무선 센서네트워크를 위한 신뢰성 있는 2-모드 인증 프레임워크

A Reliable 2-mode Authentication Framework for Wireless Sensor Network

후엔 뉴엔* 허 의 남**
Nguyen Thi Thanh Huyen Eui-Nam Huh

요 약

본 논문은 다양한 공격들(헬로우 플러딩공격, 위치배치공격, 웜홀 공격, 싱크홀 공격, 중간포획공격)로부터 안전한 방어를 보장해야 하는 무선센서네트워크상에서 확률적 키 사전분배를 위한 신뢰성있는 2-모드 인증 프레임워크를 제안한다. 신뢰하는 이웃 노드의 ID를 저장하는 본 기법은 클러스터 헤드에서의 의존성을 감소시키며, 그 결과로 인증처리를 위한 단대단 전송을 제공할 뿐 아니라 소모되는 전력 에너지도 절약한다.

Abstract

This paper proposes a reliable 2-mode authentication framework for probabilistic key pre-distribution in Wireless Sensor Network (WSN) that guarantees the safe defense against different kinds of attacks: Hello flood attacks, Wormhole attacks, Sinkhole attack, location deployment attacks, and Man in the middle attack. The mechanism storing the trust neighbor IDs reduces the dependence on the cluster head and as the result; it saves the power energy for the authentication process as well as provides peer-to-peer communication.

☞ keyword : reliable 2-mode authentication, probabilistic key pre-distribution, wireless sensor network, trust, cluster

Ⅰ. introduction

The sensor networks comprise a large number of sensor nodes collecting environment data in widespread applications such as healthcare, environment monitoring, trading, and military, etc. The inherent resource and computing constraints of sensors make security in WSN arduous. There are two kinds of security protocols: the public key and the symmetric key. In spite of the recent efforts in [1-3] to reduce the computation and energy cost of the public key operations, the public key protocols are unsuitable in wireless sensor networks due to private key operations are still expensive. Symmetric cryptography is, therefore, the typical choice for applications that cannot afford the computational complexity of asymmetric cryptography. However, the authentication mechanisms of the existing symmetric key protocols are not really efficient. The third trust party based authentications like PIKE [4], LEAP [5], SPIN [6], and Zigbee [7] limit the peer-to-peer communication, whilst non-station mechanisms [8-10] support only for a small number of nodes without mobile sensors. Basing on the real that the frequent communications are between the neighbor nodes and the trust neighbor nodes might be determined before deployment, we propose a 2-mode ID based authentication approach working two databases: the frequent and small one on each

* 준 회 원 : 경희대학교 컴퓨터공학과 석사과정
huyen@khu.ac.kr
** 종신회원 : 경희대학교 컴퓨터공학과 교수
johnhuh@khu.ac.kr(Corresponding author)
[2008/11/13 투고 - 2008/11/18 심사 - 2008/11/21 심사완료]

sensor and the full one on the cluster head. This mechanism increases the independence on the stations, provides the reliable authentication for the mobile sensor nodes, as well as reduces the information flows through peer-to-peer communications between trust neighbor nodes. We apply this model to the signal -range- based scheme [11] and do analysis on five potential popular attacks: Hello flood attacks, Wormhole attacks, Sinkhole attack, location deployment attacks, and Man in the middle attack to evaluate the performance and the resilience of the scheme. The remainder of this paper is organized as follows: In section II, we look at the related works and their drawbacks. The proposed scheme is shown in section III and its analysis in section IV. Finally, we present the conclusions in section V.

