A Grid-based Approach to Location-Dependent Key Management in Wireless Sensor Networks

Jaewoo Choi[1], Jihyun Bang[1], Mirim Ahn[2], Leehyung Kim[2], and Taekyoung Kwon[1*]
[1]Yonsei University, Seoul, Korea
{jw.choi, mogiela, taekyoung}@yonsei.ac.kr
[2]Agency for Defense Development, Seoul, Korea
mirimahn@hanmail.net, lhkim@add.re.kr

Abstract

To achieve secure communications in wireless sensor networks, sensor nodes should be able to establish secret shared keys with neighboring parties. The location information of sensor nodes can be used to generate a shared key. In this paper, we propose yet another location-based key management scheme for wireless sensor networks. After reviewing the existing location-based key management schemes, we focus on the scheme called LDK because of its pros and cons. To solve a communication interference problem in LDK and its similar methods, we devise the new key revision process that incorporates the grid-based location information. We also propose the key establishment process using the grid information. For analysis, we conducted a simulation and confirmed that our method can increase the connectivity while decrease the compromise ratio when the minimum number of common keys required for key establishment is high. Finally, we also found that hexagonal deployment of anchor nodes can save network costs in our method.

Keywords: WSN, Key management, Insider Threats, Location-based

1 Introduction

According to what Gatner said in 2014, IoT (Internet of Things) will connect 26 billion devices by 2020 and Gartner highly evaluates economic value of IoT[9]. Wireless Sensor Networks (WSN) is the foundation technique of IoT and because of this reason, its technical research is progressed actively. Particularly, the researches applied to various environments such as military, medicine, industry, traffic, and so on go along continuously[17]. Moreover, security is an important area in the study of wireless sensor networks because it uses the actual data. Insider threat is also a critical security issue in wireless sensor networks because general security techniques such as authentication and autorization cannot detect inside attackers. This is a serious threat for many applications such as military surveillance system that monitors the battlefield and other critical infrastructures. Hence, we progress key management technique which is considered as insider threats in a field of security on wireless sensor networks.

Key management technique is started by L. Eschenauer et al.[7] and so many researches have lately been a very active area of research in sensor networks. It is divided into two parts: symmetric-key based and public-key based. Moreover, there are other various methods of key management, such as pairwise key, pre-distributed random key, location-based key, and so on. Because of hardware restrictions of a sensor node, the main objectives of key management for wireless sensor networks are efficiency, scalability, heterogeneity.

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 1 (January 15, 2015)

*Corresponding author: 207, New Millenium Hall, 50 Yonsei-ro, Seodaemun-gu, Seoul, Tel: +82-(0)2-2123-4523, Web: `http://islab.yonsei.ac.kr`

In wireless sensor networks, location information is important to generate shared keys and is highly applicable. Thus, location-based key management is one core part of the key management researches in wireless sensor networks. Grid-based key management in location-based key management has a feature that a sensor node should be located in an assigned grid. This feature can be a weak point according to applied environments. For instance, when sensor networks is used for an enemy detection in a military zone, it is difficult to locate sensor nodes in an assigned grid. Anjum[2] proposed a scheme that is only dependent on a location of sensor nodes without any deployment knowledge. This paper is based on the scheme which is dependent on a location of sensor nodes.

The rest of the paper is structured as follow: We look at related works in section 2 about location-based key management for wireless sensor networks. We describe our scheme based on Location Dependent Key Management (LDK) in section 3. Simulation and discussion are described in section 4 and finally, we present our conclusion in section 5.

2 Related Work

The most of location-based key management for wireless sensor networks uses grid information. The grid information uses the coordinate after an area is divided into grids. Precondition that a sensor node is deployed in an assigned grid is essential. This condition can be a constraint according to deployed areas.

Huang et al.[10] proposed a grid-group scheme which uses known deployment information. Instead of randomly distributing keys from a large key pool to each sensor, secret keys to each sensor are systematically distributed from a structured key pool. It uses an identifier by combining grid information and an id of a sensor node. This scheme pre-distributes both an identifier and Blom's scheme to the sensor nodes. Ito et al.[11] proposed a scheme that keys are mapped to two-dimensional positions, and positions estimated using a node probability density function decide the keys that are distributed to a node. A sensor node randomly requests an assigned key to other sensor nodes within transmit range. Du et al.[6] proposed a scheme which assigns a sub key set extracted to a key pool in a grid. This scheme uses nonuniform probability density functions which suggest that a sensor is likely to be deployed in certain areas. Liu et al.[14] utilized a grid coordinate of a sensor node when generating a pairwise key by using bivariate key polynomial.

