Robustness Analysis for Sensor Networks against a Node-Destruction Attack

Shinsaku Kiyomoto[†], **Kazuhide Fukushima**[†] **and Yutaka Miyake**[†],

KDDI R & D Laboratories Inc 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan

Summary
In this paper, we present a model for analyzing the robustness of sensor networks against a node-destruction attack. We use a 3-dimensional periodic model for a sensor network and propose an index to analyze an impact of the attack. Then, we discuss attack impacts on the sensor network when some defining parameters are changed. From simulation results, we consider optimal parameters to maximize the robustness and the cover area of the sensor network.

Key words:
Sonsor Network, Robustness, Security, Node-Destruction, Master Node

1. Introduction

Sensor networks have been deployed for a wide variety of applications[1] such as environment sensing. A sensor network is an ad-hoc network consisting of many sensor nodes. Each sensor node is battery powered and equipped with integrated sensors, data processing capabilities, and short-range radio communications. Communicated data should be protected against eavesdropping and alteration by an adversary. Thus, secure communication channels established by cryptographic primitives are a mandatory requirement for sensor networks. Due to the resource-constrained nature of sensor nodes, symmetric key cryptosystems are preferred over public key cryptosystems. Thus, key distribution and key management for the symmetric key cryptosystem are primary issues for wireless sensor networks. Previous studies focused mainly on the design of an efficient key predistribution scheme for wireless sensor networks.

Another important security issue for wireless sensor networks is robustness against node-destruction attacks. Sensor networks face the serious threat that an adversary can efficiently obstruct data transactions and break some sensor nodes. In this paper, we present a model for analyzing the robustness of sensor networks against a node-destruction attack. We use a 3-dimensional periodic model of a sensor network and propose an index to analyze an impact of the attack. Then, we discuss attack impacts on the sensor network when certain defining parameters are changed.

The rest of the paper is organized as follows; section 2 introduces related work, and section 3 explains a sensor network that we will use for our analysis. We present a model for the analysis and new index estimating attack impact in section 4. Analysis results are presented in section 5 and we conclude this paper in section 6.

2. Related Work

There are several challenges to wireless sensor network security[2], and the main focus of existing research is on scalable trust management based on lightweight key management and distribution schemes appropriate for large-scale sensor networks. Perrig *et al.* presented a suite of security blocks optimized for sensor networks[19]. Kong *et al.* proposed a localized public-key infrastructure mechanism based on a secret sharing scheme[14]. Ito *et al.* proposed a strongly resilient polynomial-based random key pre-distribution scheme (RPoK)[13] for wireless sensor networks such that a private sub-key is not directly stored in each sensor node. Ruj *et al.* addressed pair-wise and triple-key establishment problems in wireless sensor networks[20], and they presented a novel concept of triple-key distribution in which a common secret key is established among three nodes.

The main difficulty in designing a lightweight key management and distribution system is how to pre-distribute initial keys to sensor nodes. Thus, existing studies usually focus on efficient key pre-distribution methods for wireless sensor networks. Gligor first proposed a random key pre-distribution scheme[10] in which each sensor node receives a random subset of keys from a large key pool before deployment. Several extensions of this scheme have been proposed [4][9][15]. Du *et al.* modeled node deployment knowledge in a wireless sensor network, and developed a key pre-distribution scheme based on this model[8]. They showed that key pre-distribution with deployment knowledge can substantially improve a network's connectivity(in terms of

Manuscript received June 5, 2012
Manuscript revised June 20, 2012

secure links) and resilience against node capture, as well as reducing the amount of memory required. However, they suggested that it was very difficult[12] to obtain exact deployment knowledge about nodes in advance, especially in large scale sensor networks. Liu *et al*. proposed a practical deployment model[16], in which sensor nodes were deployed in groups, and the nodes in each group were close to each other after deployment. He *et al*. presented an energy-efficient location-dependent key management scheme (ELKM)[12] based on local time synchronization[21] to improve the performance of location-dependent key management LDK[3]. Their scheme assumed that two types of nodes, master nodes and regular (sensor) nodes, existed on the wireless sensor network. Martin and Paterson proposed an ultra-lightweight key predistribution scheme[17] for one-dimensional wireless sensor networks.

