J Electr Eng Technol.2017; 12(3): 1307-1313
http://doi.org/10.5370/JEET.2017.12.3.1307

ISSN(Print) 1975-0102
ISSN(Online) 2093-7423

Towards Choosing Authentication and Encryption: Communication Security in Sensor Networks

Seongwook Youn* and Hyun-chong Cho†

Abstract – Sensor networks are composed of provide low powered, inexpensive distributed devices which can be deployed over enormous physical spaces. Coordination between sensor devices is required to achieve a common communication. In low cost, low power and short-range wireless environment, sensor networks cope with significant resource constraints. Security is one of main issues in wireless sensor networks because of potential adversaries. Several security protocols and models have been implemented for communication on computing devices but deployment these models and protocols into the sensor networks is not easy because of the resource constraints mentioned. Memory intensive encryption algorithms as well as high volume of packet transmission cannot be applied to sensor devices due to its low computational speed and memory. Deployment of sensor networks without security mechanism makes sensor nodes vulnerable to potential attacks. Therefore, attackers compromise the network to accept malicious sensor nodes as legitimate nodes. This paper provides the different security models as a metric, which can then be used to make pertinent security decisions for securing wireless sensor network communication.

Keywords: Sensor network, Authentication, Encryption, Security

1. Introduction

Recently, sensors are less expensive and smaller with the advanced technologies, making them widely and easily available for commercial use, and also extensively employed in many research fields. Sensors are often deployed in wireless sensor networks that involve enormous physical spaces, and communicate and coordinate with each other to provide multiple services. These sensors are normally deployed with the expectation that they will operate for long periods unattended. Consequently, the devices are designed with low bandwidth, low energy consumption and limited computational power, which means that conventional protocols and communication architectures cannot be implemented without some changes.

Fig. 1 shows the typical scheme of a sensor node. A standard sensor node consists of a microprocessor, ADC, sensors, radio, memory storage (usually very small given the size of the node), and a power source. Sensor nodes have evolved into two broad categories: small devices with 8-bit microcontrollers as CPUs, 10-100KB of working memory, and 100-1000KB of flash secondary storage; and larger devices with 32-bit CPUs and megabytes of both working memory and secondary storage [1].

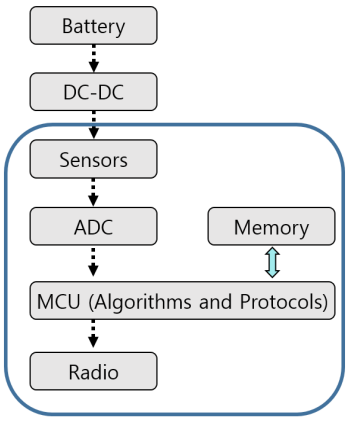

Fig. 1. The typical architecture of a sensor node

The sensors in a node are designed, based on the requirements of their application, to detect changes that occur in their electrical characteristics under certain environments or conditions, and then analyze those changes, prompting a change in whatever use the sensor nodes were required for. For example, a sensor node used to monitor temperature changes in an ecosystem would consist of materials that exhibit certain changes with changes in temperature, such as a thermistor. When this change in temperature reaches a set threshold, the sensor's microprocessor stores information related to it, or processes the information itself. A sensor node can also be used for wildlife tracking by attaching a node with an accelerometer, which senses movement patterns of the wildlife to be observed.

Because of their limited hardware, sensor nodes are

† Corresponding Author: Division of Electrical and Electronic Engineering and Interdisciplinary Graduate Program for BIT Medical Convergence, Kangwon National University, Korea. (hyuncho@kangwon.ac.kr)
* Dept. of Computer Information Technology, Korea National University of Transportation, Korea. (youn@ut.ac.kr)
Received: September 1, 2016; Accepted: February 24, 2017

prone to various attacks, like wormhole attack, Sybil attack, sinkhole attack, eavesdropping, etc. Also, various types of sensors need to monitor pressure, humidity, temperature, light condition, humidity, or the presence and absence of various objects [2].

2. Related Works

Subhash et al. proposed a software-based method to avoid byzantine wormhole attack, and was applicable to source routing protocols. Their proposed method does not require any specialized hardware. A digital signature is the key mechanism. Their mechanism blocks wormhole formation during the route discovery process [2].

