Group Rekeying in Wireless Sensor Networks: A Survey

Wei Teng Li[1], Chung-Huei Ling[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 Paper)

Abstract

Wireless sensor networks (WSNs) consist of many small sensor nodes and are commonly used to collect data and monitor hostile environments. Due to the factor of the cost, sensor nodes are lack of tamper-resistance and are deployed in unattended environments. Sensor nodes are easily captured by an intruder and compromised. An intruder will extract the secret elements in the sensor nodes including the group key. If an intruder knows the group key, he can use the group key to break down the wireless sensor network. To prevent a malicious intruder from knowing the group keys, the group keys should be updated for a period of time. In this paper, we focus on one of the distributed group rekeying called deterministic sequence-number-based group rekeying schemes and highlight the prone and cons of previous researches. According to recent studies it show the fact that there still many challenges exist in the group rekeying schemes.

Keywords: group rekeying, wireless sensor network, security

1 Introduction

Wireless sensor networks (WSNs) are commonly used to collect data and monitor hostile environment such as battlefield, pollution detection, environment monitor and health care [14], which consist of many small sensor nodes. These sensor nodes are composed of sensing unit, processing unit, transceiver, communication and power [2, 27], which are used for collecting data and transmitting data in an area. Then sensor nodes will transmit the data to the base station, regarded as a powerful data center that use these data to analyze, maintain and make decision.

Due to the factor of the cost, sensor nodes are lack of tamper-resistance and deployed in unattended environment [4, 28]. Hence, there are lots of malicious attacks in the vulnerable wireless sensor networks such as jamming, physical attack, black holes and Sybil attack [1, 13, 22, 25, 27]. Sensor nodes are easily captured by an intruder and compromised. An intruder will extract the secret elements in the sensor nodes including the group key used to encrypt the secret data and insert the secret elements in the intruder's malicious sensor nodes. Then an intruder deploys his malicious sensor nodes in the network and uses the group key to break down the wireless sensor network by injecting false report that makes a server not respond the real report immediately or eavesdrop the communication of other sensors [15, 16, 17, 18].

To prevent a malicious intruder from knowing the group keys, the group keys should be updated for a period of time. If the group keys are not updated, the intruder will compromise many sensor nodes and collect their group keys. An intruder can use these group keys to inject the false report to make a server misjudge and disturb the network. Hence, group rekeying mechanism is necessary to protect the wireless sensor network from the intruder. Group rekeying mechanism means there were several compromised nodes in the network server, it would execute group rekeying scheme to update all the member's group key to prevent attacks.

Existing group rekeying schemes are classified into two categories: *centralized schemes* [12, 23, 24, 30, 31, 32] and *distributed schemes* [10, 29, 35, 38, 39].

1) Centralized Group Rekeying Scheme: Centralized schemes need a single central controller which is always a base station or a trusted third party. A single central controller is regarded as a power center and cannot be compromised by an intruder. The central controller is responsible for managing the key materials and group rekeying mechanism on the network's nodes. According to the network structures, centralized group rekeying schemes are classified into three categories: flat [24, 32], hierarchical [23, 31] and heterogeneous [12, 30] network bases. However, centralized group rekeying scheme suffers several drawbacks [3]. The base station or the trusted third party easily suffers from a single point of failure. Nodes closest to the base station will become the target of the intruder and receive the huge traffic. A single central controller will delay the group rekeying mechanism because the messages need to be broadcasted to the whole network to reach the destination nodes [33].

2) Distributed Group Rekeying Scheme: In distributed group rekeying schemes, they do not need a central key controller. They have multiple key controllers and the multiple key controllers can be pre-assigned or dynamically assigned. Distributed group rekey schemes can be also classified into three categories: EBS-based [29, 35], polynomial-based [10, 38] and deterministic sequence-number-based [39]. The distributed schemes would not fall into a single point of failure. The group rekeying phase is much faster than centralized schemes because the messages only need to broadcast in a few hops to the destination nodes [33]. And it is more easily to expand the network size. However, the distributed schemes suffer the design errors because the compromised nodes will join in the node revocation process. In this paper, we focus on one of the distributed group rekeying called deterministic sequence-number-based group rekeying schemes and highlight the prone and cons of previous researches.