Ⅱ. RELATED WORK

In this section, previous research reports related to key management and authentication in WSN security are reviewed. Eschenauer and Gligor (EG) [8] proposed the basic probabilistic key pre-distribution where each node stores a random subset of keys from a large key pool before deployment. As a result, two nodes have a certain probability to share at least one key after deployment. Chan et al. [9] extended this scheme to enhance the security and resilience of the network significantly by requiring at least two common shared keys for authenticated communication and updating communication keys for subsequent communications. The communication is authenticated with a key in these schemes but node identities are uncertain; thus, Chan et al. [4] further advocate a random pair wise key scheme –PIKE- that allows only two nodes to share the value of a particular key and supports key revocation by either a base station or neighboring nodes. The disadvantage of PIKE is it requires the trust from the third intermediary nodes for authentication.

Watro et al. [12] developed the TinyPK system that requires each node to be preloaded with a static Diffie-Hellman key pair and a node identity string processed by a Certificate Authority's private key allowing node authentication. Perrig et al. [6] propose the SPINS Secure Network Encryption Protocol (SNEP) and the μTimed, Efficient, Streaming, Loss-tolerant Authentication (μTESLA) components as building blocks for securing sensor networks. The SNEP component offers semantic security with an incremented counter that causes a different encryption result for the same message content, a Message Authentication Code (MAC) for verification of sending and receiving nodes, replay protection, and weak assurance of data freshness via use of the encrypted counter. The μTESLA component associates symmetric key release to a particular time interval; thus allowing recognition and denial of a spoofed packet using a key after time interval expires.

Du et al. [13 - 14](DDHV, DDHV-D), Liu et al. [15-16], Zhou et al. [17], and Li et al. [18], Nguyen [19] utilize deployment knowledge to improve the probability of the key sharing and enhance the resistance to node capture. Carman [20] combined the benefits of both identity-based cryptography and random key pre-distribution into ID based authentication framework for wireless sensor network. A survey of key management in ad hoc networks is given in [21]. The latest survey of security issues for WSNs is presented in [22-23].

Ⅲ. Network architecture

In this section, we present and discuss the proposed scheme. Before that, we introduce the following symbols and notations that will be used throughout this paper as shown in Table 1.

(Table 1) Symbols

Symbol	Meaning
L	The length of a cell
r	The signal range of a node (or communication range)
K_E	Encryption key
K_A	Authentication key
s_{AB}	The number of sharing keys between two nodes, A and B
m	The size of the ring
k	The overlap keys
S_i	The key space of group Gi
e	Deployment error
a	Constant
F_A, F_E, F	One-way hash functions for authentication, encryption and key retrieval

3.1 The 2-mode authentication for 3-tier network

A large number of resource limited sensor nodes are randomly scattered around an adversarial area. Nodes within a sensor network can communicate with each other without a fixed infrastructure. They are wirelessly linked to base station that collects data from the sensor network for processing within a wired infrastructure. In the hazardous target environment like in army applications, the mobile cluster heads are replacements for the fixed stations. These mobile cluster heads are deployed with the sensors and equipped with two kinds of keys: the asymmetric keys and symmetric keys. The asymmetric keys are necessary for data exchange between the clusters whilst the symmetric keys support communication between sensor nodes. To provide a lightweight solution for these cluster heads, the number of symmetric keys can be optimized by using the signal-range based key distribution scheme mentioned in [11], [18]. As the calculation in section 3.2, the number of keys for each cluster can be reduced about kNcl keys. These mobile cluster heads play the role as intermediary nodes forwarding information to base-station. They provide partly authentication to untrust nodes in cluster. Cluster heads and nodes constitute to the hierarchical communication like in the ad-hoc network. The ID based authentication context for this hierarchical network is as follows:

Pre-communication phase:

Step 1: The sensor nodes announce themselves with other neighbor nodes through using Hello messages and their IDs.

Step 2: The neighbor nodes exchange the IDs to discover if they share the common keys.

Step 3: If the common keys exist, these IDs are kept at the node as the trust allies and a path in the communication graph is established.

Step 4: Basing on the graph, the routing algorithms are used to find the routine to the cluster head. This routing information is updated at each node's routing table.