Another issue is to ensure the robustness of sensor networks and to measure it. The random deployment of nodes results in an uneven connectivity with critical nodes, making the network non-robust to node failure. Venuturumilli and Minai proposed a distribution algorithm[22] to design a robust and energy-efficient network that optimizes the transmission range for each sensor node. Some studies consider robustness against random node failure[6][5][18], as in a general heterogeneous network that is highly optimized, and in which an adversary breaks some sensor nodes to obstruct the transmission of data. There is currently not enough discussion about robustness against node-destruction attacks. Furthermore, how to evaluate the impact of node-destruction attacks is an open issue. In this paper, we use a random distribution model of a sensor network and analyze its robustness against a sensor node breaking attack under a simple key sharing model.

3. Sensor Network

In this section, we introduce a sensor network model and key establishment mechanism for our analysis.

3.1 Nodes of Sensor Network

Generally, a sensor network consists of cheap sensor nodes that are able to communicate only with their neighbor sensor nodes, and one other type of node, a master node that communicates with sensor nodes and belongs to an upper layer network that consists of other master nodes[7][11][24]. The master nodes are needed to gather information from sensor nodes and transfer it to a system that monitors information from all sensor nodes. We assume a sensor network that consists of two types of nodes: master nodes (M) and sensor nodes (S).

-Master node. The master node has a connection with an upper layer network of master nodes and connections with sensor nodes. Thus, the master node passes communications between two different networks, as shown in Figure 1. The master nodes receive information from sensor nodes and transfer the received information to a server via the upper layer network. We assume that master nodes have two different capabilities: a master node can store n secret keys, and another type of master nodes has unlimited memory resources, so the master nodes can store any number of secret keys.

-Sensor node. The sensor nodes only have limited computing resources and short range communication capability. The sensor nodes communicate with each other and with master nodes, if a secret key is shared. The number of secret keys that is stored in a sensor node is limited to n.

The sensor network consists of clusters that have sensor nodes and a master node, and all data gathered by the sensor nodes is sent to out of the sensor network via the master node.

3.2 Key Sharing Model

We use a random pair-wise key model to share a secret key between two nodes. In this model, the compromise of any sensor nodes does not affect the secret keys established between non-compromised sensor nodes, since every key is generated randomly and independently for each connection.

A sensor node shares a secret key with n nodes. As an initialization phase, the sensor node randomly chooses a node i that is within its area of wireless communication and executes a key-exchange protocol to share a secret key k_i with the node. The sensor node finishes the initialization phase of the key exchange when it is finished sharing secret keys with n pairing nodes. A pre-shared master key k_{init} that is stored in nodes at the initialization phase is used for the key exchange protocol, and it is removed after the initialization phase. Sensor nodes communicate with other nodes using a secret key shared with each node. Note that security on the initialization phase is outside the scope of the paper; several existing random key predistribution schemes[23] are applicable to the initialization phase. For simplicity, a re-establishment scheme for a secret key in cases of destructions of paring nodes is omitted from the model.

Security Aspects. It is assumed that the initialization process is securely executed and an adversary cannot obtain the pre-shared master key after the initialization phase in the above model. Generally, there is a tradeoff between the security and the robustness of the sensor network; we can avoid leakage of the pre-shared master key to remove it after the initialization phase. However, a sensor node cannot share a new secret key with a new sensor node, where a pairing sensor node is broken or lost. We analyze the robustness based on a simplified model of the sensor network in the later section.

4. Analysis

In this section, we explain the model used in our analysis, which includes a model of a sensor network, an adversary model, and an index for estimating attack impact.

4.1 Model for Sensor Network

Figure 1 shows our model. We use a general 3-dimensional model for a sensor network. Sensor nodes are randomly assigned to lattice points of a periodic cubic lattice, with a probability *r*. A periodic boundary condition is considered for the model defining a large sensor network. In the initial phase, a sensor node randomly selects *n* nodes that lie closer than a Manhattan distance d_{max} and shares a secret key with the nodes. Note that the Manhattan distance is essentially corresponding to the physical distance under the 3-dimensional lattice model. Each sensor node can communicate with other sensor nodes and with master nodes that have the same secret key. Here, the distance $d(n_1, n_2)$ between two nodes n_1, (x_1, y_1, z_1) and n_2, (x_2, y_2, z_2) is defined as a Manhattan distance, and is calculated as follows:

$$
\begin{aligned}
d(n_1, n_2) = min\{ & |x_1 - x_2| + |y_1 - y_2| + |z_1 - z_2|, \\
& |x_1 - x_2| + |y_1 - y_2| + (L - |z_1 - z_2|), \\
& |x_1 - x_2| + (L - |y_1 - y_2|) + |z_1 - z_2|, \\
& (L - |x_1 - x_2|) + |y_1 - y_2| + |z_1 - z_2|, \\
& |x_1 - x_2| + (L - |y_1 - y_2|) + (L - |z_1 - z_2|), \\
& (L - |x_1 - x_2|) + |y_1 - y_2| + (L - |z_1 - z_2|), \\
& (L - |x_1 - x_2|) + (L - |y_1 - y_2|) + |z_1 - z_2|, \\
& (L - |x_1 - x_2|) + (L - |y_1 - y_2|) + (L - |z_1 - z_2|)\}
\end{aligned}
$$

where *L* is the length of an edge of the cubic lattice.