Anjum[1, 2] proposed a scheme called LDK that generates a key by combining a pre-distributed key ring with nonces in 2006. After that, Anjum extended the scheme in 2010. In contrast with the schemes which are dependent on a position of grids, LDK is dependent on a position of sensor nodes. By using a feature of an anchor node (AN) that transmits data within a certain distance by adjusting a power level, an area is divided. A sensor node is distributed in an area after storing a single common key k and hash function H. ANs transmit each nonce at a different power level and a sensor node generates single keys as follows : $k_j^i = H_k(n_j^i)$. When a sensor node finds common keys whose number is larger than a certain number of keys with a neighbor node, a communication key is derived as $k = H(k_1, k_2, \cdots, k_q)$. Faghani et al.[8] proposed SLDK (Sectorized Location Dependent Key Management) in 2009. It reinforces the key resiliency of LDK by adding a scheme that divides the transmit range of an AN into n sectors.

In this paper, we propose a scheme that solves some problems which can be occurred in LDK[2] and we also consider that the minimum number of common keys required for key establishment is high.

3 Proposed Scheme

3.1 Threat Model

In this paper, we apply a key management technique for a secure communication against various outside attacks. We also consider inside attacks. An inside attack is more critical than an outside attack because it avoids authentication and authorization and drops critical packets. Various types of inside attacks are modification, misrouting, eavesdropping, and packet drop. Particularly, packet drop attack is more difficult to be detected than the other inside attacks. Packet drop attack can also decrease a network performance. Packet drop attack consists of Blackhole attack, Grayhole attack, and On-off attack. Because of the features of Grayhole attack and On-off attack, they are more difficult to be detected than Blackhole attack. In this paper, one of the objectives is to provide security against packet drop attack among inside attacks[4].

3.2 Notation

Table 1 lists the symbols and the meaning of each used in this paper.

AN	An anchor node that transmits nonces
AN_{set}	A set of anchor nodes
SN	A normal sensor node
SN_{set}	A set of sensor nodes
k_c	A pre-distributed network key
G	Pre-distributed nine-grid information
H	A pre-distributed hash function
C_n	The total number of nonces
N_r	A nonce which is transmitted
C_{common}	The number of shared keys with neighbor nodes
q	The minimum number of keys for making a communication key
K_t	A key which is generated using a nonce and a grid
K_q	Shared keys in excess of the number of q
K_s	A communication key between the two nodes

Table 1: Notation

3.3 Problem of LDK

Previous LDK does not consider a communication interference. Wu et al.[16] said that Packet Reception Ratio (PRR) decreases by 40% in MicaZ motes. The packet loss affects on the number of nonces transmitted from an AN. This correlates with the connectivity. Also, we consider the environment that the minimum number of common keys is very low. Because this parameter can increase the security level, we take account of the environment that the minimum number of common keys is high.

3.4 Proposed Scheme (LDK+)

Figure 1 shows the illustration of LDK+. We add key revision phase from a neighbor node and provide key establishment process by using grid information. Similar to the LDK, each sensor node saves a network key, a hash function, and the additional grid information which is pre-distributed by a base station. The total number of grid information is nine and it consists of coordinates of the arranged grid and eight neighbor grids. We also consider that the sensor node does not deploy in the assigned grid position[13]. Key generation between sensor nodes consists of four phases: Pre-distribution phase, Initialization phase, Key establishment phase, and Key agreement phase. In the next section, we describe the details of each phase.

