Distributed Detecting Node Replication Attacks in Wireless Sensor Networks: A Survey

Wei Teng Li[1], Tung-Huang Feng[2], and Min-Shiang Hwang[2,3]

(Corresponding author: Min-Shiang Hwang)

Department of Management Information System, National Chung Hsing University[1]
Department of Computer Science & Infoarmation Engineering, Asia University[2]
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
Department of Health Services Administration, China Medical University[3]
(Email: mshwang@asia.edu.tw)

(Invited Jan. 20, 2014; revised and accepted May 4, 2014)

Abstract

Wireless Sensor Networks (WSNs) are composed of a number of resource-constrained sensor nodes which are often deployed in unattended environments. Therefore, WSNs easily encounter a variety of physical attacks.In this paper, we focus on one of physical attacks known as node replication attack, where an intruder randomly captures a legitimate sensor node, and collects all secret element. Then an intruder inserts the secret element in his malicious sensor nodes and deploys the malicious sensor nodes into the network. An intruder can use malicious nodes eavesdrop on the communication of other sensors, or inject false data reports that make a server misjudge. In recent years, detecting node replication attack is an important task in sensor network area.In our survey, we analyze previous research and demonstrate contributions of the existent literatures.

Keywords: Distributed protocol, node replication attack, wireless sensor network

1 Introduction

Wireless Sensor Networks (WSNs) are rapidly used to many areas including military\surveillance, pollution tracking, landslides detection, fire detection, nuclear power plants, ocean water quality monitoring and medical health care, etc. [2, 19]. Because WSNs consists of many tiny computing sensor nodes, they are deployed in an area for sensing data and transmitting data to base station for further processing. Base station is a data sink and is responsible for data collection, data analysis and maintaining all the sensor nodes in WSNs. It is a more powerful node than sensors in the network so that an intruder cannot compromise the base station as well.

However, the low cost sensor nodes can be easily compromised by an intruder because these sensors are exposed in an unattended and unsupervised environment [4, 34]. The resource-starved sensors lure an intruder to attack the network. Therefore, protecting WSNs from the physical attacks such as node capture attack, sybil attack and black holes [18, 32, 33], is a major area of concern. One of physical attacks is known as node replication attack that an intruder can get into the network. In this attack, an intruder randomly captures a legitimate sensor node, and collects all secret element. Then an intruder inserts the secret element in his malicious sensor nodes and deploys the malicious sensor nodes into the network. An intruder can use malicious nodes eavesdrop on the communication of other sensors, or inject false data reports that make a server misjudge [1, 35].

To prevent this attack, recently many research have proposed the scheme to solve this problem, and detecting node replication attack is an important task in sensor network area. Some solutions are based on key distribution schemes [10, 11, 16, 23, 27, 30, 38]. Some solutions are based on mutual authentication schemes [12, 17, 26]. Some solutions are based on location-aware and Trust-based protocols that detect and isolate compromised nodes [9, 10]. Some solutions are based on routing algorithms [15, 24, 25]. Some solutions are based on energy-efficient protocols [3, 13, 22]. In this survey, we focus on distributed node replication detection scheme and analyze previous researches and demonstrate contributions of the existent literatures in detail.

The rest of paper is arranged as follows. In Section 2, we introduce the basic requirements and evaluation metrics requirement used to analyze previous researches. Section 3 presents the existing schemes for replication detection in WSNs. Section 4, we analyze previous researches and demonstrate contributions of the existent literatures. In Section 5 we discuss the future work of a node replication attack. Finally, we make a conclusion in Section 6.

2 Basic Requirements and Evaluation Metrics

They are classified into two types of node replication schemes: *Centralized detection* and *Distributed detection*.

1. *Centralized detection*: In a centralized scheme, each node needs to send its neighbor's identity list and location to the base station. If the base station discovers the conflict location with the same identity, it would revoke the replication node immediately. However, this scheme has several drawbacks [31]. First, the base station suffers from a single point of failure. Second, the nodes closest to the base station will become a compromised target for the intruder and will receive heavy flooded traffic. Finally, the base station will delay revocation, because the base station has to receive all the report from the WSNs and analyze them. A centralized scheme on sensor networks can be found in [5, 6, 36].