4.2 Threat and Adversary Model

There are two essential threats to sensor networks; attacks on communicated data, and breaking of the sensor network by an adversary. The first threat is that the attacker tries to eavesdrop on, or alter, the data communicated between sensor nodes, and the threat includes the discovery of a secret key. Communicated data can be protected using cryptographic primitives: an encryption algorithm and a message authentication algorithm. The corruption of a sensor node to obtain a secret key is still an open issue; there are some practical solutions for the threat, such as tamper-resistant hardware.

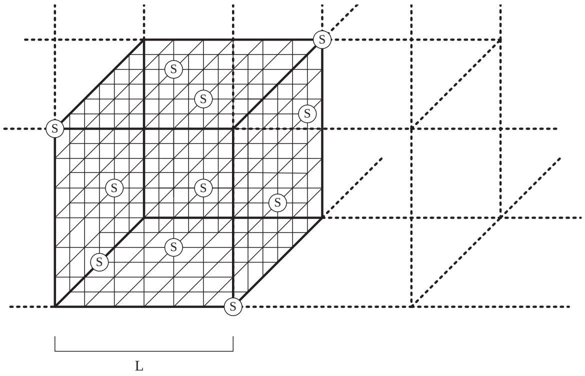


Fig. 1 Periodic Model of Sensor Network

In this paper, we focus on the other threat, which is that an adversary tries to break a sensor network. We assume an adversary model in which an adversary cannot obtain the entire structure of the target sensor network and randomly attack a node to break the entire sensor network.

Each attack randomly breaks one node that is a sensor node or a master node. Any sensor node has a limited number of connections with nearby sensor nodes, and the sensor node can transfer data to the upper layer network via master nodes. If one node is attacked and broken, communication that passes to other nodes that are connected to the broken node may be lost. The efficiency of the attack is evaluated by the number of broken sensor nodes required to isolate all sensor nodes from the upper-layer network. When all sensor nodes in the whole sensor network are broken or unable to communicate with master nodes, the attack is completely successful.

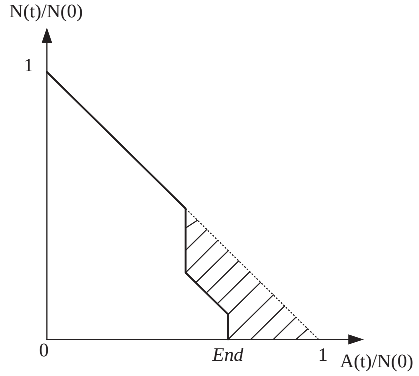


Fig. 2 Example of Simulation Result

4.3 Impact of Attack

We evaluate the robustness of sensor networks as we modify the number of sensor nodes and master nodes. We execute a simulation program and estimate the impact of an attack against a sensor network. An example of simulation results is shown in Figure 2. The functions $N(t)$ and $A(t)$ are the number of sensor nodes that can send data to the upper-layer network via master nodes, and the total number of attacked nodes at time t, respectively. The number of sensor nodes in the initial state is denoted as $N(0)$. The simulation is terminated when $N(t) = 0$. The graph shows the change in the number of nodes that can communicate with a master node as the number of attacks increases. The graph is a straight line from $N(t)/N(0) = 1$ to $A(t)/N(0)$, where the number of nodes that are disconnected from master nodes is the same as the number of broken nodes. The shaded area indicates the impact of the attack. For evaluation of the robustness of the sensor network, we define the index $I(N(t), A(t), N(0))$ as the ratio of the shaded area for the area of the triangle $T = 1/2$.

We use the percolation theorem[25] to consider the condition that all sensor nodes make a large network. The maximum number of sensor nodes within distance d can be calculated as $\frac{2d(2d^2+3d+4)}{3}$. Thus, we estimate the number of sensor nodes $N_S^C(0)$ that a sensor node can communicate with as follows:

$$N_S^C(0) = \frac{2d(2d^2+3d+4)}{3} \times r$$

where r is the probability that a sensor node exists on the lattice point in the initial state.