The Exclusion Basis System (EBS) [8] was proposed by Eltoweissy et al. in 2004. The EBS is based on a combinatorial formulation of the group multicast key management problem which provides a general framework for the key management systems. In ESB-based scheme. Nodes are assigned with several keys from a global key pool. And the group rekeying mechanism is executed from periodical time, or it is executed when certain number of nodes are compromised. In the group rekeying phase, the temporary keys are create. Therefore, these temporary keys encrypted with all the new group key are sent to the nodes which are not compromised by the intruder. The ESB-based schemes can be found in [7, 8, 9, 21, 29, 35].

The Polynomial-based schemes hide the new group key in a polynomial. When the compromised nodes are detected, the network will do the group rekeying process. The new calculated polynomial will broadcast to the whole wireless sensor network. The new polynomial is constructed by the secret element of the nodes which are not compromised and the new group key. All nodes receive the new polynomial and put their secret elements in the new polynomial. If the nodes are legitimate, they will get the new group key from the polynomial. Otherwise, the compromised nodes cannot derive the new group key from the polynomial. The Polynomial-based schemes can be found in [5, 10, 37, 38].

In this paper, we survey the previous researches of deterministic sequence-number-based group rekeying schemes on wireless sensor networks. Our purpose is to analyze the previous researches focused on their strengths and weaknesses. Finally, we proposed the future work about the group rekeying scheme.

The rest of paper is assigned as follows: Section 2, we classify the basic requirements of security and efficiency used to analyze previous researches. Section 3, we discuss the existing schemes of deterministic sequence-number-based group rekeying in detail. Section 4, we analyze previous researches and demonstrate their pros and cons.Finally, we summarize and discuss the future work of group rekeying schemes in wireless sensor networks in Section 5.

2 Basic Requirements and Evaluation Metrics

According to [11, 20, 26, 34] in survey papers, we focused on the security and efficiency of group rekeying schemes to sort out their basic requirements. We classified these requirements into two categories: security metrics and efficiency metrics. We discuss as follows. Then we use these requirements to analyze the existing schemes in Section 4.

2.1 Security Metrics

Group rekeying schemes have to ensure the network security. When detecting malicious nodes in the network, the group rekeying phase must be executed and the compromised nodes must be revoked. The new group key must keep in secret and the compromised nodes cannot use the old group key to derive the current new group key. Hence, a secure group rekeying scheme has to revoke the malicious nodes immediately when they are detected. The group key has to ensure both forward and backward secrecy and collusion resistance. In addition, resilience is a guide to see if the group rekeying scheme is efficiency or not.

1) Node Revocation: Once an intruder deploys his malicious sensor nodes in the network and tries to use the group key to break down the network, a secure solution should detect the malicious sensor nodes immediately and revoke them from the network. A effective scheme is good to protect the network from suffering the compromised nodes interference by injecting false report that makes a server not respond the real report immediately or eavesdrop the communication of other sensors.

2) Forward and Backward Secrecy: Forward secrecy means even if an intruder extracts the old group key from a legitimate sensor node, he cannot use the old group key to decrypt new messages. Backward secrecy ensures that a compromised node knows a current new group key cannot go backward to disclose the previous encrypted messages. Both forward and

Table 1: Notations for deterministic sequence-number-based group rekeying scheme

BS	Base station
CH	Cluster head
ID_α	Node α's identity
$f(\cdot)$	Pseudo-random function
$E_k(M)$	Encrypt message M with key k
R_B	A random number generated by base station
R_α	A random number generated by node α
$H(\cdot)$	A one-way hash function
$MAC_k(M)$	Message authentication code of message M using a symmetric key k
T_L	Life time of pairwise key or group key
N	Group size
d	number of member nodes

backward secrecy are important to prevent node capture attacks.

3) Collusion Resistance: An intruder might capture numbers of sensor nodes in the network. He can extract a number of group keys in the same time. And the intruder deploys his malicious sensor nodes in the network. Collusion resistance means an intruder cannot use these compromised nodes collaboratively to disclose all the current group key. A secure scheme must withstand the collaboration of compromised nodes attack.

4) Resilience: Resilience is used to describe the whole network. An intruder can compromise a number of sensor nodes in the wireless sensor network. If resilience is weak, just a few compromised nodes will lead to the whole network breaking down. On the other hand, if resilience is high, the network can tolerate a large number of compromised nodes in the network and not to affect the function of wireless sensor networks.

