

A Misused Key Detection Mechanism Using the Token in Wireless Sensor Networks

Dong-Min Kang*, Min-woo Park*, Young-Ju Han*, Seon-Ho Park* and Tai-Myoung Chung**

Internet Management Technology Laboratory,

**Dept. of Electrical and Computer Engineering, Sungkyunkwan University,*

***School of Information and Communication Engineering, Sungkyunkwan University,*

300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Republic of Korea

{dmkang, mwpark, yjhan and shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract— In Wireless Sensor Networks, key management is required to offer a secure communication between sensor nodes. Many key management mechanisms have been proposed while considering the characteristics of sensor nodes. Despite the advances of key management techniques, wireless sensor networks still have vulnerable point since sensor nodes have the communication restrictions such as an ultralight, a low power and a short distance. Therefore an adversary can compromise easily a few sensor nodes and may obtain keys between non-compromised nodes. By using obtained keys, the adversary can insert forged or modified messages. The abused key by adversary is called “misused key”. In wireless sensor network, the misused key can cause mortal consequences to user. This paper introduces a misused key detection mechanism of Liu and Dong and proposes efficient and secure misused key detection mechanism in wireless sensor networks. Additionally, in our simulation result, the energy consumption of our scheme is 20% more efficient than that of the Liu and Dong’s scheme on the average.

Keywords— Sensor networks, Misused key, Security, Token, Energy consumption;

I. INTRODUCTION

Wireless sensor networks consist of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate in short distances through wireless links. Recently, researchers are on progress of active research about wireless sensor networks. In the result, wireless sensor networks are applied into various fields of industry. Despite of these efforts, wireless sensor networks still have vulnerable point. To solve the problem, wireless sensor networks needs to security services. Key management is very necessary to achieve the security services. In wireless sensor networks, a key uses mainly a symmetric key method rather than a public key method due to feature of sensor nodes has restricted resource. However sensor nodes do not have a symmetric key corresponded with every others nodes. Thus wireless sensor networks use the probability key distribution

method. The probability key distribution method uses symmetric key method, each node share key with a few nodes not using unique key matching to individual node. If a sensor node and a communicating node share a key, then they communicate via that key, otherwise, they communicate via another node.

In wireless sensor networks using the probability key distribution method, adversary can compromise easily a few sensor nodes and may obtain keys between non-compromised nodes due to feature of sensor nodes. By using obtained keys, the adversary can insert forged or modified messages. The abused key by adversary is called as “misused key”. The misused key causes mortal consequences in wireless sensor networks.

In this paper, we propose token misused key detection scheme based on the Liu and Dong’s method.

The remainder of this paper is organized as follows. In the section 2, we will describe Liu and Dong’s misused key detection scheme. In the section 3, we will present our token misused key detection scheme. In the section 4, we will present energy efficiency and security evaluation of our scheme and Liu and Dong’s scheme. Finally, section 5 will present conclusion of our paper and discuss about future research.

II. RELATE WORKS – LIU AND DONG’S WORK

Liu and Dong proposed the mechanism for detecting the misused key among the non-compromised nodes in wireless sensor networks using a probability key distribution method. An adversary can compromise easily a few sensor nodes and may obtain keys between non-compromised nodes because the probability which another node has the keys, which non-compromised nodes have, exists according to a probability key distribution method. By using obtained keys, the adversary can insert forged or modified messages. The Base station can make wrong decisions due to forged or modified messages. To prevent these kinds of attacks, Liu and Dong suggested the

additional protection for non-compromised sensor nodes even if an adversary has stolen the shared keys between them.

A. Assumption

Before we explain the Liu and Dong's scheme, let me draw your attention to some assumptions of their scheme. These are following:

1. The sensor node u and the cluster head v are non-compromised nodes.
2. The detecting node i can have unique secret key shared by itself and each node.
3. Their scheme is used in environment that uses a probability key distribution scheme based on cluster.