Al-Mohidat et al. proposed an efficient modification mechanism of the IEEE 8902.11 MAC layer on multi-channel mode. The proposed method improves performance significantly compared to the literature, and to a single channel mode. Basically, the IEEE 802.11 MAC layer is designated for a single hop wireless network [3].

Wen et al. proposed an efficient wormhole detection algorithm. Based on this algorithm, a simple random walk route method was proposed. The proposed method avoids routes from wormholes chosen without using the low latency link created by the wormhole [4].

Benenson et al. showed some example of attack of sensor nodes. Sensor nodes get the information about the real world through their sensors, hence the ability to forge sensor data could be classified as a severe attack. For example, while the attacker passes unnoticed through the region under surveillance, the surveillance system might be fooled by thinking the situation is normal. If the sensors are integrated into the printed circuit board design, replacement of those sensors entails fabrication of the conductor wires, soldering new connections, and cutting those [5].

Barcena et al. tested a possible attack against wireless IoT devices. They use LightwaveRF and Belkin MeMo smart hubs though similar attacks are possible against other devices. Precondition is that the attacker cracked the Wi-Fi password and has access to the local network. The network traffic can be analyzed using a network sniffer like a Wireshark and the LightwaveRF smart hub generates certain network traffic each time it restarts and every 15 minutes to check for firmware updates. The LightwaveRF sends the traffic to a remote trivial file transfer protocol (TFTP) server, in which the connection is not encrypted or authenticated, so it could be an easy target of an attacker. Another attack example is on the Belkin WeMo connected switch, which does not require authentication procedure in order to connect. Hence, any attacker on the same network as the device can send any command to the connected switch. To protect this kind of attack, device's firmware should be encrypted and authenticated [6].

Stanislav et al. showed the result of a case study on baby monitor device. Known vulnerabilities are cleartext local API, cleartext cloud API, unencrypted storage, remote shell access, backdoor accounts, etc. In order to avoid local network traffic cleartext exposure, customers must inquire with the vendor about a firmware update. Also, to avoid authentication bypass and privilege escalation, customers must use the device only in a local network mode and use firewall rules to block the camera from the Internet [7].

3. Sensor Network Security Goals and Limitations

In this section, we look at the goals desired when designing the security architecture for a sensor network, and the challenges that sensor networks face in attempting to achieve these goals.

In terms of threats the security concerns of a sensor network are similar to those of a wired environment, such as a wired WAN or an Ethernet LAN. Nowadays, wireless sensor networks are used in many public and private areas like universities, hospitals, governments, the military, airports and home. The use of WLAN is exploding all around the world and is easy to use in any place. To protect the information in a wireless sensor network environment, security mechanisms should be enhanced. Network security protocols such as WEP, WPA, and WPA2 have been developed to secure the wireless network. In a wireless environment, radio signals can pass through walls, ceilings, and floors, hence data is being unintentionally transmitted to recipients on different floors or even outside the building. These situations allow attackers to intercept the information. Also, to protect the wireless networks, we have to understand that there are different kinds of security attacks at different layers [8].

3.1 Security goals

There are various security goals (Data Confidentiality, Data Integrity, Data Availability, Data Authentication, Data Freshness, Accountability, etc.) required by a sensor network, and an understanding of these goals provides the foundation for designing an appropriate security model. Data confidentiality is management of access to files in storage or in transit. Any message communication in a wireless sensor network should have guaranteed confidentially by blocking attacks from an attacker. Data integrity is ensuring reliability from malicious altering or accidental altering. Data authentication is ensuring that the data has originated from a reliable resource. Data authentication is a big challenge in a wireless sensor network environment because of the unattended nature of the wireless sensor network. Data availability involves making any of the network services available. Data availability can be challenged for several reasons, such as out of battery, denial of service attack, failure of base station, etc. Data freshness should be guaranteed by

making certain no old data is replayed. There is no central organizer for a wireless sensor network, so every sensor node has to have some self-organization capability. In addition, sometimes we have to turn off the nodes periodically for time synchronization [9].

It should be noted that some security issues are exacerbated in a wireless sensor network environment, and that some are only applicable to the wireless sensor network environment [8].

Confidentiality has to do with keeping information secret or concealed from unauthorized users. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized changes. An adversary has to modify the data packet as well as add additional packets to the original whole packet stream. Hence, the receiver should make sure that the data originated from the correct source. Cryptographic schemes play a role in achieving data authentication. Although it is imperative to check for confidentiality and integrity of data, freshness is also of great importance.