2. *Distributed detection*: The first distributed detection scheme was proposed by Parno et al. in 2005 [31]. In a distributed detection, each node broadcast its identity and location information to its neighbor. Then its neighbor will send the node's information to a randomly selected node called a witness node. The witness node can detect node replication attack by checking the ID with its location. Distributed detection scheme can revoke replicated node quickly and the base station will not become a single point of failure. In this paper, we focus on the distributed detection scheme and analyze previous researches and demonstrate contributions of the existent literatures. Notations for distributed replication detection are summarized in Table 1.

The previous survey [20, 39] did not classify security metrics. In this paper, we summarize basic security requirements of a node replication attack. All distributed detection schemes must follow traditional security requirements: data confidential, data protection, integrity and non-repudiation. In addition, according to the unique features of a node replication attack, we present the basic requirements and evaluation metrics in the following security metrics and efficiency metrics.

2.1 Security Metrics

1. Node revocation: When replicated nodes are detected, the WSN should be capable of revoking them quickly. To prevent a node replication attack, an efficient scheme has to detect whether the nodes are compromised or not. Therefore, an intruder can not use this malicious nodes eavesdrop on the communication of other sensors, or inject false data reports that make a server misjudge.

2. Collusion resistance: If a number of nodes leave the network or are compromised by the intruder, the intruder cannot use these nodes' security element to compromise the whole network. A good detection mechanism must resist the collusion of malicious nodes.

3. Resilience: When an intruder physically captures several sensor nodes and collects all secret element. Then he inserts the secret element in his malicious sensor nodes and deploys the malicious sensor nodes into the network. If resilience is high, the network is still available. Otherwise, if resilience is low, it may make the whole network broken down.

4. Lightweight: Sensor nodes are usually composed of low memory, energy and computation. Sensors can not afford the heavy replication detection mechanism which will consume large power and complex computation. Therefore, a lightweight detection scheme is an important principle for resource-constrained wireless sensor network.

2.2 Efficiency Metrics

1. Memory: Sensor's memory always stores node's identity that can identify each legitimate sensor node in the network, security element, such as node's public, private key and session key.

2. Energy: Energy consumption is one of the most important thing that has to be concerned in wireless sensor network. Complex computation will lead to a amount of energy consumption, so designing an efficient detection scheme is a necessary task.

Table 1: Notations for distributed replication detection

BS	Base station
ID_α	Node α's identity
SK_α	α's private key
l_α	Deployment location by node α
R_B	a random number generated by base station
R_α	a random number generated by node α
$H(.)$	a one-way hash function
n	Network size
d	Network density
g	number of witness nodes
N_Z	number of zone-leader in the network
p	The probability a neighber becomes a reporter
p_s	The probability a node becomes a witness node

3 Distributed Detection Schemes

In this section, we investigate several previous researches and analyze their contributions of the existing literatures.

There is not a central authentication in a distributed detection scheme. Each node broadcasts its identity and location information to its neighbor. Then its neighbor would send the identity and location claim to a randomly node called witness node. These detection mechanisms are often used in a distributed detection scheme called claimer-reporter- witness.

3.1 Node-to-Network Broadcasting and Deterministic Multicast

Node-to-network broadcasting (N2NB) were proposed by Parno et al. [31] which is a slightly simplified approach. In N2NB, each node in the network broadcasts an authenticated message in the entire network to claim its own location. Each node has a responsibility to store the location claim for its neighbors, incurring a storage cost of $O(d)$; and if a conflict happened, it would revoke the malicious nodes immediately. The N2NB protocol can achieve 100% detection rate of all replicate location claims as long as the broadcast reaches every node. Each node's location claim broadcast requires $O(n)$ message, and the total communication cost for N2NB protocol is $O(n^2)$.