B. Idea

The main idea of this scheme is the committing value (CV) and the secret key between a sensor node and the base station. The CV is used to detect the misused key about a one-way communication. Each sensor node u and the cluster head v keep a variable $C_{u,v}$ which is the cumulative hashed value of transferred messages from the sensor node u to the cluster head v . If $C_{u,v}$ of these nodes are identical, we can be convinced that messages transferred from the sensor node u to the cluster head v are not forged, modified or inserted. In this scheme, a node that compares $C_{u,v}$ to detect the misused key must receive securely $C_{u,v}$ of the sensor node u and the cluster head v without obstruction of an adversary. Therefore a verifying node which detects the misused key can be the base station that has unique keys with all of sensor nodes. However the base station will be burdened with heavy computation if only the base station detects the misused key of all nodes. To distribute overhead of the base station, they introduced the detecting sensor nodes. The detecting sensor nodes have shared pair-wise keys with every node, just like the base station.

C. Operation

Every sensor node u is pre-loaded with a unique and random key K_u . This key is only known by the base station and the sensor node u . Every detecting sensor node i stores a hash value $H(K_{u,i})$ for every sensor node u . After deployment, every sensor node u discovers neighbourhood and transfers messages to the cluster head v . Both sensor node u and cluster head v maintain the variable $C_{u,v}$ to track the history of the communication from the sensor node u to the cluster head v . For every new message M from the sensor node u to the cluster head v , these nodes update $C_{u,v} = H(C_{u,v} || M)$. And every sensor node u creates not only messages but also the V_1 and the V_2 . Each value makes the calculation as showed in figure 1.

$$\begin{aligned} V_1 &= H(C_{u,v} || H(K_u)) \\ V_2 &= H(C_{u,v} || K_u) \end{aligned}$$

Figure 1. Committing value of sensor node u

The V_1 will be used by the detecting node i to check the committing value, while V_2 will be used only when the detecting node i notices the misuse of the key and needs to revoke key to the base station. The detecting node i checks messages transferred from cluster head v on probability p . The cluster head v decides the value of Probability p . If $C_{u,v}$ of the sensor node u and the cluster head v are not same each other, it means that the $K_{u,v}$ was misused by the adversary. The detecting node i sends the reporting message to the base station when the detecting node i finds the misused key.

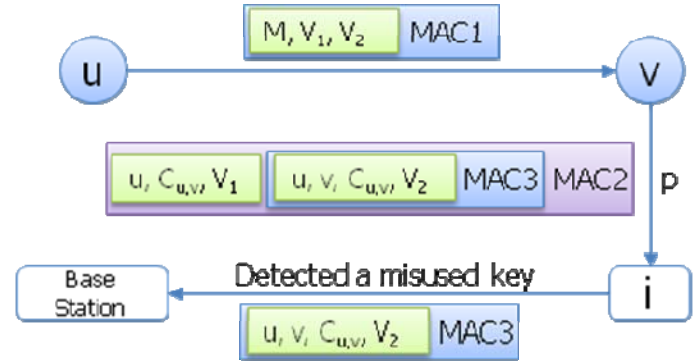


Figure 2. Operation of Liu and Dong's scheme

D. Limitation of the Liu and Dong's scheme

Let us consider limitation of the Liu and Dong's scheme from three perspectives.

1. The misused key detection is detected by comparing all $C_{u,v}$ of general sensor nodes and cluster head. When this method detects a misused key within one cluster, comparing $C_{u,v}$ of all nodes results in high energy consumption.
2. To detect the misused key, cluster head cumulates messages and $C_{u,v}$ of general sensor nodes. The aggregated message cannot be corrected due to wrong information by using a misused key. Thus the base station reported the wrong aggregated message cannot use the aggregated message.
3. If the base station wants to use sensing information of the sensor nodes without delay, it is impossible because the aggregated message cannot guarantee authenticity of data. Authenticity of data is always defined as perfect data that does not include wrong information.