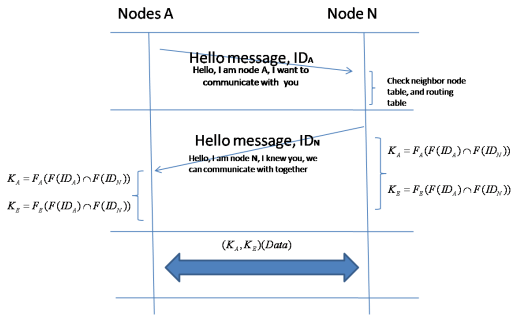
Communication phase:

The sensor node A wants to communication with node B or cluster head H. Firstly, he finds in his database the possible neighbor nodes N, then sends Hello messages to those nodes.

- If A is a trust neighbor of node N, node N sends the hello message with his ID to A, in the mean time he calculates the authentication key KA and encryption key KE

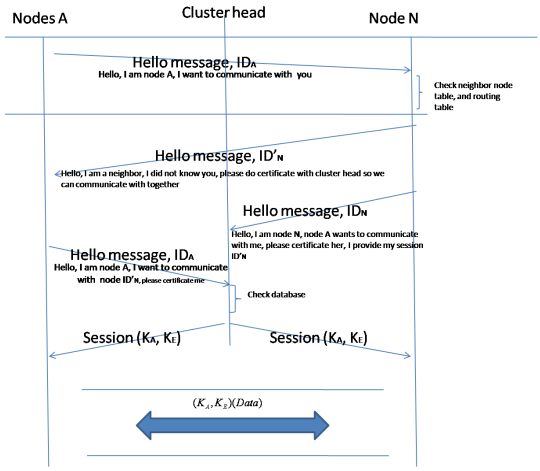
$$K_A = F_A(F(ID_A) \cap F(ID_N))$$
$$K_E = F_E(F(ID_A) \cap F(ID_N)) \quad (1)$$

where FA, FE, and F are the one-way hash functions for authentication, encryption and key retrieval [20]. At the next step, KA and KE are used for encryption and authentication between node A and N through MAC mechanism. The peer - to-peer communication between the trust neighbor nodes is established as Fig. 1.



(Fig 1) Communication protocol between two trust nodes.

- If A is not a trust neighbor of node N, node N sends the hello message with his session ID'_N to A to notify that initially A should authenticate with cluster head. Meanwhile, he sends hello message to cluster head to announce that A wants to communicate with him and provide his session ID'_N. Node A also sends hello message to cluster head to require an authentication for her. Cluster head checks the database then provides the session encryption keys and session authentication keys. Node A and N use these keys to encrypt and authenticate with MAC mechanism. The prototype for station-based authentication is described as in Fig. 2.



(Fig 2) Communication protocol between two unknown nodes through cluster head.

3.2. The key assignment for cluster head

The number of keys assigned for cluster heads is calculated as follows:

- N_{cl} is the number of nodes in each cluster; Si are the keys assigned for each node, Sclh are the keys assigned for each cluster head, we have

$$S_{clh} = \bigcup_{i=1}^{N_{cl}} S_i \tag{2}$$

- Assumed Nclr and Nclc are respectively the number of nodes in the row and the column of the grid area that the cluster head is the centre. Because two neighbor nodes share k keys, the number of different keys in one row is as follows:

$$S_{clhr=1} = S_{1,1} \cup \bigcup_{i=1}^{N_{clc}-1} (m-k) K_{S_{i+1,1}|S_{i,1}} \tag{3}$$

Where $K_{S_{i+1}|S_i}$ are the keys appearing in $S_{i+1,1}$ not

in $S_{i,1}$

- The nodes at the second row are k keys different with the node in the same column at the first row, so we have

$$S_{clh} = \bigcup_{j=1}^{N_{clr}-1}(S_{1,j} \cup \bigcup_{i=1}^{N_{clc}-1}(m-k)K_{S_{i+1,j}|S_{i,j}}) = \bigcup_{j=1}^{N_{clr}-1}(S_{1,1} \cup (m-k)K_{S_{1,j+1}|S_{1,j}} \cup \bigcup_{i=1}^{N_{clc}-1}(m-k)K_{S_{i+1,j}|S_{i,j}}) \quad (4)$$