The Deterministic Multicast (DM) is to improve on the communication cost of the previous protocol. The DM is a good example to explain claimer-reporter-witness framework. A claimer is a node which shares its location claim to its neighbors and its neighbors act as a reporter. The reporter uses claimer's ID and a function to choose the witness nodes. Then the reporter forwards the location claim to the chosen witness. If a replication node is deployed on the network, the witness will receive two different location claims from the same node. If the conflict happens, the witness will trigger the revocation mechanism. There is a problem in DM. If an intruder knows the claimer's ID and function, he/she will know the witness's location and compromise them before deploying his replication node.

3.2 Randomized Multicast and Line-Selected Multicast

Randomized multicast (RM) and line-selected multicast (LSM) were proposed by Parno et al. [31] in 2005, which is the distributed node replica detection mechanism proposed for the first time. The first algorithm is called Randomized multicast. In RM, each node α broadcasts its location claim (ID_α, l_α) to its one-hop neighbor. Then its neighbor(with probability p) send its location claim to a $O(\sqrt{n})$, a randomly selected witness node by using geographic routing. They claim using Birthday Paradox that can ensure at least one witness node will receive the location conflict of a replicated node with higher probability. However, assume the network average path length is $O(\sqrt{n})$, and the total communication cost is $O(n^2)$ which is as expensive as N2NB.

Because of the RM protocol's high communication cost, Parno et al. proposed another protocol to reduce the communication overhead and increase the probability of detection, which is called line-selected multicast (LSM). In LSM, a location claim travels a line from one node to another. Every intermediate node in this line has to store the location claim and each of them can also be witness nodes. If a node at the intersection of two lines can detect a conflict location claims. Compared with RM, LSM has a lower communication cost. However, it has several drawbacks which were mentioned by Zhang et al. [37] in 2009 and we will discuss [37] in Section 3.4.

3.3 Randomized, Efficient and Distributed Mechanism

Randomized, efficient and distributed mechanism (RED) was proposed by Conti et al. [7, 8] in 2007 and 2011. RED combines both advantage of DM and RM, but this protocol uses the witnesses chosen by pseudo-randomly based on a network-wide seed to improve network performance and a distributed protocol to detect node replication attacks. RED includes two steps: the first step, BS chooses a random number R_B and broadcasts this R_B to all nodes in the network. The second step, the claimer's neighbor uses a pseudo-randomly function to select the witness node. The pseudo-randomly function takes claimer's (ID_α, l_α), random number R_B and the number of witnesses. Node α needs to sign its location claim by using its private key SK_α before broadcast. Every node in the line from claimer to the witness node forwarding the signed claim is not allowed to add any message. When BS changes the R_B, the witness nodes will change as well. It can protect the witness nodes from an intruder knowing the witness's location and compromise them before deploying his replication node.

3.4 Memory Efficient Multicast: B-MEM, BC-MEM, C-MEM and CC-MEN

Zhang et al. [37] mentioned that LSM had three drawbacks. The three problems are memory overhead problem, crowded center problem and cross over problem. In the first problem, each node in LSM needs to store $O(\sqrt{n})$ claims and ensure high-level security, so the size of the claims should be so large to lead to sensor memory overhead. In the second problem, Zhang et al. claim the nodes which set up in the center area may have much higher communication cost than the nodes near the boundary. In the third problem, there is a certain probability that two line segments crossing each other do not intersect a real node. This makes cross over problem and the replica node will not be detected. So Zhang et al. [37] have proposed four mechanisms to detect node replication attacks efficiently. These four protocols are memory efficient multicast with Bloom filters (B-MEM), memory efficient multicast with Bloom filters and Cell Forwarding (BC-MEM), memory efficient multicast with cross forwarding(C-MEM), and memory efficient multicast with cross and cell forwarding (CC-MEM). They are discussed below.

3.4.1 B-MEM

The other three protocols are based on the B-MEN. B-MEN uses two compact Bloom filters to reduce the storage of location claims in LSM. In B-MEN, node α multicasts its location claim to its neighbor. Each neighbor has a probability p_s to become a witness node and sends a node α's location claim to a randomly location. The node which is close to this random location will become another witness node. Every node in the line segment just stores ID_α and l_α in the Bloom filters. The membership in the line segment can use Bloom filters to help them detect conflicting location claim.