3.2 Security limitations/challenges in sensor networks

There are some challenges to attaining the above mentioned goals, most of which stem from the characteristics of sensor nodes. The challenges include limited memory and processing power, low bandwidth, time synchronization, physical tampering of nodes, power limitation, etc.

Wireless communication by its very nature creates interception, alteration and disruption. There are two ways to protect the confidentiality of wireless transmission. To reduce the risk of eavesdropping, we can make it more difficult to locate and intercept the wireless signal, and use encryption to maintain confidentiality even when the wireless signal is intercepted [8].

The alteration of intercepted communications might be avoided through strong encryption and authentication of both devices and users. Also, problem areas can be identified by periodic audits of wireless networking performance and activity. To deal with a problem area issue, we can remove the offending devices, or increase signal strength and coverage within the problem area. In this way, the risk of denial of service could be decreased.

4. Treat Model

For better understanding of the security problems faced by sensor networks, it is important to clarify what should be protected, what attacks might be performed, what security measures are in place and how well the sensor network is protected.

Perfect protection to a sensor network is not feasible because of the constraints on bandwidth, computational processing power and energy resources. Trial to defend against all kinds of attack is not good strategy because it is expensive and in itself can induce a denial of service attack, when the node is occupied with trying to defend against an attack and consequently cannot perform it basic essential jobs.

When we create a threat model, it is widely supposed that an attacker knows as much as there is to be known about the topology and protocols used in the sensor network. In the Dolev-Yao model, all data are represented symbolically as terms of an algebra and all operations on data, including cryptographic primitives, are represented as algebraic operators that are applied over terms in order to create new terms. Other operators could be used for other kinds of encryption, for pairing messages into structured messages, and for extracting public and private keys from key pairs or for building shared keys from their key material [9].

4.1 Threats/attacks on wireless sensor network

Threats/Attacks against a wireless sensor network can be conducted in different layers of the protocol stack. In here, WSN attacks are classified based on the protocol stack.

Attacks like clock skewing, clone attack and data aggregation distortion are done in the top-level application layer. A clone attack can be avoided with the use of unique pairwise keys. Usually, the types of attacks in the application layer are subversion or malicious nodes. Therefore, it is important to detect malicious node and isolation.

Attacks like SYN flooding and de-synchronization are conducted in the transport layer. SYN flooding attack can be blocked through the minimization of connection numbers and client puzzles.

A lot of attacks, like sinkhole, node capture, Sybil attack, hello flood, ping flood, selective forwarding, wormhole, spoofed or altered, replayed routing information, homing, internet smurf, misdirection, and acknowledge spoofing are performed in the network layer. Replayed routing information could be avoided by encryption techniques and strict authentication. Hello flood attacks can be avoided by 2-way authentication or 3-way handshaking. A wormhole attack can be blocked by a flexible route selection mechanism. Sinkhole attacks can be blocked by monitoring, redundancy scheme or authentication scheme. A selective forwarding attack can be dodged with a probing or redundancy scheme. Sybil attacks can be evaded by an authentication scheme. Fig. 2 shows a Sybil attack and Fig. 3 shows a wormhole attack.

Attacks like unfairness, collision, and exhaustion are performed in the data link layer. Error correcting code can make collision avoidable and rate limitation can make exhaustion avoidable.

Attacks like jamming and tampering are conducted in the physical layer. Jamming could be avoided by lowering