By the bond-percolation theorem, it is expected that the sensor nodes construct a large network when $N_S^C(0) > 1.5$.

5. Simulation Results

In this section, we present the results of simulations that evaluate attack impacts on the sensor network. Parameters for the simulation are summarized in Table 1.

We discuss the difference between two methods and consider the optimal parameters for a constant cost to develop a sensor network.

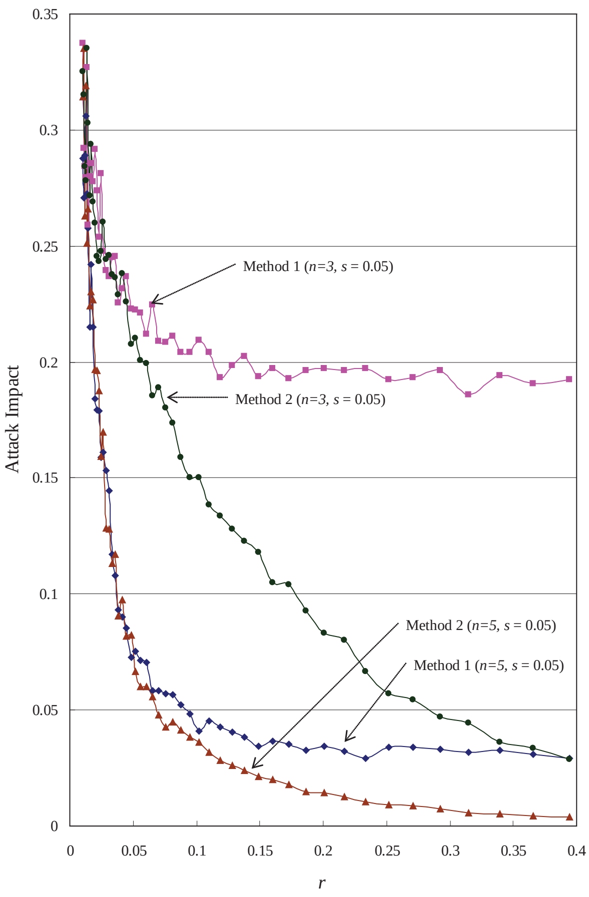


Fig. 3 Comparison of Attack Impacts

5.1 Result

We implemented a simulation program for estimating attack impacts on the sensor network model. We evaluated the following two methods that construct a sensor network:

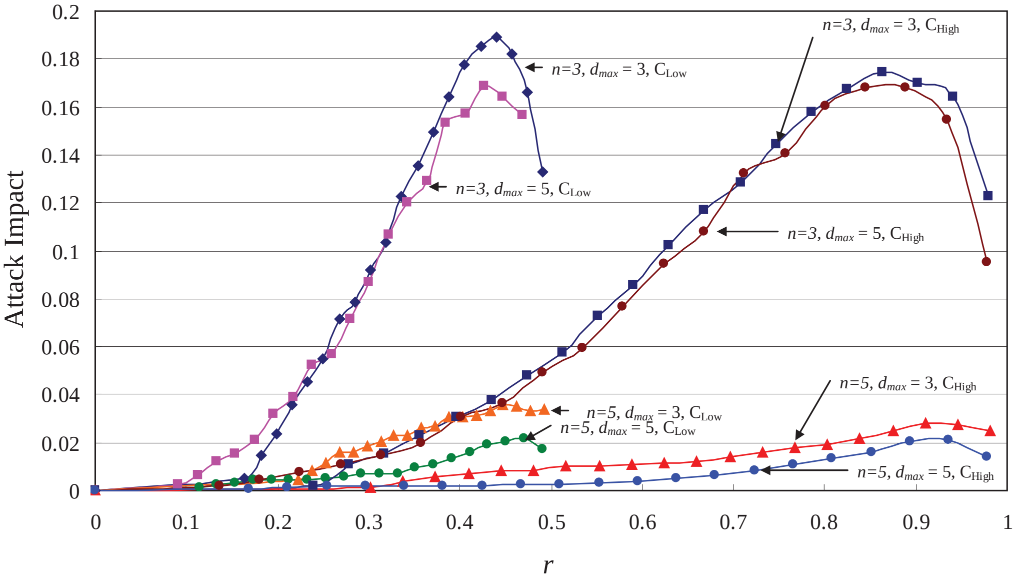


Fig. 4 Attack Impact under Constant $C/\alpha L^3$

Table 1: Parameters for Analysis

	Parameter	Value
L	Length of an edge	20
r	Prob. that a sensor node exists on the lattice point in the initial state	0.001--0.5
s	Ratio of a master node t o sensor nodes	0.05--0.45
N(0)	Number of sensor nodes(including master nodes) in the initial state	rL^3
$N_S(0)$	Number of sensor nodes in the initial state	(1-*s*)*N*(0)
$N_M(0)$	Number of master nodes in the initial state	*sN*(0)
d_{max}	maximum distance that a sensor node can communicate	3,5
n	Number of secret keys that a sensor node can store	3,5

-Method 1. The master nodes and sensor nodes can store *n* secret keys, and *n* nodes are randomly selected to share a secret key with nodes that are closer than d_{max} .

-Method 2. The sensor nodes can store *n* secret keys. A sensor node first shares the secret key with a master node that is closer than d_{max} , then shares *n*-1 secret keys with randomly selected sensor nodes that are closer than d_{max} .

The sensor node randomly selects *n* nodes to share the secret key when no master node lies closer than d_{max} . The master nodes have unlimited memory resources, so a master node can share a secret key with all nodes within the distance $\frac{2d_{\max}(2d_{\max}^2+3d_{\max}+4)}{3}$.

Result of Method 1. Figure 5 and figure 6 in Appendix A show simulation results of attack impacts for several conditions of **Method 1**. In the simulation in figure 6, we set parameters $n = 5$, $d_{max} = 5$ and $s = 0.05$, 0.15, 0.25, 0.35, 0.45. We estimated the attack impact according to the probability *r*. To increase the probability *r*, the attack impact dramatically declined, and it remained almost stable for any case of the probability *s*, where $r \geq 0.1$. Figure 7 shows the case of $n = 3$. The reduction of the attack impact is similar to the case of $n = 5$ and it is also almost constant where $r \geq 0.1$. However, the attack impact is still high due to the limitation on the number of shared secret keys. The results suggest that we configure $r \geq 0.1$ and that we should select a large enough *n*, such as $n = 5$.

Result of Method 2. Figure 7 and figure 8 in Appendix A show simulation results of attack impacts for several conditions of **Method 2**. The results are similar to the result of **Method 1**. The attack impacts are dramatically reduced where $r \geq 0.1$, except $s = 0.05$. The results when $s = 0.05$ suggest that the outcome is sensitive to the proportion of master nodes, due to the rule in **Method 2** that a sensor node must first connect with a master node within the communication range d_{max} .

5.2 Comparison and Optimization

We compare two models in Figure 3. The attack impact is reduced by changing to **Method 2** from **Method 1**. Especially, **Method 2** is very effective where *n* is small.

Now, we assume that the cost ratio *w* of a sensor node and a master node is defined as the ratio of their memory sizes. That is,

$$w = \frac{r \times 2d_{\max}(2d^2_{\max} + 3d_{\max} + 4)}{3}$$

The total cost C of the system is calculated as:

$$C = \alpha\ L^3(r(1-s)n + rsw)$$

where α is a constant value. We evaluate some pairs of (r, I), where $C/\alpha\ L^3$ is a constant value. We uses two different value of C: C_{High} and C_{Low} = $C_{High}/2$. We evaluated two values of n and d_{max}, that are 3 and 5, and variable r. Figure 4 shows the results of the evaluation. The attack impact increases with increasing r due to the reduction of the number of master nodes, and this trend is the same for different values of d_{max}, because the total cost is a constant value and the ratio of the master nodes is reduced according to increase of the total number of nodes. However, the attack impact is reducing for enough large values of r, because the number of connections between sensor nodes is increased and the increase of the connections makes the sensor network more robust against the node-destruction attack. That is, the increase of sensor nodes covers the decrease of master nodes, and connectivity is kept by the network between sensor nodes, even though the number of connections between a sensor node and a master node is reduced. A size of area for the sensor network depends on the total number of sensor and master nodes. Thus, it is a good solution that the total number of sensor nodes is enough large beyond a threshold value that has the highest attack impact, in terms of improving both the cover area and the robustness against a node-destruction attack.