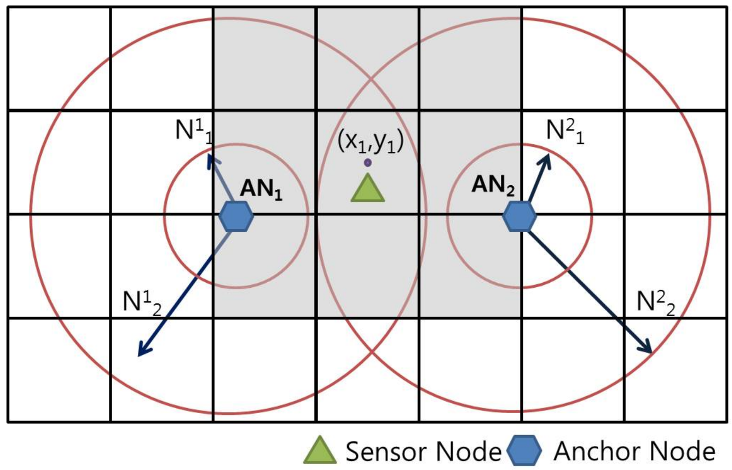


Figure 1: Illustration of LDK+

3.4.1 Pre-distribution Phase

In pre-distribution phase, sensor nodes save the information that is needed to manage key before a deployment. The factors saved in sensor nodes are described as follows: a network key K_c for a secure communication before establishing a communication key K_s, a hash function H that is used to generate a key, and nine-grid information G. The followed Eq. (1) shows the algorithm in pre-distribution phase.

$$\begin{aligned} AN_{set} &= AN_1, AN_2, \cdots, AN_n \\ SN_{set} &= SN_1, SN_2, \cdots, SN_n \\ SN_{set} &\leftarrow K_c, G, H \end{aligned} \tag{1}$$

Blackhole attacks can be divided into three sequential stages. First, the attacker captures a sensor node and extracts critical information. Second, he redeploys a compromised node to wireless sensor networks. Third, he launches Blackhole attacks. Hence, before the key is established, we consider the node capture as a countermeasure of Blackhole attacks. Each sensor node generates its neighbor table using a hello message, similar to the work presented in [5]. The followed Eq. (2) shows the algorithm of creating a neighbor table.

$$
\begin{aligned}
& SN_o \rightarrow *SN_l : hello\ message \\
& \quad IF\ SN_l \rightarrow SN_o : ACK \\
& \qquad SN_o : add\ SN_l\ in\ neighbor\ set \\
& ELSE \\
& \qquad IF counter\ threshold \geq hello\ count\ of\ SN_o \\
& \qquad\quad delete\ SN_l\ in\ neighbor\ set \\
& \qquad ELSE \\
& \qquad\quad SN_o \rightarrow SN_l : hello\ message \\
& \qquad\quad hello\ count\ of\ SN_o = hello\ count\ of\ SN_o + 1
\end{aligned}
\tag{2}
$$

3.4.2 Initialization Phase

The initialization phase is a process that a sensor node is transmitted from ANs. In this phase, the nonce revision is progressed. The AN transmits encrypted nonces to sensor nodes at different power levels. Then the sensor node transmits encrypted coordinate of the assigned grid to the neighbor nodes. The neighbor node which has the same coordinate of the assigned grid transmits the number of nonces to the sensor node. If the number of nonces transmitted by the other neighbor node is greater than its number of nonces, the sensor node requests the nonces from the other neighbor node to revise its nonces. The followed Eq. (3) shows the algorithm in initialization phase.

$$
\begin{aligned}
& AN_{set} \rightarrow SN_{Set} : E_{k_c}(N_{uv})\ \ (1 \leq u \leq n, 1 \leq v \leq powerlevel) \\
& \quad SN_o \rightarrow SN_l : E_{k_c}(G(x,y)) \\
& \quad SN_l \rightarrow SN_o : E_{k_c}(C_n) \\
& \quad IF(\ C_n\ of\ SN_o < C_n\ of\ SN_l) \\
& \qquad SN_o \rightarrow SN_l : request\ nonces \\
& \qquad SN_l \rightarrow SN_o : ACK(E_{k_c}(N_r)) \\
& \qquad (1 \leq r \leq C_n\ of\ SN_l)
\end{aligned}
\tag{3}
$$

3.4.3 Key Establishment Phase

In key establishment phase, a sensor node generates a key by combining nonces and nine-grid information. Thus, each sensor node can generate keys which are nine times larger than the number of nonces. After that, the sensor node deletes the nonces. The followed Eq. (4) shows the algorithm in key establishment phase.