2.2 Efficiency Metrics

Saving energy resources and storage are an important task in wireless sensor networks. Because the limited resources are precious in the network. All overheads must be overall reduced, such as the cryptographic keys, operations and computational complexity. The group rekeying schemes should be as lightweight as possible.

1) Memory: Sensor nodes typically do not contain sufficient storage and use the memory to store secret elements such as identity of itself, public and private key, group key, pairwise key, identity of its neighboring and certificate. Due to the resource-starved sensors, the storage of sensors should be as low as possible.

2) Energy: Limited energy is a problem in wireless sensor networks. It is generally considered that data transmission and data reception are the most energy consumption operations [19]. However, the energy consumption are also involved in the group rekeying process. If the operation of generating new group keys is too complex, it will waste too much energy in nodes. Hence, saving energy is one of the most important tasks in WSNs.

3 Deterministic Sequence-number-based Group Rekeying Scheme

In this section, we review the deterministic sequence-number-based group rekeying scheme for WSNs. We survey several previous schemes and discuss the existing literatures in detail. We also highlight their contributions and analyze them in Section 4. In deterministic sequence-number-based group rekeying schemes, each node broadcast its randomly chosen number to its neighboring nodes, and uses the random number to establish the pairwise key between its neighbors. We will discuss the differences between the various schemes below and the notations for Deterministic sequence-number-based group rekeying schemes are summarized in Table 1.

3.1 LEAP Scheme

In the LEAP protocol proposed by Zhu et al. [39], the base station (BS) generates an initial key K_I in predeployment phase and inserts K_I in each node. A node α can derive its master key $K_\alpha = f_{K_I}(ID_\alpha)$. When the deploy phase is done, node α tries to find its neighbors. First, node α broadcasts ID_α to its neighbors and waits for its neighbors responding their identity. For example, as shown in Figure 1, when node α's neighboring node v received ID_α, node v respond its ID_v and $MAC_{K_v}(ID_\alpha|ID_v)$. Node α use initial key K_I to calculate $K_v = f_{K_I}(ID_v)$ and verify the identity of node v. Then, node α and v calculate their pairwise shared key in-

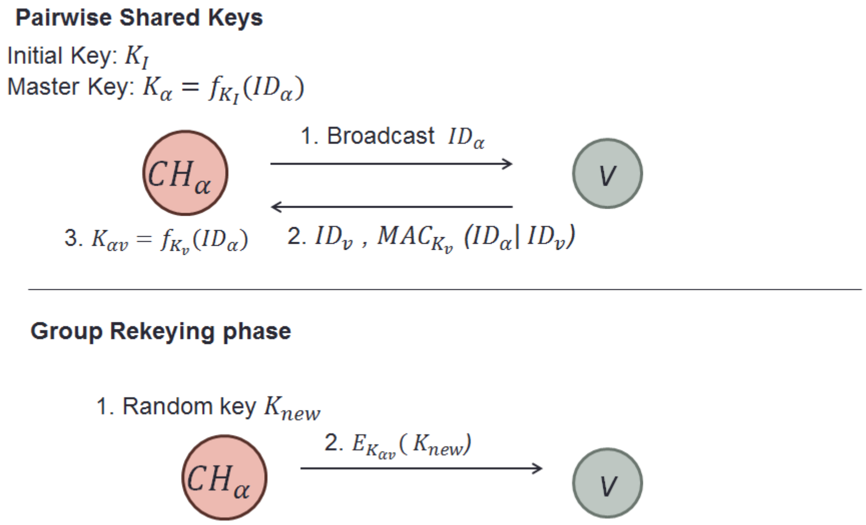
Pairwise Shared Keys
Initial Key: K_I
Master Key: $K_\alpha = f_{K_I}(ID_\alpha)$
CH_α
1. Broadcast ID_α
V
3. $K_{\alpha v} = f_{K_v}(ID_\alpha)$
2. ID_v , $MAC_{K_v}(ID_\alpha | ID_v)$
Group Rekeying phase
1. Random key K_{new}
CH_α
2. $E_{K_{\alpha v}}(K_{new})$
V

Figure 1: LEAP Scheme

dependently. Node α uses K_I to calculate $K_v = f_{K_I}(ID_v)$ and derives pairwise shared key $K_{\alpha v}$ by $K_{\alpha v} = f_{K_v}(ID_\alpha)$. Node v use the same way to calculate $K_{\alpha v}$.