- To increase the resilience of the nodes, a mask [11] is used to cover the real relationship between the nodes, so we have:

$$S_{clh}(new) = Update(N_{cl} * \frac{\alpha}{3}, S_{clh}) \quad (5)$$

The number of keys stored in the cluster heads in formula (4) is smaller than (1) is about kNcl keys.

Ⅳ. Analysis

In this session, we will do the analysis on the three popular attacks on sensor network as follows:

- Attacks on routing mechanism
- Attacks on key distribution mechanism
- Man in the middle attacks

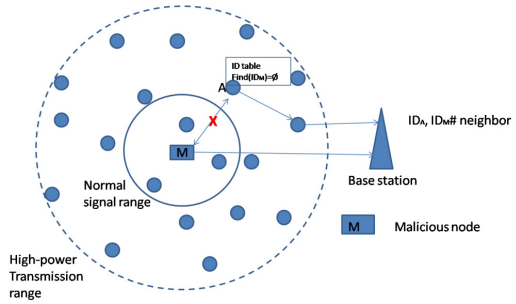
4.1 Attacks on routing mechanism.

There are several network layer attacks against sensor networks. Among them, sinkhole attacks, wormholes, HELLO flood attacks are well known attacks that try to manipulate sensed data.

a. HELLO flood attacks

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within radio range of the sender. The attacker can use a laptop-class to broadcast routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor with high quality route to destination. This may cause other nodes to follow the same route to destination. However, most messages from the legitimate nodes may not be sent to attacker as these nodes have smaller signal range.

In the proposed scheme, one node keeps the IDs of the neighbor nodes, so it only communicates with these neighbor nodes as Fig. 4. If one new node announces that it is the neighbor node then an authentication mechanism utilizing the cluster head as the trust third party to help two sensor nodes verify each other.



(Fig 3) Hello flood attacks and defense

b. Sinkhole attacks

In a Sinkhole attack, a malicious node tries to draw all or as much traffic as possible from a particular area, by making it look attractive to the surrounding nodes with respect to the routing metric. As a result, the adversary manages to attract all traffic that is destined to the base station. By taking part in the routing process, she can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through. There are two possible cases:

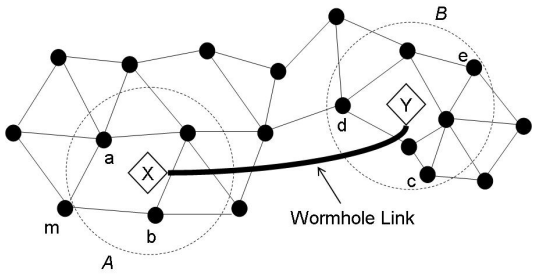
- If malicious node is a new one, as the default he may not be a reliable node, then the

message will be forwarded to other neighbor nodes.

- If the malicious node is a compromised node, then the mechanism called the ratio of routes through a particular node is used. By combining the neighbor ID table and routing table, a node will balance the frequency of data transmission to the nodes, preventing the dependence to a particular node.

In both cases, the Sinkhole attacks are dismissed.

c. Wormhole attacks

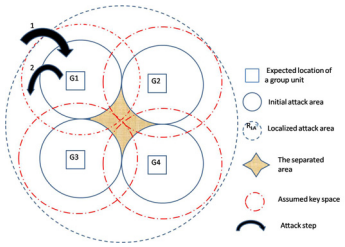


(Fig 4) Wormhole attacks

In the wormhole attacks [24], X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) as Fig 4. The effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption.

Like the sinkhole attack, wormhole attacks are prevented efficiently through the routing table and neighbor ID table.