$$
SN_{set} : K_t = H_{k_c}(N_r || G(x,y)) \tag{4}
$$

3.4.4 Key Agreement Phase

In key agreement phase, the sensor node generates a communication key with a neighbor node. The sensor node encrypts all the keys which are generated by itself and attaches MAC. The MAC value assures the integrity. The neighbor node checks whether or not it has the same keys among transmitted keys. If the number of the same keys is greater than a certain number, the sensor node generates the communication key by implementing XOR operation with the same keys. The followed Eq. (5) shows the algorithm in key agreement phase.

$$
\begin{aligned}
& SN_o \rightarrow * : E_{k_c}(k_1||k_2||\cdots||k_t)|MAC \\
& \quad IF\ Num\ of\ common\ key > q \\
& \qquad SN_l \rightarrow SN_o : E_{k_c}(k_q)||MAC \\
& \qquad SN_o, SN_l : K_s = K_q \oplus \cdots \\
& ELSE \\
& \qquad SN_l \rightarrow SN_o : none\, msg
\end{aligned}
\tag{5}
$$

3.4.5 Rekeying and Revocation

After all the sensor nodes finish all phases related to the secure communication, it can be occurred to add a new sensor node or discharge a battery of the sensor node or get damaged by malicious attacks. Particularly considering inside attacks, detecting by neighbor nodes is needed to counteract packet drop attacks. Rekeying and revocation are also demanded for the damaged nodes. For this, each node periodically transmits a status check packet to the neighbor nodes. If the sensor node does not respond to the status check packet, the neighbor nodes remove a related routing path and revoke a communication key. The neighbor nodes also send a request to base station for rekeying. The base station transmits a rekeying message to all the ANs and ANs transmit new nonces to sensor nodes. After that, a new communication key is generated by sequentially implementing the Eq. (3) - (5). If a sensor node gets damaged by Blackhole attack, it is excluded from rekeying because all the packets are blocked.

3.5 Hexagonal Deployment

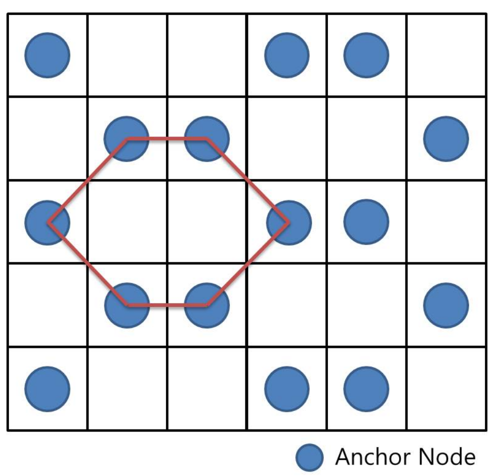


Figure 2: Hexagonal Deployment

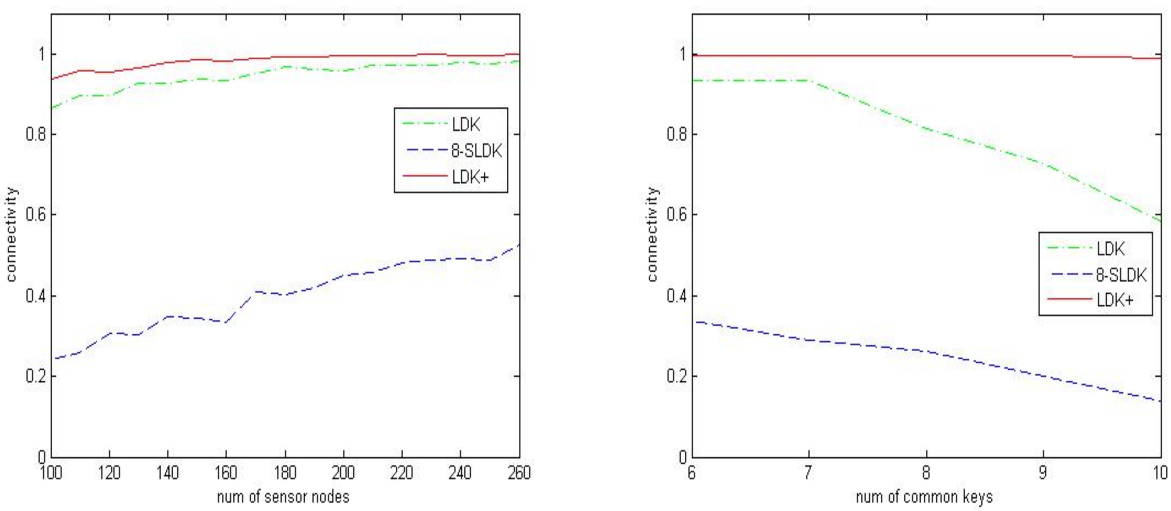
The research of hexagonal grouping form has been conducted continuously[12, 15]. In this paper, a hexagonal deployment of ANs is researched for reducing network costs. Figure 2 shows the hexagonal deployment in network. When ANs are deployed as a form of hexagons in 20 x 20 grids, 200 ANs can be deployed. In comparison to deploying an AN per a grid, the number of ANs can be reduced by 1/2. If the hexagonal deployment provides good connectivity and suitable security without any additional process, the network costs can be saved. We describe the applicability of the hexagonal deployment in the next section.