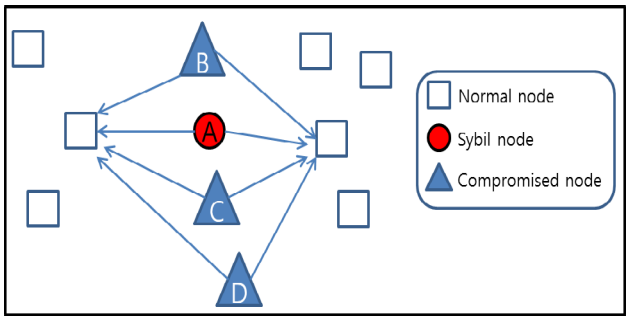

Fig. 2. Sybil Attack

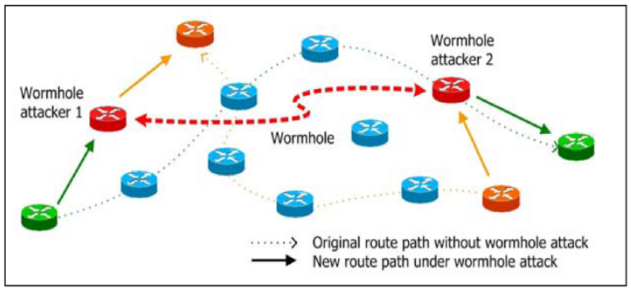

Fig. 3. Wormhole Attack

the duty cycle or with a spread-spectrum technique. A key management scheme can make tampering avoidable [10,13,14].

5. Security Model

There are multiple applications for the sensor network. They differentiate requirements for the hardware, software and communication protocols. Most of the suggested mechanisms generalize that sensor networks are all extremely resource constrained, but require the same level of security protection compared to the traditional network. Sensor network components have various characteristics, hence it might be important to determine whether nodes are predominantly stationary or mobile; deployed densely or sparsely. Also, certain tradeoffs exist when considering the security of the sensor network and the resource constraints of the components.

Taking this into consideration, we can now proceed to design the network security based on the following:

- The characteristics of the sensor networks, such as processing power, energy source, deployment, topology required, etc.
- The advantages/cost benefits of using certain security mechanisms.
- The complexity of the security mechanism to be implemented.

Having discussed a threat model which provides an understanding of how attacks can occur, it seems equitable

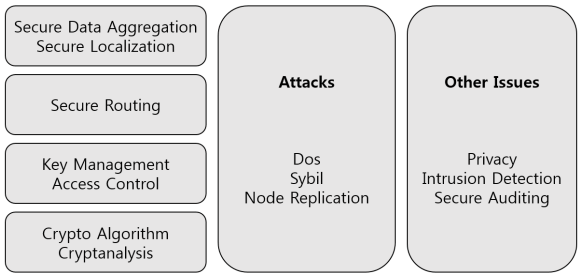

Fig. 4. Security Architecture for a WSN (Wireless Sensor Network)

that we look at mechanisms that protect sensor networks, with an analysis of the attacks defended by the aforesaid mechanism and the effects of these mechanisms on certain resource constraints on the sensor network. Fig. 4 shows the security scheme for a wireless sensor network.

5.1 Mechanisms for confidentiality

Confidentiality is the control the secrecy of information. It includes prevention of leakage as well as way of secret writing of information. Confidentiality mechanisms make use of cryptography to provide assurance that data is kept obscured from anyone not authorized to access the data. In wireless sensor network environment, public key encryption schemes are not feasible because of the limited processing power of sensor nodes and rapid depletion of the energy source of sensor nodes as compared to the other alternative, symmetric encryption schemes.

There is some tradeoff to be expected depending on what kind of key is used. With network keys, distribution of the keys is easy since it is just a single key, and less memory is required of the sensor nodes to store the key. There is also less computation when processing the key. Although convenient and less burdensome on the sensor node because of less memory use for key store and less computation for key processing, the security provided here is a very lax, compromised node can be vulnerable to attackers

Pair-wise keys are ideal to ensure node to node security. There is a tradeoff according to the number of sensor nodes in the network scale up and the amount of keys to be kept increase. When a node joins or leaves the network, a broadcast is sent to all nodes to notify them of this change in the key revocation/addition of the node, increasing the communication time of the nodes in the network, ergo, depleting its energy source.

Some approaches have been suggested which attempt to harness the power of pair-wise key sharing without the processing overhead associated with it. Eschenauer and Gligor [11] make use of probabilistic key sharing among nodes, where each node receives a certain amount of keys from a pool of available keys. Although a pair of nodes may not share a key, if a set of nodes is sharing keys pair-wise between the two nodes, then a path is set through

these nodes [15].

5.2 Mechanisms for integrity

Integrity guarantees that a transferred message will never corrupt. Integrity could be compromised by the malicious alteration of a bank account number or accidental alteration, like a transmission error [16].

Nodes in a sensor network need an assurance that the party they are communicating with is who they claim to be. The freshness of data is also an issue, as this is a check against replay attacks. Encryption keys are used to generate message authentication codes (MAC) which are included in each message sent between nodes, and vouches for the integrity of a node.