3.4.2 BC-MEM

BC-MEN protocol divides the network into several cells that not only solve the cross problem but also reduce the storage overhead. In BC-MEN, there is an anchor point assigned for every node in the same cell. The anchor point is decided by every node's *ID* and a hash function. A node closest to the anchor point is assigned for an anchor node. Node's location claim is forwarded from one node to the other cell's anchor node, continuing until to the destination.

3.4.3 C-MEM and CC-MEM

C-MEN uses a new technique called *cross forwarding* to solve a crowded center problem. In C-MEN, C-MEN first selects a random point called cross point for each node in the network. The node closest to the cross point is assigned for a witness node and the location claim is forwarded to a witness node along the horizontal and vertical lines that pass the cross point. Note that C-MEN does not divide the network into cells and does not use cell forwarding.

CC-MEN is a combination of BC-MEN and C-MEN. It combines cell forwarding and cross forwarding to solve the cross over problem and crowded center problem. Similar to BC-MEN and C-MEN, CC-MEN divides the network into several cells, and each node has its corresponding anchor node. Also, CC-MEN randomly selects a cell and let the anchor point be the cross point as well. It can improve the probability of detecting node replication attack and performance.

3.5 Randomly Directed Exploration

In 2009, Li and Gong [28] proposed a randomly directed exploration (RDE) of a node replication attack. This protocol is based on N2NB. When deployed, every node in the network knows its neighbor ID and location. Each node uses a neighbor ID and location to make its own neighbor-list. This neighbor-list is used to detect node replication attack and for message forwarded. The network will set a global parameter direction, so each node should follow this direction to forward the message. The intermediate nodes will detect the node replication attack when a conflict happens. RDE's memory cost $O(\sqrt{d})$ is the same as N2NB, but the communication cost reduces from $O(n^2)$ to $O(\sqrt{n})$. However, RDE seems not feasible for a real wireless sensor network.

3.6 Distributed Detection of Node Capture Attacks in Wireless Sensor Networks

In 2010, a technique proposed by Ho [14] used the sequential probability ratio test to detect a replica node attack in the wireless sensor network. When a node is physically captured by an intruder, there is a period of time the node would not present in the network. Therefore, the protocol measures the absence time period of each sensor node and contrast the value to a pre-defined threshold. The protocol's detection rate depends on the properly threshold.

3.7 Zone-based Node Replica Detection Scheme

Mishra et al. [29] have proposed a node replication detection scheme based on dividing the network into several zones and each zone has a zone-leader, which has the ability to detect replica nodes in the network. Every node has to do the registration phase after deployment. Zone-leaders will broadcast a zone registration($ZONE\_REGD$) to every node in the network. Then the node will send back the zone join($ZONE\_JOIN$) message to a zone-leader which is close to it.

In this protocol detecting mechanism is done at two-levels. The first level is called intra-zone detection. If a node wants to join in a zone after all nodes finish registration. A zone-leader will receive the join message of the new node. The zone-leader will check the member list in its own zone. If node ID is already in its member list, the zone-leader will broadcast a zone revoke message for the replica node and remove the replica node from the network immediately. Otherwise, it will go to the second level check. When a new node ID is not in the member list of the current zone. The zone-leader will send the join message to other zone-leader to check whether the node ID exists in other member list or not. When the two-level is done, the node will be added in the member list and joined in the network.