4 Analysis

In this section, we compare the proposed scheme to the existing schemes and simulate connectivity and compromise ratio using MATLAB.

4.1 Connectivity

We firstly divide the installed area into 20 x 20 grids, put an AN per a grid to assume an environment with 400 ANs, and measure the connectivity of LDK, 8-SLDK[8], and LDK+ respectively. The numerical value is the average of 10 simulation results in the same environment. When C_{common} is low, three schemes have the similar connectivity. In the assumed environment, we divide the power level of AN into 2 parts and set the transmit range of AN as 1 unit and the transmit range of SN as 2 unit. C_{common} is configured as 6. Figure 3(a) shows the simulation results of the connectivity of each scheme. The connectivity of LDK+ is higher than that of LDK and both the connectivity increase as the number of SN increases. Figure 3(b) shows the connectivity of each scheme according to C_{common}. We think of the environment where 150 SNs whose transmit range is 3 unit are deployed randomly. In this case, as C_{common} increases, the connectivity of LDK+ stays as it is, whereas the connectivity of LDK decreases. Generally, it turns out that the connectivity of 8-SLDK which is divided into 8 sectors is low.

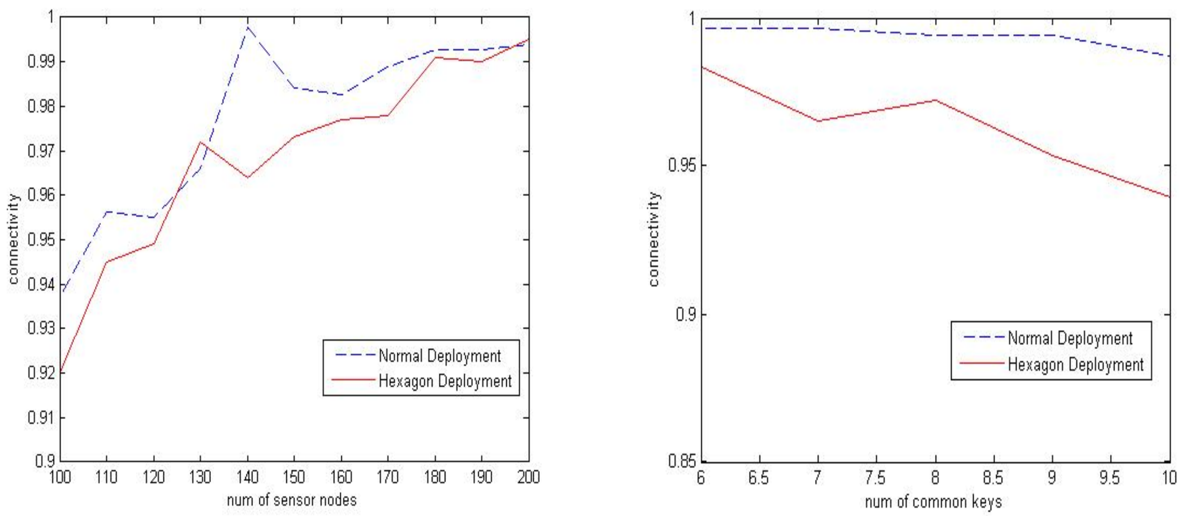


(a) Num of SN (b) Num of C_{common}

Figure 3: Comparing the connectivity of LDK+ with the others