In group rekeying phase, cluster head (CH_α) establishes the pairwise key among its member nodes before group rekeying phase. When all the member in the same group are establishing the pairwise key among the CH_α. Then CH_α randomly chooses new group key K_{new} and encrypts K_{new} with pair-wise key $E_{K_{\alpha v}}(K_{new})$ sending to its member nodes. However, this group rekeying scheme falls into two drawbacks [36]. First, the pairwise key always uses the same formula and the initial key K_I to compute. It makes a easy way for an intruder to get a pairwise key. If an intruder captures a sensor node, he would get K_I easily and use K_I, so all pairwise keys can be easily computed. Second, the above processes are not authenticated, an intruder can exhaust resource by injecting fake hello messages. In 2006, Zhu et al. proposed an improved scheme of the LEAP protocol, but that scheme did not solve these two problems [40].

3.2 OTMK Scheme

Deng et al. proposed OTMK scheme in 2005, which was used for improving the LEAP scheme [6]. In OTMK, sensor nodes are pre-assigned with a master key K_m. When a node α wants to establish pairwise keys to its neighboring nodes, as shown in Figure 2, it first broadcasts the encrypted $JOIN$ message $E_{K_m}(ID_\alpha||R_\alpha)$ using the master key K_m where R_α is a random number chosen by node α. Then its neighboring node v receives this decrypted this message and replies to node α. If both nodes, α and v, receive $JOIN$ message from each other,they will use their ID and a random number to establish their pairwise key, $K_{\alpha v} = f(ID_\alpha||ID_v||R_\alpha||R_v)$ when $ID_\alpha < ID_v$. Otherwise, $ID_\alpha > ID_v$ their pairwise key is $K_{v\alpha} = f(ID_v||ID_\alpha||R_v||R_\alpha)$. In OTMK, the group rekeying phase followed LEAP protocol. When a node is revoked, the CH generates a new group key K_{new} and encrypts K_{new} with their pairwise key.

However, OTMK uses the master key K_m to encrypt the $JOIN$ message, which is similar to initial key K_I in LEAP protocol. If an intruder knows K_m, he can easily break down the network by deploying his malicious nodes. Because the function $f(\cdot)$ is public known to everyone. Hence, an intruder can eavesdrop the encrypt $JOIN$ message between two nodes and get the (R, ID). Then he can use the leaking information to compute all the pairwise keys in the network. Therefore, he can disturb the WSNs by injecting a false report, forging or overhearing.

3.3 LEAP$^+$ Scheme

In 2006, Zhu et al. proposed an improved scheme of the LEAP protocol named LEAP$^+$ [40]. LEAP falls into two drawbacks. First, the pairwise key always uses the same formula and the initial key K_I to compute. Second, the above processes are not authenticated. To prevent an intruder form capturing sensor nodes in the network and easily knowing the initial key K_I, LEAP$^+$ let the base station randomly generate i keys: $K_I^1, K_I^2, \cdots, K_I^i$. These keys are initial keys for different life time intervals. The life time of wireless sensor network is divided into different intervals. Each interval has its own initial key. For example, as shown in Table 2, $T_1, T_2, \cdots, T_i$ have their own initial keys $K_I^1, K_I^2, \cdots, K_I^i$.