4.2 Attacks on key distribution mechanism



(Fig 5) Localization attacks on key distribution

The adversary tries to do the localized attack through separating a number of nodes whose key spaces are broken. The radius of the attack area is RLA as described in Fig .5. The adversary does the attacks on four key spaces to create the separated area where the probability of a key string broken is higher. The context of this attack is as follows:

1. The initial attack area for each key space is assumed smaller than its real key space area.
2. The adversary in succession does the attacks to break these initial areas of G1, G2, G3, and G4.
3. After breaking all nodes in these areas, the adversary attacks the nodes outside except the nodes in the separated area.
4. The adversary basing on the broken key spaces to guess the keys are used between two uncompromised nodes in the separated area.

As presented in [8- 9], the probability that at least one space is broken is as follows:

$$P(\text{a direct key is compromised}|C_x) = wP(K \in S_1)\sum_{j=\lambda+1}^{x}\frac{x!}{j!(x-j)!}\theta^j(1-\theta)^{x-j} \quad (6)$$

where

- $P(K \in S_1)$ is the probability that the secret key K of that link is derived from S1,
- w is the number of the key spaces in the attack area,

- Cx is the event that x nodes are compromised in the attack area,
- Θ is the probability that each compromised node carries information about S1
- $\lambda = \lambda_G * 9L^2 \sum_{i=1}^{n_{skg}} i$ is the threshold for key space (pool) of group 1 being broken.
- $n_{skg} = 2\left\lceil \frac{1}{3}\left(\frac{r}{L\sqrt{2}}\right)+3 \right\rceil - 2$ as the signal-range-based scheme proposed in [11].

The number of the key spaces of all nodes deployed in this area is equal to

$$w = \frac{\pi\left(R_{LA}+e\right)^2}{9L^2\sum_{i=1}^{n_{skg}} i} \tag{7}$$

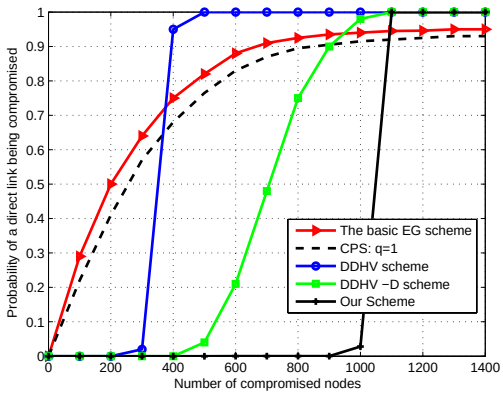
Each node carries information from 1, 2, 4 key spaces, this distribution is almost equal, so on average $\tau = 2$, we have

$$\theta = \frac{\tau}{w} = \frac{18L^2\sum_{i=1}^{n_{skg}} i}{\pi\left(R_{LA}+e\right)^2} \tag{8}$$

The probability the broken key belongs to S1, S2, S3, or S4 is equal then $P(S_1 \mid C_x) = 1$

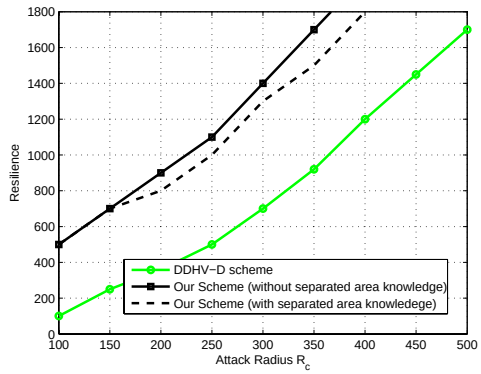
Finally, the probability of a direct link being compromised is as follows

$$P(\text{a direct link is compromised}|C_x) = w\sum_{j=\lambda+1}^{x}\frac{x!}{j!(x-j)!}\left(\frac{18L^2\sum_{i=1}^{n_{skg}} i}{\pi(R_{LA}+e)^2}\right)^j\left(1-\frac{18L^2\sum_{i=1}^{n_{skg}} i}{\pi(R_{LA}+e)^2}\right)^{x-j} \tag{9}$$



(Fig 6) The probability of a direct link being compromise versus on number of compromised nodes

The result presented in Fig 6 indicates that the probability of a direct link being compromised in our scheme in this kind of attack is higher than the existing schemes. With the same probability is equal to 0.5, the number nodes need to be compromised in our scheme is 1050, while in the others are 700, 355, 250, 200 (DDHV-D, DDHV, CPS, EG).