Aside from this, we simulate several conditions in various environments. We assume that 100 SNs are deployed and C_{common} is 1. Then the connectivity of LDK+ is 0.937, when the transmit range of SN is 2 unit. The connectivity of LDK+ is 1 when the transmit range of SN is 3 unit. Eventually, if there are neighbor nodes within the transmit range of each SN, all the SNs can communicate each other. If SNs spread out ideally, the connectivity of SNs will be 1.

The connectivity can be changed according to the number of nonces it gets from an AN and C_{common} that affects on security. In the assumed environment, each SN receives 14 nonces from ANs on average. In this condition, the connectivity decreases as C_{common} increases. The connectivity of LDK drops rapidly when C_{common} is 6 and the connectivity of LDK+ drops rapidly when C_{common} is 19. Therefore, it is considered that the highest security is obtained when C_{common} is 18 in LDK+.



(a) Num of SN (b) Num of C_{common}

Figure 4: Comparing the connectivity of hexagonal deployment with normal deployment

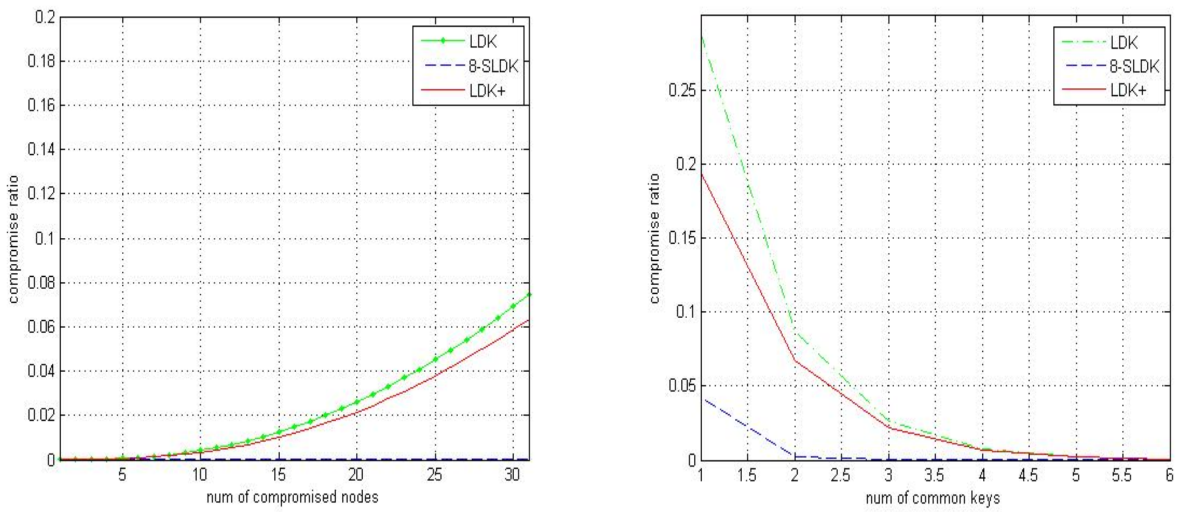
The number of AN relates to sensor network costs. If connectivity can be maintained as the number of AN reduces, network generating costs can be saved. To reduce the number of AN, we apply a hexagonal deployment. When deploying in a hexagonal shape, we can form network only with 200 ANs whereas 400 ANs are needed before. When we set transmit range as 1.6 unit and remain the other conditions same, the connectivity of 100 SNs is almost as same as the previous value. Figure 4 shows a result of the simulation which compares the connectivity according to deployments. Therefore, we see from the simulation that the connectivity can be maintained similarly, while the number of ANs reduces when nodes are in a hexagonal shape.