Most of the node replication detection protocols have to maintain the location claims. It would cost additional storage overhead. In zone-based detection, each node does not need to store any location claim in their memory, and the locations are independent. It can minimize the storage overhead problem. However, the protocol is based on the trusty zone-leader. When an intruder replicates the zone-leader, the wireless network will be compromised. In

Table 2: Summary of scheme

Scheme	Advantage	Disadvantage
N2NB [31]	Higher detection rate	Higher communication cost
DM [31]	Lower communication cost	Higher Memory cost
RM [31]	1.More resilience 2.Unpredictable witness	1.Lower detection probability 2.Higher communication cost
LSM [31]	1.Improved communication cost 2.Enhance detection probability	1.Crowded center problem 2.Cross over problem
RED [8, 7]	1.Lower memory cost 2.Higher detection rate	Need trusted third party
Zhang et al. [37]	1.Solve Crowded center problem 2.Solve Cross over problem 3.Solve memory overhead problem	Location dependent
RDE [28]	1.Higher detection rate 2.Consume minimum memory	feasible for ideal network model
Ho [14]	Use the sequential analysis	Set properly threshold
ZBNRD [29]	1.Location independent 2.No memory overhead 3.Higher detection probability	Compromised zone-leader threat

the same year 2013, another zone based protocol has been proposed by Koshy et al. [21]. This protocol includes four modules:zone formation, trust management, replica detection and performance analysis. Zone-leaders use trust factors to detect the replica node. The detection of a node replication attack is based on trust value, which will be calculated for each node.

4 Discussions

In this section, we summarize the above protocols of their pros and cons in Table 2. Then we use basic requirements and evaluation metrics mentioned in Section 2 to analyze the security and performance of the related work. Each protocol has its advantage and drawbacks. According to the recent study, it shows that there still have a lot of challenges in a node replication attack.

4.1 Security and Performance Analysis

Table 3 shows the basic security merits summarized in Section 2. We use these four requirements to analyze the previous protocol. Each protocol has reached the node revocation which can detect the malicious nodes in the network and revoke them immediately. We also show the performance of the related work in Table 4.

5 Future Research

According to the recent researches, it shows the future work of node replication attack still needs to design for a real-life WSNs situations. Because of resource-constrained environments, the protocol has to be equipped with lightweight and security. A zone-based replication detection will be a target to follow. A zone-based detect mechanism does not need to store any location claim in nodes memory, and it provides network with efficient self-organization as well as self-healing. The protocol to be designed can be implemented in a real environment. For instance, we can implement these protocols to military surveillance, pollution tracking, landslides detection, fire detection, nuclear power plants, ocean water quality monitoring and medical health care to let these protocols can bring what they have learnt into full play.

6 Conclusions

Recently a wireless sensor network has been used in many areas. In this paper, we focus on one of physical attacks known as s node replication attack and have reviewed the existing techniques that can detect a node replication attack on a distributed scheme. We also give the basic requirements of security and efficiency metrics using these basic requirements to highlight security and performance advantage and disadvantage of previous researches. However, according to the recent study, it shows that there still have a lot of challenges in a node replication attack. It needs to be designed for a real-life situations and resource constrained wireless sensor network.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC102-2221-E-468-020 and NSC101-2622-E-468-002-CC3. The authors gratefully acknowledge the anonymous reviewers for their valuable

Table 3: Summary of scheme security

Scheme	Node revocation	Collusion resistance	Resilience	Lightweight
N2NB [31]	Yes	No	Medium	No
DM [31]	Yes	Partial	Medium	No
RM [31]	Yes	Partial	Low	No
LSM [31]	Yes	Partial	Medium	Yes
RED [8, 7]	Yes	Yes	High	Yes
Zhang et al. [37]	Yes	Yes	High	Yes
RDE [28]	Yes	Partial	High	No
Ho [14]	Yes	Partial	Medium	Yes
ZBNRD [29]	Yes	Partial	High	Yes

Table 4: Summary of scheme costs

Scheme	Communication	Storage
N2NB [31]	$O(n^2)$	$O(d)$
DM [31]	$O(dlog\sqrt{n}/d)$	$O(g)$
RM [31]	$O(n^2)$	$O(\sqrt{n})$
LSM [31]	$O(n\ \sqrt{n})$	$O(\sqrt{n})$
RED [8, 7]	$O(d\ g\ p\ \sqrt{n})$	$O(d\ p\ g)$
B-MEN [37]	$O(n\ \sqrt{n})$	$O(\sqrt{n})$
RDE [28]	$O(d\ n\ \sqrt{n})$	$O(d)$
Ho [14]	$O(n\ \sqrt{n})$	$O(n)$
ZBNRD [29]	$O(n\ \sqrt{N_Z})+O(N_Z\ \sqrt{n})$	$O(d)/O(N_Z)$

comments.

