

Fig 4 shows data receive rate plotted against number of misbehaving nodes for single path DSR and the proposed framework. It can be seen that the data receive rate in network suffering different percentage of dropping data misbehaving nodes. The percentage of misbehaving nodes in the network is varied from 0 to 20%. With the increase of misbehaving nodes in network, the data receive rate for the single DSR decreases dramatically while those for the proposed scheme is affected in a much lesser extent.

VII. Conclusion

In this paper we have depicted a secure framework for multipath routing in wireless multihop network, which can be seen as a comprehensive solution for secure data transmission in wireless multihop ad hoc networks. The algorithm is lightweight as it uses only hash and encryption techniques.

We have simulated the experimental scenarios with implementation of proposed scheme and single path DSR in wireless ad hoc network. It can be seen that under adverse environment with the increase of misbehaving nodes in network, the data receive rate for the proposed scheme is affected in a much lesser extent.

참 고 문 헌

[1] C.E Perkins and E. Royer, Ad-hoc on-demand distance vector routing, *Proceedings of the 2nd IEEE Worksho*

p on Mobile Computing Systems and Applications, Fe b. 1999, pp 90-100

[2] D. Johnson and D. Maltz, Dynamic source routing in ad hoc wireless networks, Mobile Computing, Vol. 353, 1996, pp. 153-181

[3] S. Marti, T.J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehaviour in Mobile Ad hoc Networks. Proceedings of the Sixth Annual IEEE/ACM Internati onal Conference on Mobile Computing and Networkin g (MobiCom 2000), Aug. 2000 pp. 255-265

[4] P. Papadimitratos and Z. Hass, Secure Message Trans mission in Mobile Ad hoc Networks, Elsevier Ad hoc Networks Journal, 1(1), 2003

[5] P. Papadimitratos and Z. Hass, "Securing Mobile Ad Hoc Networks", *The Handbook of Ad Hoc Wireless Networks,* M. Ilyas, Ed. Boca Raton: CRC Press, 2002

[6] H. Yang, H. Luo, F. Ye, S. Lu, and U. Zhang, "Securit y in Mobile Ad Hoc Networks: Challenges and Solutio ns", *IEEE Wireless Communications,* Vol. 11, No. 1, Feb. 2004, pp. 38-47

[7] S. Yi, P. Naldurg, and R. Kravets, A Security Aware Ad hoc Routing Protocol for Wireless Net-works, The 6th World Multi-Conference on Systemic, Cybernetics and Informatics (SCI 2002), 2002

[8] P. Papadimitratos, and Z. Haas, Secure Routing for Mobile Ad hoc Networks, SCS Communication Netw orks and Distributed Systems Modeling and Simulatio n Conference (CNDS 2002), San Antonio, USA,Jan. 2002

[9] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E.M. Belding-Royer, A Secure Routing Protocol for Ad hoc Networks, Proceedings of 2002 IEEE Internati onal Conference on Network Protocols (ICNP), Nov. 2002

[10] Y.C. Hu, A. Perrig and D. B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Net works, Springer Wireless Networks, Vol 11, Nos 1-2 / Jan. 2005, pp. 21-38

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On demand Secure Routing Protocol resili ent to Byzantine failures, Proceedings of ACM Works hop on Wireless Security (WiSe'02), Atlanta, USA, Sep. 2002

[12] Y.C. Hu, D. B. Johnson, and A. Perrig, SEAD: Secure Efficient distance vector routing for mobile Ad hoc Networks, Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCS A 2002), IEEE, Calicoon, NY, Jun. 2002, pp. 3-13

[13] M. G. Zapata, and N. Asokan, Securing ad hoc routin g protocols, Proceedingsof the 3rd ACM workshop on Wireless security WiSe'02, Atlanta, USA, Sep 200 2

[14] F. Stajano and R. J. Anderson. The resurrecting duckli ng: Security issues for ad-hoc wireless networks. Proc. of 7th Security Protocols Workshop, Lecture Notes in Computer Science Vol. 1796, 1999, pp. 172–194.

[15] L. Zhou, and Z. J. Haas, "Securing ad hoc networks", *IEEE Network,* Nov/Dec 1999, pp 24-30.

[16] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWO ACK: Preventing Selfishness in Mobile Ad Hoc Netw orks," *in Proc. of IEEE Wireless Communications & Networking Conference (WCNC'05),* Vol. 4, New Orle ans, USA, Mar. 2005, pp. 2137-2142.

[17] A. Tsirigos, Z.J. Haas, Multipath routing in the presen ce of frequent topological changes, *IEEE Comm.* Nov 2001, pp. 132–138.

[18] W. Lou, W. Liu and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks", *Proc. of IEEE INFOCOM 2004,* Vol 4, Hong Kong, China, Mar 2004, pp. 2404–2413

[19] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, A Secure User Authentication Scheme using Hash Functions, A CM Operating System Review, Vol 38, No 2, Apr. 2004

[19] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, A Secure User Authentication Scheme using Hash Functions, A CM Operating System Review, Vol 38, No 2, Apr. 2004

[20] William Stallings, Network and Internetwork Securit y, Prentice Hall, 1995

이 상 덕 (李相德)

1997년 2월 : 조선대학교 전자공학과 학사
1999년 2월 : 조선대학교 대학원 전자공학과 석사
2000년 2월 ~ 현재 : 조선대학교 대학원 전자공학과 박사과정
2005년 ~ 현재 : 조선대학교 정보통신공학과 외래교수

관심분야 : 네트워크 및 시스템보안, 임베디드 시스템, DRM

박 종 안 (朴鍾安)

1975년 2월 조선대학교 공과대학 전자공학과 공학사
1978년 2월 조선대학교 공과대학 전기공학과 공학석사
1986년 2월 조선대학교 공과대학 전기공학과 공학박사
1983년~1984년 미국 Massachus sette주립대학 전기&전자공학과 객원교수
1990년~1991년 영국 Surrey 주립대학 전기 & 전자공학과 객원교수
1975년~현재 조선대학교 전자정보공과대학 정보통신공학과 교수

관심분야 : 디지털신호처리, 멀티미디어 영상처리

한 승 조 (韓承朝)

1980년:조선대학교 전자공학과
1982년: 조선대학교전자공학과 석사
1994년: 충북대학교 전자계산학과 박사
1986년 6월 ~1987년 3월: 뉴올리언스대학 객원교수
1995년 2월~ 1996년 1월: 텍사스대학 객원교수
2000년 12월~2002년 2월: 버클리대학 객원교수
2005년 11월~ 현재 조선대학교 정보전산원장
1998년 3월 현재: 조선대학교 전자정보통신공학부 정교수

관심분야 : 정보보안, 컴퓨터네트워크, DRM, S/W 불법복제방지시스템

변 재 영(邊宰瑩)

1997년 2월 : 조선대학교 전자공학과 졸업
1999년 2월 : 전남대학교 전자공학과 석사
2003년 8월 : 고려대학교 전자공학과 박사
2003년 9월 ~ 2004년 2월 : (주) 삼성전자 단말사업부 선임연구원
2004년 3월 ~ 현재 : 조선대학교 정보통신공학과 전임강사/조교수

관심분야 : Mobile QoS, IP QoS, Video communication, Video compression, Wireless communication, Sensor network