4.2 Compromise Ratio

For simulation of compromise ratio, we refer to Eq. (6) in Chan et al.[3]. The size of key pool is S. The number of captured nodes is x. The size of key ring is m. The minimum number of shared key is q.

$$\sum_{i=q}^{m}(1-(1-\frac{m}{|S|})^{x})^{i}\frac{p(i)}{p} \tag{6}$$

Figure 5 shows a result of the simulation. The size of m is configured as 7 in LDK and 8-SLDK. The maximum m of LDK+ is set as 63. This is because LDK+ generates keys by combining nonces and 9 grid information. When C_{common} is 6, the total compromise ratio is lower than 0.08 according to the number of captured nodes. The compromise ratio of LDK+ is lower than that of LDK, but higher



(a) Num of compromised node

(b) Num of C_{common}

Figure 5: Comparing the compromise ratio of LDK+ with the others

than that of 8-SLDK. However, LDK+ is much more feasible than 8-SLDK. This is because LDK+ has a higher connectivity than 8-SLDK when C_{common} is 6. The compromise ratio totally increases as the number of common keys increases. This result implies that an increase in the number of common keys improves security.

In conclusion, the connectivity of LDK+ is high when the minimum number of common keys required for key establishment is high. The compromise ratio of LDK+ is lower than that of LDK, but higher than that of 8-SLDK. We also confirm that the absolute value of compromise ratio is low.

4.3 Comparison

The existing key management schemes using a grid for wireless sensor networks[10, 11, 14, 6] utilize a grid as key ring or an identifier which uniquely identifies a sensor node. One of the conditions among the schemes is that a sensor node should be deployed in an assigned grid. On the other hand, there is no deployment condition in Anjum scheme[2]. However, LDK is simulated to generate a communication key in low C_{common} environment. C_{common} is an important variable in network security. C_{common} for generating the communication key relates to the security in wireless sensor networks. When a node is captured, secure link is likely to be broken as C_{common} is low because the communication key is derived from a few common keys. Thus, we only consider the condition when C_{common} is high.

5 Conclusion

In this paper, we present LDK+ which is an improved scheme of LDK by Anjum[2]. We add key revision by utilizing grid information to the previous dividing method, and suggest key generation by combining grid information. Thus, we solve the lack of the number of nonces that can be occurred when communication interference happens. We also consider key establishment and key revocation considering packet drop attack among insider attacks.

Through the simulation, we confirm LDK+ has a higher connectivity and lower compromise ratio than those of LDK, which means stability and security are improved. Moreover, through the hexagonal deployment of AN arrangement, we show that network costs can be lowered with the similar connectivity by decreasing the number of AN.

Acknowledgments

This research was supported by the project named "A Research on Dynamic Networking and Security for Wireless Sensor Networks and Mobile Networks" supervised by the ADD(Agency for Defense Development), Korea, and the MSIP(Ministry of Science, ICT&Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1010) supervised by the NIPA(National IT Industry Promotion Agency)

References

[1] F. Anjum. Location dependent key management using random key-predistribution in sensor networks. In *Proc. of the 5th ACM Workshop on Wireless Security (WiSe'06), Los Angeles, CA, USA*, pages 21–30. ACM, September 2006.

[2] F. Anjum. Location dependent key management in sensor networks without using deployment knowledge. *Wireless Networks*, 16(6):1587–1600, August 2010.

[3] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. of the 2003 Symposium on Security and Privacy (S&P'03), Oakland, CA, USA*, pages 197–213. IEEE, May 2003.

[4] Y. Cho, G. Qu, and Y. Wu. Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks. In *Proc. of the 2012 IEEE Symposium on Security and Privacy Workshops (SPW'12), San Francisco, CA, USA*, pages 134–141. IEEE, May 2012.

[5] W. Ding, Y. Yu, and S. Yenduri. Distributed first stage detection for node capture. In *Proc. of the 2010 IEEE GLOBECOM Workshops (GC Wkshps'10), Miami, Florida, USA*, pages 1566–1570. IEEE, December 2010.

[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A key predistribution scheme for sensor networks using deployment knowledge. *IEEE Transactions on Dependable and Secure Computing*, 3(1):62–77, February 2006.

[7] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of the 9th ACM conference on Computer and communications security, Washington, DC, USA*, pages 41–47. ACM, November 2002.

[8] M. R. Faghani and S. A. Motahari. Sectorized location dependent key management. In *Proc. of the 5th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WMNC'09), Marrakech, Morocco*, pages 388–393. IEEE, October 2009.