References

[1] A. Agah and S. K. Das, "Preventing dos attacks in wireless sensor networks: A repeated game theory approach," *International Journal of Network Security*, vol. 5, no. 2, pp. 145–153, 2007.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications*, vol. 40, no. 8, pp. 102–114, 2002.

[3] M. Asadi, C. Zimmerman, and A. Agah, "A game-theoretic approach to security and power conservation in wireless sensor networks," *International Journal of Network Security*, vol. 15, no. 1, pp. 50–58, 2013.

[4] B. S. Babu, N. Jayashree, and P. Venkataram, "Performance analysis of steiner tree-based decentralization mechanism (STDM) for privacy protection in wireless sensor networks," *International Journal of Network Security*, vol. 15, no. 5, pp. 331–340, 2013.

[5] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Trans. Systems, Man and Cybernetics, Part C: Applications and Rev.*, vol. 37, no. 6, pp. 1246–1258, 2007.

[6] H. Choi, S. Zhu, and T. F. La Porta, "Set: Detecting node clones in sensor networks," in *Proceedings of the 3rd international conference on security and privacy in communications networks and the workshops(SecureComm'07)*, pp. 341–350, 2007.

[7] M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 5, pp. 685–698, 2011.

[8] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 07)*, pp. 80–89, 2007.

[9] G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," *International Journal of Network Security*, vol. 12, no. 2, pp. 107–117, 2011.

[10] A. K. Das, "An identity-based random key predistribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *International Journal of Network Security*, vol. 6, no. 2, pp. 134–144, 2008.

[11] A. K. Das, “Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks,” *International Journal of Network Security*, vol. 14, no. 1, pp. 1–21, 2012.

[12] F. Dressler, “Authenticated reliable and semi-reliable communication in wireless sensor networks,” *International Journal of Network Security*, vol. 7, no. 1, pp. 61–68, 2008.

[13] S. Faye and J. F. Myoupo, “Secure and energy-efficient geocast protocol for wireless sensor networks based on a hierarchical clustered structure,” *International Journal of Network Security*, vol. 15, no. 3, pp. 151–160, 2013.

[14] J. W. Ho, “Distributed detection of node capture attacks in wireless sensor networks,” *Smart Wireless Sensor Networks InTech*, pp. 345–360, 2010.

[15] B. Kadri, M. Feham, and A. Mhammed, “Efficient and secured ant routing algorithm for wireless sensor networks,” *International Journal of Network Security*, vol. 16, no. 2, pp. 149–156, 2014.

[16] D. Kar, R. Tatum, and K. Zejdlik, “MHIP: Effective key management for mobile heterogeneous sensor networks,” *International Journal of Network Security*, vol. 15, no. 4, pp. 280–290, 2013.

[17] J. Kar, “Provably secure online/off-line identity-based signature scheme for wireless sensor network,” *International Journal of Network Security*, vol. 16, no. 1, pp. 29–39, 2014.

[18] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[19] V. Katiyar, N. Chand, and N. Chand, “Recent advances and future trends in wireless sensor networks,” *International Journal of Applied Engineering Research*, vol. 1, no. 3, pp. 330–342, 2010.

[20] W. Z. Khan, M. Y. Aalsalem, M. N. B. M. Saad, and Y. Xiang, “Detection and mitigation of node replication attacks in wireless sensor networks: A survey,” *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1–22, 2013.

[21] S. S. Koshy and M. Sajitha, “Zone based node replica detection in wireless sensor network using trust,” *International Journal of Computer Trends and Technology*, vol. 4, no. 7, pp. 2316–2320, 2013.

[22] N. Kumar, M. Kumar, and R. B. Patel, “A secure and energy efficient data dissemination protocol for wireless sensor networks,” *International Journal of Network Security*, vol. 15, no. 6, pp. 490–500, 2013.