5. Conclusion

We modeled a sensor network as a periodic cubic lattice and proposed an index for estimating the impact of a node-destruction attack. We then presented simulation results that indicated effective strategies to design a sensor network that is robust against a node-destruction attack. First, it is showed that sensor nodes preferentially should share secret keys with master nodes in the initial phase. Furthermore, it is cost-effective to increase the number of sensor nodes beyond a threshold value, in terms of both the cover area and the robustness. We believe that our results will be useful for improving the trustworthiness of sensor network design.

Appendix

We show simulation results in this appendix. Figure 5 and Figure 6 show the results of **Method 1**, cases n = 5 and n = 3. Figure 7 and Figure 8 show the results of **Method 2**, cases n = 5 and n = 3.

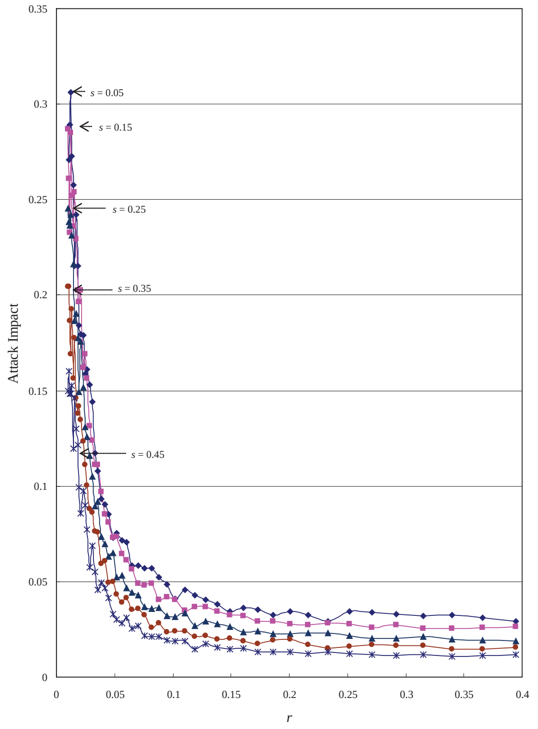


Fig. 6 Attack Impact(Method 1, n = 5)

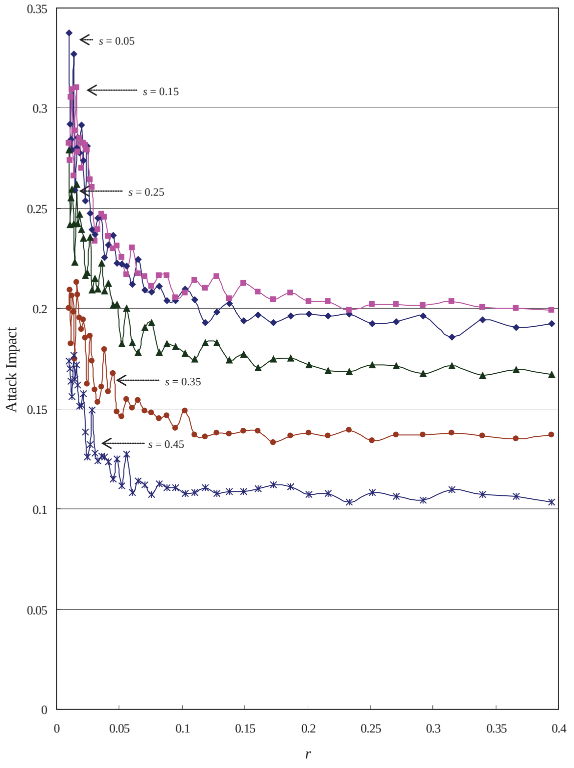


Fig. 7 Attack Impact (Method 1, n = 3)

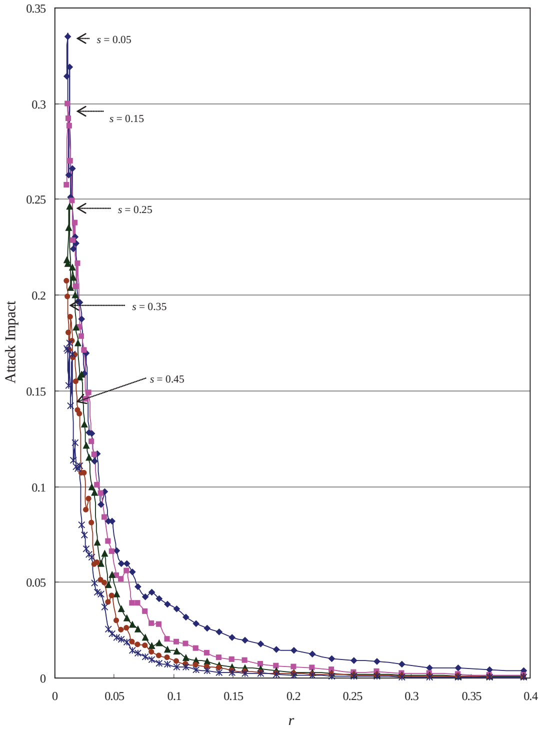


Fig. 8 Attack Impact(Method 2, n = 5)