[9] Gartner. The internet of things will transform the data center. `http://www.gartner.com/newsroom/id/2684915`.

[10] D. Huang, M. Mehta, D. Medhi, and L. Harn. Location-aware key management scheme for wireless sensor networks. In *Proc. of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN'04), Washington, DC, USA*, pages 29–42. ACM, October 2004.

[11] T. Ito, H. Ohta, N. Matsuda, and T. Yoneda. A key pre-distribution scheme for secure sensor networks using probability density function of node deployment. In *Proc. of the 3rd ACM workshop on Security of Ad hoc and Sensor Networks (SASN'05), Alexandria, VA, USA*, pages 69–75. ACM, November 2005.

[12] K. Kumar, A. Verma, and R. Patel. A location dependent connectivity guarantee key management scheme for heterogeneous wireless sensor networks. *Journal of Advances in Information Technology*, 1(3):105–115, August 2010.

[13] T. Kwon, J. Lee, and J. Song. Location-based pairwise key predistribution for wireless sensor networks. *IEEE Transactions on Wireless Communications*, 8(11):5436–5442, November 2009.

[14] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1):41–77, February 2005.

[15] X. Ma, Z. Dong, and J. Li. A novel key management scheme for wireless sensor networks. In *Proc. of the 6th Internet Computing for Science and Engineering (ICICSE'12), Zhengzhou, Henan, China*, pages 198–203. IEEE, April 2012.

[16] Y. Wu, J. A. Stankovic, T. He, and S. Lin. Realistic and efficient multi-channel communications in wireless sensor networks. In *Proc. of the 27th IEEE Conference on Computer Communications (INFOCOM'08), Phoenix, AZ, USA*, pages 1867–1875. IEEE, April 2008.

[17] L. Xu, W. He, and S. Li. Internet of things in industries: A survey. January 2014.

Author Biography

Jaewoo Choi received his B.S. degree in game engineering from Korea Polytechnic University, Siheung-si, Korea, in 2014. He is currently pursuing a M.S. degree at the Graduate School of Information, Yonsei University, Seoul, Korea. He current research interests include computer network security and information security and privacy.

Jihyun Bang received her B.S. degree in mathematics and professional English from Ewha Womans University, Seoul, Korea, in 2014. She is currently pursuing a M.S. degree at the Graduate School of Information, Yonsei University, Seoul, Korea. Her current research interests include cryptographic protocol, computer network security, and smart card security.

Mirim Ahn received her B.S., M.S. degrees in computer science from George Mason University, Fairfax, VA, USA, Korea University, Seoul, Korea, in 1985, 1994, respectively. She is currently a principal researcher at Agency for Defense Development, Seoul, Korea. She has involved in projects for developing military conscription and mobilization system, military satellite system, surveillance and reconnaissance sensor network, etc. as a participating researcher and a project manager since 1986. Her current research interests include information security and privacy, network protocol, computer network, and cyber warfare simulation.

LeeHyung Kim received his B.S., M.S. degrees in computer engineering from Kwangwoon University, Seoul, Korea, in 1994, 1996, respectively. He is currently a Senior researcher at Agency for Defense Development, Seoul, Korea. He has involved in project for developing surveillance and reconnaissance sensor network. as a participating researcher. His current research interests include sensor signal processing, mission planning system, power optimization, network protocol and cyber warfare simulation.

Taekyoung Kwon Taekyoung Kwon received his B.S., M.S., and Ph.D. degrees in computer science from Yonsei University, Seoul, Korea, in 1992, 1995, and 1999, respectively. He is currently an Associate Professor of information at Yonsei University, Seoul, Korea. From 1999 to 2000, he was a Post-Doctoral Research Fellow at the University of California, Berkeley, CA, USA, and developed a cryptographic protocol, which was later standardized by IEEE P1363.2 and ISO/IEC JTC1 SC27 11770-4, respectively. From 2001 to 2013, he was a professor of computer engineering at Sejong University, Seoul, Korea. From 2007 to 2008, he was on sabbatical at the University of Maryland, College Park. In 2013, he returned to Yonsei University, Seoul, Korea. His current research interests include information security and privacy, applied cryptography, cryptographic protocol, network protocol, usable security, and human-computer interactions.