Table 2: Initial keys for different life time intervals

T_1	T_2	$\cdots$	T_{i-1}	T_i
K_I^1	K_I^2	$\cdots$	K_I^{i-1}	K_I^i

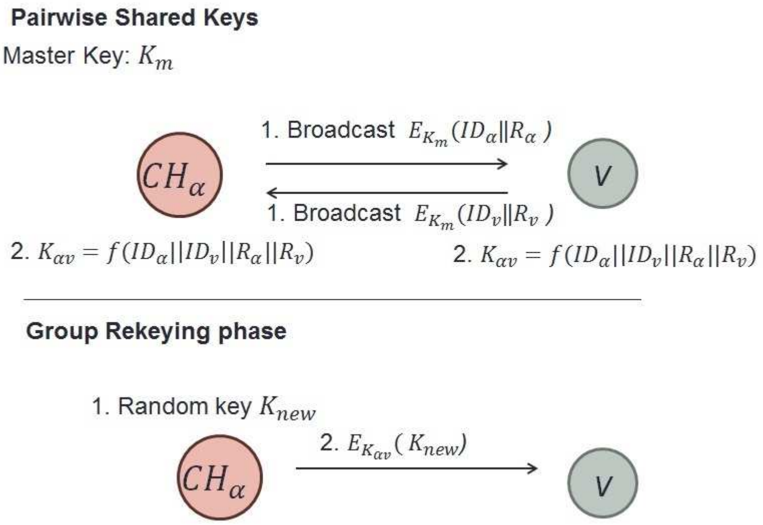
Pairwise Shared Keys
Master Key: K_m
1. Broadcast $E_{K_m}(ID_\alpha||R_\alpha)$
CH_α
V
1. Broadcast $E_{K_m}(ID_v||R_v)$
2. $K_{\alpha v} = f(ID_\alpha||ID_v||R_\alpha||R_v)$
2. $K_{\alpha v} = f(ID_\alpha||ID_v||R_\alpha||R_v)$
Group Rekeying phase
1. Random key K_{new}
2. $E_{K_{\alpha v}}(K_{new})$
CH_α
V

Figure 2: OTMK Scheme

When the nodes are deployed in the networks, a node α tries to find out its neighboring nodes. As shown in Figure 3, first, node α broadcasts a $HELLO$ message which contains ID_α and the interval i. The neighboring nodes use K_I^i to compute the current master key $K_v^i = f_{K_I^i}(ID_v)$. Then node v responds its ID_v and $MAC_{K_v^i}(ID_\alpha|ID_v)$. Node α also knows the initial key K_I^i, it can compute K_v^i by using ID_v to verify the $MAC_{K_v^i}$.

The group rekeying phase is processed as same as LEAP protocol. To establish the group key, it follows the pairwise key phase. A CH_α wants to share the a unique key called group key with all its member. First, a CH_α randomly generates a new group key K_{new} sent to the member $v^1, v^2, \cdots, v^i$ in the its group. Then it encrypts the new group key using their pairwise keys $E_{K_{\alpha v_i}}(K_{new})$. LEAP$^+$ protects the initial key K_I easily by intruders. But the first step to finding neighboring nodes in the network is not authenticated. An intruder can inject fake $HELLO$ messages to exhaust the resource of sensor nodes and delay the real situation in WSNs.

3.4 EDDK Scheme

Zhang et al. proposed an energy-efficient distributed deterministic key management scheme (EDDK) in 2011 [36], which was proposed to solve resource exhausting attacks and DoS attacks in OTMK [6]. In EDDK scheme, each node is preloaded with a pseudo-random function $f(\cdot)$, initial key K_I, and local group key K_G is used to communicate with all its member nodes. Each node needs to store the pairwise keys, a neighboring table and the random number. Like LEAP, every node can use the pseudo-random function $f(\cdot)$ and initial key K_I to compute its individual key. For example, node α's individual key can be derived as $K_\alpha = f_{K_I}(ID_\alpha)$.

In the pairwise key establishment phase, as shown in Figure 4, a node α first computes its individual key K_α, generates a random sequence number R_α and broadcasts the $JOIN$ message to its neighboring nodes. $JOIN$ message contains $ID_\alpha||E_{K_\alpha}(R_\alpha||K_G)||MAC_{K_\alpha}(ID_\alpha||E_{K_\alpha}(R_\alpha||K_G))$. When both nodes, α and v receive the $JOIN$ message from each other, they will verify the correctness of the $JOIN$ message. After verifying the pairwise keys are generated: $K_{\alpha v} = f(K_\alpha \oplus K_v, R_\alpha \oplus R_v)$.

To prevent an intruder from compromising a number of sensor nodes in the network, both pairwise key and group key have to rekey periodically. When an intruder captures a large number of sensors and tries to break down the network, the rekeying phase will be started. In EDDK, the smallest ID will do the rekeying procedure which is similar to OTMK. For instance, if $ID_\alpha < ID_v$, node α will do the rekeying procedure. Node α will unicast node v pairwise rekeying message which contains ID_α || ID_v || T_L || $E_{K_{\alpha v}^{old}}(K_{\alpha v}^{new})||MAC_{K_{\alpha v}^{old}}(ID_\alpha||ID_v||T_L||E_{K_{\alpha v}^{old}}(K_{\alpha v}^{new}))$. When node v receives the message and uses the old pairwise key to authenticate and get the new pairwise key. Then node v will send back the acknowledgement $ID_\alpha||ID_v||T_L + 1||MAK_{K_{\alpha v}^{new}}(ID_\alpha||ID_v||T_L + 1)$. The group rekeying phase is the same as pairwise rekeying phase. The CH_α will generate a new group key K_G^{new} and broadcast to all its member ID_α || T_L || $E_{K_G^{old}}(K_G^{new})$ || $MAC_{K_G^{old}}(ID_\alpha$ || T_L || $E_{K_G^{old}}(K_G^{new}))$.