5.3 Mechanisms for availability

Most security mechanisms for sensor networks are primarily built to provide confidentiality and integrity, but availability is harder to guarantee, since it is tied to a lot of factors relating to hardware and software. While trying to enforce a high level of security, many computations are required and energy is spent in performing such computations, and the communications that occur between the nodes in the network. If the energy source is constant, in that it has no means of harvesting energy to recharge itself, it is likely that it will run itself out. With no energy source, the node is effectively useless. A denial of service attack could happen at any layer of the network. Authorized user actions should be assured for secure communication, which is the guarantee of reliable data delivery to a destination node, and protection of the message and data against a denial of service. Thus, we can make the network service available any time [16].

5.4 Mechanisms for key management

Key distribution and management is a major talking point in the security model design. Usually, public key cryptography and key pre-distribution mechanism is used in wireless networks.

It has been argued [17] that the initial deployment of keys used for providing security when communicating over a sensor network is not totally secure, as the initial deployments by some of the distribution approaches [11,18,19] do not have a specified secure key distribution mechanism.

5.4.1. Public key cryptography

Asymmetric cryptography, where a node is uniquely identified in the network by its public key, makes a broadcast, which is the communication from a node to multiple nodes, easy since the encryption/decryption keys used by each node are distinct, there is no effect on the other nodes in the network even if a node is compromised. An example of a public key crypto system is the Diffie-Hellman scheme [20]. However, asymmetric cryptography has some issue. The big issue with asymmetric cryptography is that while it is handled efficiently and with little burden by traditional computing systems, the computational power of sensor nodes are not adept at dealing with such intensive calculations. Fig. 5 shows the scheme of the public key cryptography.

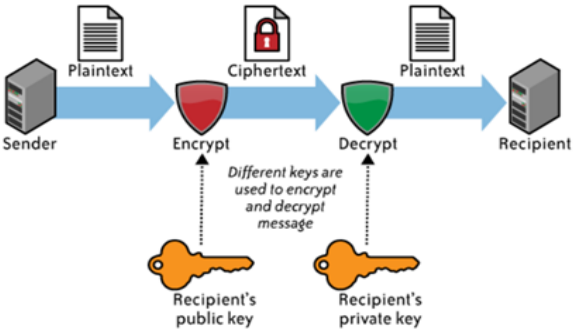

Fig. 5. Public Key Cryptography

5.4.2. Key pre-distribution approach

Key pre-distribution approach uses symmetric cryptography. This is a feasible under computationally less intensive environment Symmetric cryptography uses the same key for encryption and decryption. Because the key used in communication is to be shared between two parties, a means has to be developed that enables secure communication between the nodes in question and prevents inference of the data being exchanged by any other person, potentially an attacker eavesdropping. This can pose a problem, as it requires that a secure way of distribution of the shared key be developed. Eschenauer and Gligor [11] have approached this problem in different ways. Their approach relies on probabilistic key sharing among nodes, where nodes in the network select a certain amount of keys among the available keys, which they then use for subsequent communication. The latter enhancement is achieved by using random pair-wise keys, an adaptation of the standard pair-wise key sharing, based on the fact that not all n–1 keys (where n is the number of nodes in the network) need to be stored in the nodes key ring to have a connected random graph with high probability [15,18].

6. Conclusion

Sensor networks are a rapidly growing technology. Most network security threats are applicable to wireless sensor network. These threats are more complicated with the physical limitations. Security issues of wireless sensor network are still remaining open and many researchers are working on more research activities on topic. Wireless

sensor network can provide multiple services to their users if those security issues are handled efficiently.

While analyzing a threat model that is specific to the sensor network, the challenges that sensor networks face were discussed in the paper.

According to the increase of mobile devices, wireless sensor networks have become promising to many applications in the future. However, deployment of wireless sensor networks is vulnerable to various attacks without appropriate security mechanism. Many researches are going on a trusted environment so far, but we are experiencing may security attacks these days. Hence, we definitely need a strong security mechanism against attacks in wireless sensor networks. The purpose of this paper is to provide a general overview of sensor network security, and a further review of the relevant literature can be completed by interested researchers.

Acknowledgements

This study was supported by Korea National University of Transportation in 2016 and 2016 Research Grant from Kangwon National University.