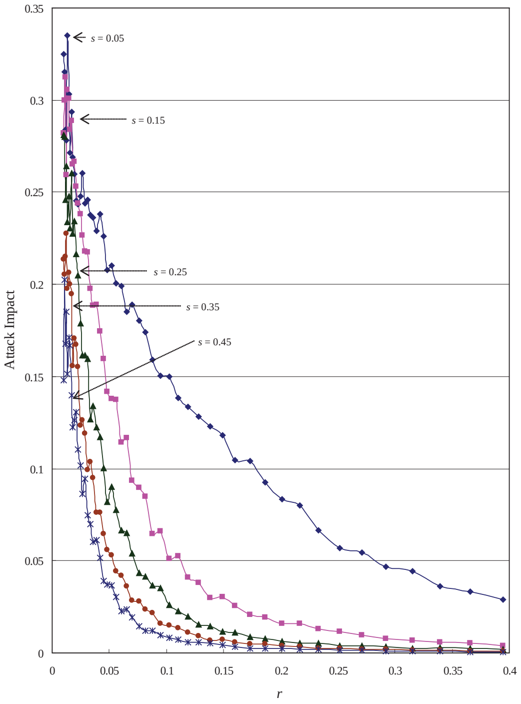


Fig. 9 Attack Impact (Method 2, n = 3)

References

[1] I.F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *Communications Magazine*, *IEEE*, 40(8):102 - 114, 2002.

[2] Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives, and Insup Lee. Sensor network security: more interesting than you think. In *Proc. of the 1st USENIX Workshop on Hot Topics in Security* 25-30, 2006.

[3] F. Anjum. Location dependent key management in sensor networks without using In *Proc. of 2nd International Conference on Communication Systems Software and Middleware*, COMSWARE 2007, 2007.

[4] Haowen Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *Proc. Of 2003 symposium on Security and Privacy*, pages 197-213, 2003

[5] P. Crucitti, Latora V., M. Marchiori, and Rapisarda A. Error and attack tolerance of complex networks. In *Physica A*, volume 304, Issue 1-3, pages 388 - 394, 2004.

[6] Anthony H. Dekker and Bernard D. Colbert. Network robustness and graph topology. In *Proc. of the 27th Australasian conference on Computer Science*, volume 26 of *ACSC* '04, pages 359 - 368, 2004.

[7] Peter Desnoyers, Deepak Ganesan, and Prashant Shenoy. Tsar: a two tier sensor storage architecture using interval skip In *Proc. of the 3rd international conference on Embedded networked sensor systems*, SenSys '05, pages 39 - 50, 2005.

[8] Wenliang Du, Jing Deng, Y.S. Han, Shigang Chen, and P.K. Varshney. In *Proc. of 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, INFOCOM 2004, 2004.

[9] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In *Proc. of the 10th ACM conference on Computer and communications security*, CCS '03, pages 42 - 51, 2003.

[10] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *Proc. of the 9th ACM conference on Computer and communications security*, CCS '02, pages 41 - 47, 2002.

[11] Omprakash Gnawali, Ki-Young Jang, Jeongyeup Paek, Marcos Vieira, Ramesh Govindan, Ben Greenstein, August Joki, Deborah Estrin, and Eddie Kohler. The tenet architecture for tiered sensor networks. In *Proc. of the 4th international conference on Embedded networked sensor systems*, SenSys '06, pages 153 - 166, 2006.

[12] Lin He, Yi-Ying Zhang, Lei Shu, A.V. Vasilakos, and Myong-Soon Park. Energy-efficient location-dependent key management scheme for wireless sensor networks. In *Proc. of 2010 IEEE Global Telecommunications Conference*, GLOBECOM 2010, 2010.

[13] H. Ito, A. Miyaji, and K. Omote. Rpok: A strongly resilient polynomial-based random key pre-distribution scheme for multiphase wireless sensor networks. In *Proc. of 2010 IEEE Global Telecommunications Conference*, GLOBECOM 2010, 2010.