(Fig 7) The comparison between two kinds of attacks with the separated area knowledge

The simulation result of the comparison between two kinds of attacks with the separated area knowledge or not is depicted as in Fig 7. When the

attack radius increases, the resilience of our scheme in both two cases of attacks are better than DDHV-D scheme. The resilience against the attack using separated knowledge is a little lower than in the attack without the separated knowledge. With the same attack is 300, the numbers of nodes need to be compromised are nearly 1300, and 1400 respectively to compromise 10% direct link between two un-capture nodes.

Briefly, our scheme has the better resilience against the localized capture attack.

4.3 Man-in-middle attack

Man-in-middle attack (MIMA) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.

When two nodes exchange IDs to retrieve the common keys, the indices of keys assigned to a node are determined by the hash value of its identity (the one – way functions F, FA, FB). As the result, the share keys are different between the couple of nodes and so that MIMA attacker cannot intercept his ID as a mediate node between two communication nodes. Besides, data is encrypted with KE, and authenticated with KE through MAC mechanism. So if one adversary tries to modify the message, the terminate nodes will compare the MAC and find that the received message is not original.

In the signal-range based scheme, as the connectivity is high [10], one node has the higher probability to keep IDs of the trust neighbor. He can authenticate the sender by comparing the received ID with his neighbor IDs without base-station. Besides, the static-genuine sensors deployed at the beginning exchange data more frequently; so their peer-to-peer communications reduce efficiently the information flow in network. The mobile sensors are often higher power but also conceal the risks, therefore, they require more effort for authenticate through the cluster head as the second mode. After nodes are authenticated, they exchange data through peer-to-peer channel.

V. CONCLUSION

In this paper, a framework for security in wireless sensor network has been introduced. Its 2- mode authentication approach for 3-tier communication supports in-network processing, provides a flexible option for the security in a complex network like Ubiquitous sensor network where mobile and static sensors exist at the same time. The peer-to-peer communication optimizes the information flows in network as well as provides the safe channel, while the cluster head based authentication provide the advantages for mobile sensors. Although the security analysis was on five popular attacks, this framework can prevent against other attacks on sensor networks: like Sybil attack s, misdirection routing.

Acknowledgment

This research was partially supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2009-C1090-0902-0002) and by TTA. [22008-P1-28-08J45, The Development of Standard for Internet Infrastructure Security Technologies]

Reference

[1] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 162.175, New York, NY, USA, 2004.

[2] A. Liu and P. Ning. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In IPSN '08: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (ipsn 2008), pages 245.256, Washington, DC, USA, 2008.

[3] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus. Tinypk: securing sensor networks with public key technology. In SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pages 59.64, New York, NY, USA, 2004.

[4] H. Chan and A. Perrig, PIKE: Peer Intermediaries for Key Establishment in Sensor Networks. In IEEE Proc. the 24th Annual Joint Conference of the IEEE Computer and Communications Societies Vol. 1, pp. 524-535, 2005.

[5] S. Zhu, S. Setia, and S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks. In Proceedings of the 10th ACM conference on Computer and communications security, pp. 62 - 72, USA, 2003.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, SPINS: Security protocols for sensor networks, Wireless Networks, pp. 521-534, 2001.

[7] Zigbee Alliance, http://www.zigbee.org/en/index.asp

[8] L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks. In ACM Conference on Computer and Communications Security, pages 41.47, 2002.