References

[1] J. G. Heidemann, R, "An Overview of Embedded Sensor Networks," USC/Information Sciences Institute November 2004.

[2] P. Subhash and S. Ramachandram, "Preventing Wormholes in Multihop Wireless Mesh Networks," IEEE third International Conference on Advanced Computing & Communication Technologies, 2013.

[3] M. N. Al-Mohidat and F. M. Salem, "IEEE 802.11 Based Wireless Mesh Networks: A Multi-Channel MAC Baseline Study," CISS, pp. 1-6, 2013.

[4] H. Wen and G. Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbour in Wireless Mesh Networks," *Journal of Information & Computational Science*, vol. 10,14, pp. 4461-4476, 2013.

[5] Z. Benenson, P. M. Cholewinski, and F. C. Freiling, "Vulnerabilities and Attacks in Wireless Sensor Networks," in Wireless Sensor Networks Security, ser. Cryptology & Information Security Series (CIS), J. Lopez and J. Zhou, Eds. Philadelphia, PA, USA: IOS Press, 2008.

[6] Insecurity in the Internet of Things "https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf," 2015.

[7] M. Stanislav, T. Beardsley: HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, Rapid7 Report, 2015.

[8] R. Rathika and D. Sowmydevi, "Wireless Sensor Network Security: Vulnerabilities, Threats and Countermeasures," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 6, no. 1, January 2016.

[9] D. Dolev and A. Yao. "On the Security of public-key protocols," *IEEE Transactions on Information Theory,* 29:198-208, 1983.

[10] M. Abdus Salam and N. Halemani, "Performance Evaluation of Wireless Sensor Network under Hello Flood Attack," *International Journal of Computer networks & Communications(IJCNC)*, vol. 8, no. 2, March 2016.

[11] L. Eschenauer and V. D. Gligor, "A key-management Scheme for Distributed Sensor Networks," Presented at the Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, DC, USA, 2002.

[12] A. Pironti, D. Pozza, and R. Sisto, "Formally based Semi-automatic Implementation of an Open Security Protocol," *Journal of Systems and Software,* vol. 85, pp. 835-849, 2012.

[13] S. Raja Rajeswari and V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," *The Scientific Wrold Journal*, vol. 2016.

[14] I. Gawdan, C. Chow, H. Ishii, and T. Zia, "Threat Models and Security Issues in Wireless Sensor Networks," *International Journal of Computer Theory and Engineering.* IACSIT Press. vol. 5, no. 5. DOI: 10.7763/IJCTE2013.V5.806. ISSN: 1793-8201, 2013

[15] M. A. IshwaryaMathi Manickavasagam, Sivasankar Sundaram, "Secure Key Pre-distribution in Wireless Sensor Networks using Combinatorial Design and Traversal Design based Key Distribution," *International Journal of Research in Engineering and Technology,* vol. 03, Apr-2014 2014.

[16] R. Regan and J. Martin Leo Manickam, "A Survey on Wireless Networks and its Security Issues," *International Journal of Security and its Applications*, vol. 10, no. 3, pp. 405-418, 2016

[17] C. Kuo, M. Luk, R. Negi, and A. Perrig, "Message-in-a-bottle: User-friendly and Secure Key Deployment for Sensor Nodes," Presented at the Proceedings of the 5th International Conference on Embedded Networked Sensor Systems, Sydney, Australia, 2007.

[18] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Presented at the Proceedings of the 2003 IEEE Symposium on Security and Privacy, 2003.

[19] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," *Wirel. Netw.,* vol. 8, pp. 521-534, 2002.

[20] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theor.,* vol. 22, pp. 644-654, 2006.

Seongwook Youn He received the B.S. degree in Computer Science from Sogang University, Seoul, Korea in 1997, and M.S. and Ph.D. degrees in Computer Science from University of Southern California, Los Angeles, CA in 2002 and 2009, respectively. Dr. Youn's current interests are Market Data Forecast, Data Science, Personal Information Management, etc. He is currently an Assistant Professor at Department of Computer Information Technology, Korea National University of Transportation, South Korea.

Hyun-chong Cho He received the M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Florida, USA in 2009. During 2010-2011, he was a Research Fellow at the University of Michigan at Ann Arbor, USA. From 2012 to 2013, he was a Chief Research Engineer in LG Electronics, South Korea. He is currently an Assistant Professor at Kangwon National University, South Korea.