[23] T. Landstra, S. Jagannathan, and M. Zawodniok, “Energy-efficient hybrid key management protocol for wireless sensor networks,” *International Journal of Network Security*, vol. 9, no. 2, pp. 121–134, 2009.

[24] C. T. Li and M. S. Hwang, “A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks,” *Information Sciences*, vol. 181, no. 23, pp. 5333–5347, 2011.

[25] C. T. Li, M. S. Hwang, and Y. P. Chu, “Improving the security of a secure anonymous routing protocol with authenticated key exchange for ad hoc networks,” *International Journal of Computer Systems Science and Engineering*, vol. 23, no. 3, pp. 227–234, 2008.

[26] C. T. Li, M. S. Hwang, and Y. P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,” *Computer Communications*, vol. 31, no. 12, pp. 2803–2814, 2008.

[27] C. T. Li, M. S. Hwang, and Y. P. Chu, “An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks,” *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107–2124, 2009.

[28] Z. Li and G. Gong, “Randomly directed exploration: an efficient node clone detection protocol in wireless sensor networks,” in *Proceedings of the 6th IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS 09)*, pp. 1030–1035, 2009.

[29] A. K. Mishra and A. K. Turuk, “A zone-based node replica detection scheme for wireless sensor networks,” *Wireless personal communications*, vol. 69, no. 2, pp. 601–621, 2013.

[30] A. Mohaisen, D. Nyang, and K. Lee, “Hierarchical grid-based pairwise key pre-distribution in wireless sensor networks,” *International Journal of Network Security*, vol. 8, no. 3, pp. 282–292, 2009.

[31] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in *Proceedings of the IEEE Symposiumon Security and Privacy (IEEE S and P’05)*, pp. 267–281, 2005.

[32] H. K. D. Sarma and A. Kar, “Security threats in wireless sensor networks,” in *Proceedings 2006 40th Annual IEEE International, Carnahan Conferences Security Technology*, pp. 243–251, 2006.

[33] A. Singla and R. Sachdeva, “Review on security issues and attacks in wireless sensor networks,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 4, pp. 529–534, 2013.

[34] H. S. Soliman and M. Omari, “Application of synchronous dynamic encryption system (sdes) in wireless sensor networks,” *International Journal of Network Security*, vol. 3, no. 2, pp. 160–171, 2006.

[35] L. M. Wang, J. F. Ma, and Y. B. Guo, “Node-failure tolerance of topology in wireless sensor networks,” *International Journal of Network Security*, vol. 7, no. 2, pp. 261–264, 2008.

[36] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, “Real-time detection of clone attacks in wireless sensor networks,” in *Proceedings of the 28th international conference on distributed computing systems(ICDCS08)*, pp. 3–10, 2008.

[37] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, “Memory efficient protocols for detecting node replication attacks in wireless sensor networks,” in *Pro-*

ceedings of the 17th IEEE International Conference on Network Protocols (ICNP 09), pp. 284–293, 2009.

[38] B. Zhou, S. Li, J. Wang, S. Yang, and J. Dai, "A pairwise key establishment scheme for multiple deployment sensor networks," *International Journal of Network Security*, vol. 16, no. 3, pp. 221–228, 2014.

[39] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–1034, 2012.

Wei-Teng Li received his B. M. in Management Information Systems from National Chung Hsing University, Taichung, Taiwan, ROC, in 2012. He is currently pursuing the M.S. degree with the Department of Management Information Systems from National Chung Hsing University. His research interests include information security, wireless sensor network, and cryptography.

Tung-Huang Feng received his M.S. in Information Management from Chao-Yang University of Technology, Taichung, Taiwan, ROC, in 2002. He is currently pursuing the Ph.D. degree from Computer Science & Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and Sensor Networks.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China (ROC), in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999-2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002-2003. He is currently a professor of the department of Management Information System, National Chung Hsing University, Taiwan, ROC. He obtained 1997, 1998, 1999, 2000, and 2001 Outstanding Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang had published 170+ articles on the above research fields in international journals.