Although, EDDK can prevent replay attacks, Sybil attacks and node replication attacks, an intruder does not have enough information such as neighboring table, random sequence number and pairwise key to decrypt and authenticate the message. EDDK is not suitable for large wireless sensor networks specifically for those sensor nodes which have many neighboring nodes.

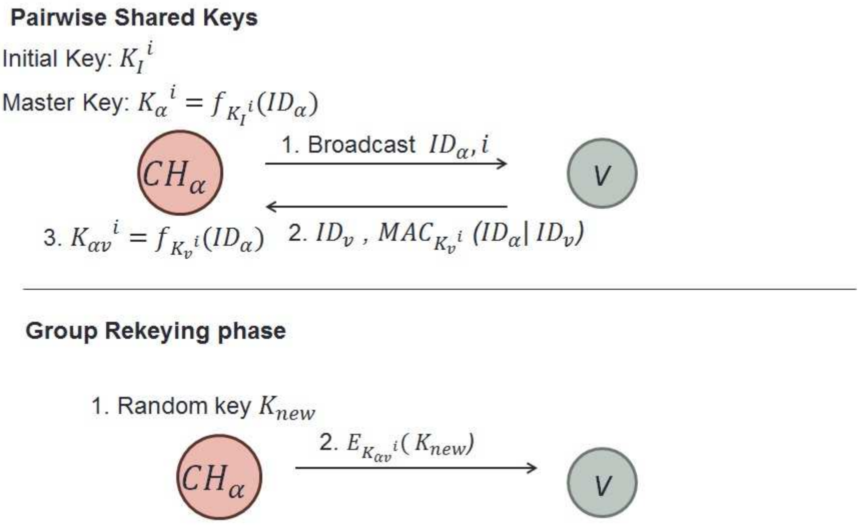
Pairwise Shared Keys
Initial Key: $K_I{}^i$
Master Key: $K_\alpha{}^i = f_{K_I{}^i}(ID_\alpha)$
CH_α
1. Broadcast ID_α, i
V
3. $K_{\alpha v}{}^i = f_{K_v{}^i}(ID_\alpha)$
2. ID_v , $MAC_{K_v{}^i}(ID_\alpha | ID_v)$
Group Rekeying phase
1. Random key K_{new}
2. $E_{K_{\alpha v}{}^i}(K_{new})$
CH_α
V

Figure 3: LEAP$^+$ Scheme

4 Discussions

In this section, we organize advantages and disadvantages of the above related papers in Table 2. We also from the perspective of security and efficiency analyze the above literatures. In Section 2, we focus on the group rekeying scheme to summarize the basic requirements and evaluation metrics. Then we use these basic requirements to discuss the recent studies. Recent studies indicate that there are still many challenges existing in group rekeying schemes.

4.1 Security and Performance Analysis

We summarize the basic security merits in four requirements and analyze the above related works in Table 3. In resilience, “High” means the compromised nodes cannot affect the network despite having a number of compromised nodes in the network, which cannot break down the whole network. “Medium” means the compromised nodes affect less non-compromised nodes. “Low” means the compromised nodes lead to break down the network. We also list the communication and storage overhead in Table 4.

5 Future Research and Conclusions

In the deterministic sequence-number-based group rekeying scheme, the security of group rekeying phase is based on a secured establishing pairwise key in the wireless sensor networks. According to the above literatures, before the group rekeying phase, to establish a secure pairwise key is crucial. A secure pairwise wise key can protect the safety of the new group key to transfer to its member nodes. The future work of deterministic sequence-number-based group rekeying schemes still has a task in establishing a secure pairwise key and need to be designed for resource-constrained situations in WSNs. Not only the group keys need to be updated, but also the pairwise keys have to be done. It also can use an efficient detection of the node replication protocol [20]to detect the compromised nodes in the WSNs first, and it then execute the group rekeying schemes to update the old group key. Combining these two protocols can be implemented in a real WSNs situation. For example, we can implement in a hostile environments such as battlefield, pollution detection, environment monitor and health care.