[9] H. Chan, A. Perrig, and D. X. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Security and Privacy, pages 197, 2003

[10] C. Karlof, Naveen Sastry, and David Wagner, TinySec: a link layer security architecture for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems, pp. 162 – 175, USA, 2004.

[11] N. T.T. Huyen and E. Huh. An efficient signal range based key pre-distribution scheme ensuring the high connectivity in wireless sensor network. In ICUIMC '08, pages 441.447, 2008.

[12] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruss, TinyPK: Securing sensor networks with public key technology, In Proceedings of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks, pp. 59-64, 2004, USA.

[13] W. Du, J. Deng, Y. S. Han, S. Chen, and P.K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM, 2004.

[14] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In ACM Conference on Computer and Communications Security, pages 42.51, 2003.

[15] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In Processings of the 10th ACM Conference on Computer and Communications Security (CCS), 2003.

[16] D. Liu and P. Ning. Improving key predistribution with deployment knowledge in static sensor networks. TOSN, 1(2):204. 239, 2005.

[17] L. Zhou, J. Ni, and C. V. Ravishankar, Efficient Key Establishment for Group-based Wireless

Sensor Deployments. In Proc. the 4th ACM Workshop on Wireless security, pp. 1-10, 2005.

[18] G. Li, J. He, and Y. Fu, A Hexagon-Based Key Predistribution Scheme in Sensor Networks. In Proc. of the 2006 International Conference Workshops on Parallel Processing, pp. 175-180, 2006.

[19] H.T.T. Nguyen, S. Na, G. Lee, and E. Huh. Accomplishment of the key setting up: The fexible approach. The 2008 World Congress in Computer Science, Computer Engineering, and Applied Computing, July 2008, U.S.A.

[20] D.W. Carman. New directions in sensor network key management. International Journal of Distributed Sensor Networks, Volume 1:3.15, 13-5, 2005.

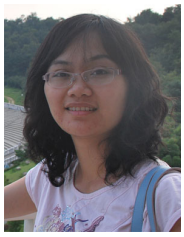
[21] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, A Survey of Key Management in Ad Hoc Networks. In IEEE Communications Surveys & Tutorials, 3rd Quarter, Vol. 8, No. 3, pp. 48-66, 2006.

[22] Y. Wang, G. Atterbury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Communications Surveys and Tutorials, 2nd Quarter, Vol. 8, No. 2, pp. 2-23, 2006.

[23] A. Vaseashta and S. Vaseashta, A Survey of Sensor Network Security. Sensors and Transducers Journal, V.7, pp. 91, 2007.

[24] R. Maheshwari, J. Gao, S. R Das, ″Detecting Wormhole Attacks in Wireless Networks using Connectivity Information″, In IEEE INFOCOM, 2007, USA

◐ 저 자 소 개 ◑



Huyen Thi Thanh Nguyen

received the B.S. degree in Computer Science from Ha Noi U. of Technology, Viet Nam (HUT), in 2006. She is now MS candidate in the Department of Computer Engineering, Kyung Hee University, South Korea. Under the guidance of Prof. Eui-Nam Huh, Her interesting study areas are: Key management, Authentication and Security protocols in Wireless Sensor Networks.

Eui-Nam Huh

has earned BS degree from Pusan National University in Korea, Master’s degree in Computer Science from University of Texas, USA in 1995 and Ph. D degree from the Ohio University, USA in 2002. He has served for the WPDRTS/IPDPS community as program chair in 2003. He has been an editor of Journal of Korean Society for Internet Information and Korea Grid Standard group chair since 2002. He was also an Assistant Professor in Seoul Women’s University, South Korea. Now he is with Kyung Hee University, South Korea as Professor in Dept. of Computer Engineering. His interesting research areas are: High Performance Network, Sensor Network, Distributed Real Time System, Grid, Cloud Computing, Network Security.