[14] Jiejun Kong, Z. Petros, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing robust and ubiquitous security support for

mobile ad-hoc networks. In *Proc. of 9th International Conference on Network Protocols*, pages 251 - 260, 2001.

[15] Donggang Liu and Peng Ning. Establishing pairwise keys in distributed sensor networks. In *Proc. of the 10th ACM conference on Computer and communications security*, CCS '03, pages 52 - 61, 2003.

[16] Donggang Liu, Peng Ning, and Wenliang Du. Group-based key pre-distribution in wireless sensor networks. In *Proc. of the 4th ACM workshop on Wireless security*, WiSe '05, pages 11 - 20, 2005.

[17] Keith M. Martin and Maura B. Paterson. Ultra-lightweight key predistribution in wireless sensor networks for monitoring linear infrastructure. In *Proc. of the 3rd IFIP WG 11.2 International Workshop on Information Security Theory and Practice. Smart Devices, Pervasive Systems, and Ubiquitous Networks*, WISTP '09, LNCS, pages 143 - 152, 2009.

[18] G. Paul, T. Tanizawa, Havlin S., and Stanley H. E. Optimization of robustness of complex networks. In *The European Physical Journal B*, volume 38, pages 187 - 191, 2004.

[19] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, and David E. Culler. Spins: security protocols for sensor networks. *Journal of Wireless Networks*, 8:521 - 534, 2002.

[20] S. Ruj, A. Nayak, and I. Stojmenovic. Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs. In *Proc. of INFOCOM, 2011, IEEE*, pages 326 - 330, 2011.

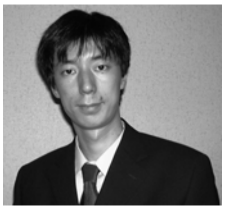
[21] Kun Sun, Peng Ning, and Cliff Wang. Tinysersync: secure and resilient time synchronization in wireless sensor networks. In *Proc. of the 13th ACM conference on Computer and communications security*, CCS '06, pages 264- - 277, 2006.

[22] A. Venuturumilli and A. Minai. Obtaining robust wireless sensor networks through self-organization of heterogeneous connectivity. In *Proc. of the 6th International Conference on Complex Systems*, 2006.

[23] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway. A survey of key management schemes in wireless sensor networks. *Comput. Commun.*, 30(11-12):2314- - 2341, 2007.

[24] Rui Zhang, Jing Shi, and Yanchao Zhang. Secure multidimensional range queries in sensor networks. In *Proc. of the 10th ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '09, pages 197 - 206, 2009.

[25] Seymour, P. D. and Welsh, D. J. A. Percolation probabilities on the square lattice. Advances in graph theory (Cambridge Combinatorial Conf., Trinity College, Cambridge, 1977). Ann. Discrete Math., 3, (1978), 227 - 245.



Shinsaku Kiyomoto received his B.E. in Engineering Sciences, and his M.E. in Materials Science, from Tsukuba University, Japan, in1998 and 2000, respectively. He joined KDD (now KDDI) and has been engaged in the research on stream cipher, cryptographic protocol, and mobile security .He is currently a senior researcher of the Information Security Lab. in KDDI R&D Laboratories, Inc. He received the Dr. degree in engineering from Kyushu University in 2006.He was a visiting researcher of the Information Security Group, Royal Holloway University of London from 2008 to 2009.He received the Young Engineer Award from IEICE in 2004.He is a member of the Physical Society of Japan and Institute of Electronics, Information and Communication Engineers.

Kazuhide Fukushima received his M.E. in Engineering from Kyushu University, Japan, in 2004.He joined KDDI and has been engaged in research on digital rights management (DRM) technologies, including software obfuscation and key-management schemes. He is currently a researcher at the Information Security Lab. of KDDI R&D Laboratories, Inc. He received his Doctorate in Engineering from Kyushu University in 2009.He is a member of Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan, and ACM.

Yutaka Miyake received his B.E. and M.E. degrees in Electrical Engineering from Keio University, Japan, in 1988 and 1990, respectively. He joined KDD (now KDDI) in 1990 and has been engaged in the research on high-speed communication protocol and secure communication system. He received his Dr. degree in Engineering from the University of Electro-Communications, Japan, in 2009. He is currently a senior manager of the Information Security Laboratory in KDDI R&D Laboratories Inc. He received IPSJ Convention Award in 1995 and the Meritorious Award on Radio of ARIB in 2003. He is a member of Institute of Electronics, Information and Communication Engineers, and the Information Processing Society of Japan.