In recent years, wireless sensor networks have been widely used in many fields. In our survey papers,we focus on one of the distributed group rekeying called deterministic sequence-number-based group rekeying schemes and discuss the related works in detail. We also highlight the prone and cons of previous researches and propose the future work about the group rekeying scheme. According to recent studies, it shows that there are still many challenges existing in group rekeying schemes.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 102-2811-E-468 -001, 103-2622-E-468 -001 -CC2, and 103-2622-H-468 -001 -CC2. The authors gratefully acknowledge the anonymous reviewers for their valuable 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.

Table 3: Summary of scheme

Schemes	Advantage	Disadvantage
LEAP [39]	1. Efficient computation 2. Lower memory usage	1. Resource exhausting attack 2. Reveal initial key 3. No authenticate message
OTMK [6]	1. resilience 2. Improve secured	1. Resource exhausting attack 2. Reveal initial key 3. DoS attack
LEAP$^+$ [40]	1. More resilience 2. Dynamic initial key	1. Resource exhausting attack 2. Higher communication cost 3. No authenticate message
EDDK [36]	1. Authenticate message 2. Prevent replay attack 3. Prevent sybil attack 4. Prevent node replication attack	1. Higher memory usage 2. Not suitable for large-scale WSNs

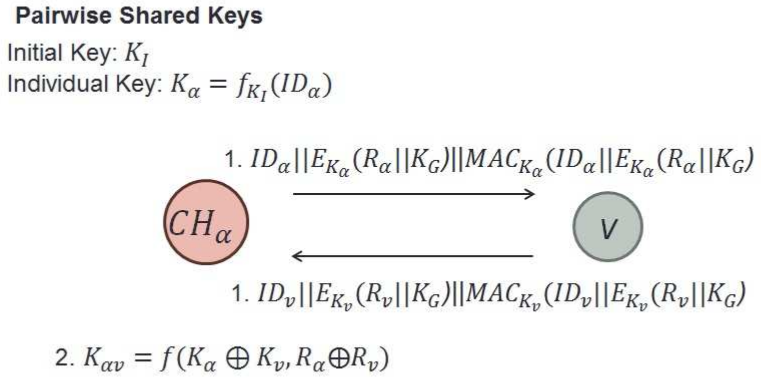
Pairwise Shared Keys
Initial Key: K_I
Individual Key: $K_\alpha = f_{K_I}(ID_\alpha)$
1. $ID_\alpha||E_{K_\alpha}(R_\alpha||K_G)||MAC_{K_\alpha}(ID_\alpha||E_{K_\alpha}(R_\alpha||K_G)$
CH_α
V
1. $ID_v||E_{K_v}(R_v||K_G)||MAC_{K_v}(ID_v||E_{K_v}(R_v||K_G)$
2. $K_{\alpha v} = f(K_\alpha \oplus K_v, R_\alpha \oplus R_v)$

Figure 4: EDDK Scheme

Table 4: Summary of scheme security

Schemes	Node revocation	Collusion resistance	Resilience	Lightweight
LEAP [39]	Yes	No	No	Low
OTMK [6]	Yes	No	No	Medium
LEAP$^+$ [40]	Yes	Both	Yes	Medium
EDDK [36]	Yes	Both	Yes	High

Table 5: Summary of scheme costs

Schemes	Communication	Storage
LEAP [39]	$O(N)$	$O(d)$
OTMK [6]	$O(N^2)$	$O(d)$
LEAP$^+$ [40]	$O(N)$	$O(d)$
EDDK [36]	$O(N\sqrt{N})$	$O(d^2)$

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

[3] A. Perrig B. Parno and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proceedings of the IEEE Symposiumon Security and Privacy*, pp. 267–281, 2005.

[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] A. Chadha, Y. Liu, and S. K. Das, "Group key distribution via local collaboration in wireless sensor networks," in *Proceedings of the IEEE Conference on Communications Society*, pp. 46–54, 2005.

[6] J. Deng, C. Hartung, R. Han, and S. Mishra, "A practical study of transitory master key establishment for wireless sensor networks," in *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05)*, pp. 289–299, 2005.

[7] R. Divya and T. Thirumurugan, "A novel dynamic key management scheme based on hamming distance for wireless sensor networks," *International Journal of Scientific and Engineering Research*, vol. 2, pp. 1–12, 2011.

[8] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial optimization of group key management," *Journal of Network and Systems Management*, vol. 12, no. 1, pp. 33–50, 2004.

[9] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, 2006.

[10] S. Guo and V. Leung, "A secure and scalable rekeying mechanism for hierarchical wireless sensor networks," *IEICE Transactions on Information and Systems*, vol. E93D, no. 3, pp. 421–429, 2010.

[11] X. He, M. Niedermeier, and H. de Meer, "Dynamic key management in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 611–622, 2013.

[12] J. Y. Huang, I. E. Liao, and H. W. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 6, pp. 1–10, 2011.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] J. Li and J. Li, "Data sampling control and compression in sensor networks," *Mobile Ad-hoc and Sensor Networks*, vol. 3794, pp. 42–51, 2005.

[20] W. T. Li, T. H. Feng, and M. S. Hwang, "Distributed detecting node replication attacks in wireless sensor networks: A survey," *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.

[21] C. C. Lo, C. C. Huang, and S. W. Chen, "An efficient and scalable EBS-based batch rekeying scheme for secure group communications," *IEEE Military Communications Conference (MILCOM 2009)*, pp. 1–7, 2009.

[22] Pooja Manisha and Yudhvir Singh, "Security issues and sybil attack in wireless sensor networks," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 1, pp. 7–13, 2013.

[23] M.-L. Messai, M. Aliouat, and H. Seba, "Tree based protocol for key management in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, no. 59, pp. 1–10, 2010.

[24] K. J. PAEK, U. S. SONG, H. Y. KIM, J. KIM, and J. N. Hwang, "Energy efficient key management (EEKM) protocol for large scale distributed sensor networks," *Journal of Information Science and Engineering*, vol. 24, no. 6, pp. 1837–1858, 2008.

[25] 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.

[26] M. A. Jr. Simplicio, P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Computer Networks*, vol. 54, no. 15, pp. 2591–2612, 2010.

[27] 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.

[28] 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.

[29] M. K. R. R. Syed, H. Lee, S. Lee, and Y. K. Lee, "Muqami+: a scalable and locally distributed key management scheme for clustered sensor networks," *Annuals of Telecommunications*, vol. 65, no. 1-2, pp. 101–116, 2010.

[30] C. L. Wang, T. P. Hong, G. Horng, and W. H. Wang, "A ga-based key-management scheme in hierarchical wireless sensor networks," *International Journal of Innovative. Computing, Information and Control*, vol. 5, pp. 4693–4702, 2009.

[31] G. Wang, S. Kim, D. Kang, and D. Choi, "Lightweight key renewals for cluster sensor networks," *Journal of Networks*, vol. 5, no. 3, pp. 300–312, 2010.

[32] Y. Wang, B. Ramamurthy, and Y. Xue, "A key management protocol for wireless sensor networks with multiple base stations," in *Proceeding of IEEE International Conference on Communications*, 2008.

[33] Y. Wang, B. Ramamurthy, X. Zou, and Y. Xue, "An efficient scheme for removing compromised sensor nodes from wireless sensor networks," *Security and Communication Networks*, vol. 3, no. 4, pp. 320–333, 2010.

[34] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Computer Communications*, vol. 30, no. 11, pp. 2314–2341, 2007.

[35] M. Younis, K. Ghumman, and M. Eltoweissy, "Location-aware combinatorial key management scheme for clustered sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006.

[36] X. Zhang, J. He, and Q. Wei, "EDDK: energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011:765143 doi:10.1155/2011/765143, 2011.

[37] Y. Zhang, C. Wu, J. Cao, and X. Li, "A secret sharing-based key management in hierarchical wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 2013, pp. 1–7, 2013.

[38] W. Zhanga, S. Zhub, and G. Caob, "Predistribution and local collaboration-based group rekeying for wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1229–1242, 2009.

[39] S. Zhu, S. Setia, and S. Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03)*, pp. 62–72, 2003.

[40] S. Zhu, S. Setia, and S. Jajodia, "Leap+: efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500–528, 2006.

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.

Chung-Huei Ling received his M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California, USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and radio frequency identification.

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.