III. PROPOSED SCHEME

In this section, we propose an energy-efficient method for detecting misused keys. We improved the Liu and Dong's scheme in the aspects of security and energy-efficiency. The key concept of our scheme is to use a token between the communicating nodes. The cluster head checks whether the communicating node is the compromised node by checking the

token. Therefore communicating nodes can communicate more secure.

The assumption of proposed scheme is same as the assumption of Liu and Dong's scheme.

A. The goal of the proposed scheme

To enhance a misused key detection mechanism, more energy efficient and secure mechanism is required in wireless sensor networks. Let us consider the goal of our scheme from three perspectives.

1. Energy efficiency: In wireless sensor network, to prolong lifetime of network is very important.. The high energy efficiency increases lifetime of network. Therefore the proposed scheme will decrease overhead and will increase energy efficiency by using the token.
2. Trustworthiness of the aggregated message: The Liu and Dong's scheme does not satisfy trustworthiness of the aggregated message due to incorrect information by using misused key. The proposed scheme will be satisfied with trustworthiness of the aggregated message by using the token.
3. QOS-delay: In the proposed scheme, the base station offers QOS that can use immediately the aggregated message.

B. Operation

The operation of our token misused key detection scheme is divided into three steps. Figure 3 illustrates it.

In the first step, the detecting node i generates tokens and transfers them to the cluster header v . The token values are generated randomly so that other node which is not a cluster header cannot predict the token values. Also the message M included tokens transfers by using the secret key shared between the detecting node i and the cluster header v because tokens should be protected.

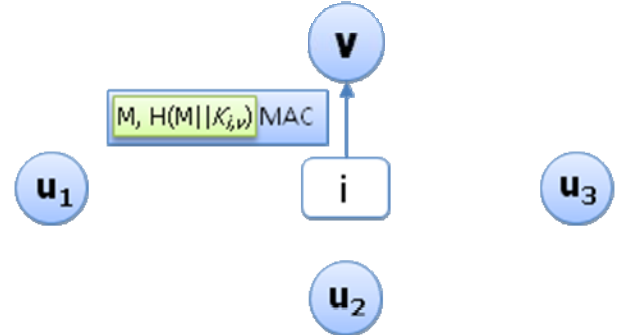
In the second step, the detecting node i transfers a token to each sensor nodes (u_1, u_2, u_3). The message M transferred by detecting node i is XOR value of token and hashed value $H(K_{u,i})$. Through XOR operation, the token is hidden against other nodes. The other nodes except the sensor node cannot find out $H(K_{u,i})$ because only the sensor node knows the token value and the other nodes do not know the token value.

In the third step, the sensor node u transfers message to the cluster head v . The message includes the message sensed by the sensor node u and $H(token||K_{u,v})$. The $K_{u,v}$ of communicating nodes can be exposed $K_{u,v}$ by the other nodes due to using probability key distribution mechanism. But other nodes cannot create message due to unknown token. Every time the sensor node u transfers message to cluster head, it calculates token value $+\alpha$. Thus other nodes cannot predict token value. Also sensor nodes can prevent replay attack. The cluster head v compares hash value of received message. If hashed value is not equivalent, key between the sensor node u and the sensor node v is the misused key. If the cluster head v detects the misused key, it cuts off message and reports to base station. After the preceding steps, the

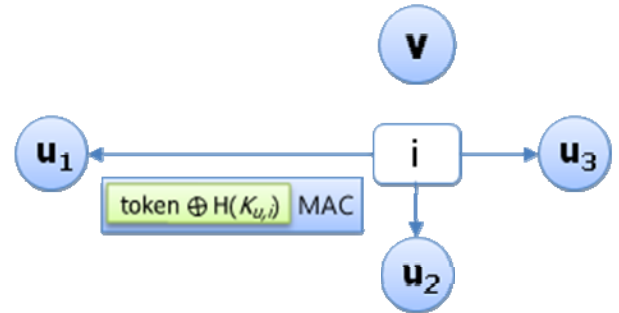
cluster head aggregates only verified messages and transfers aggregated message to base station.

The first and second step occurs during network deployment and the change of cluster head. The third step occurs when data transfers among communicating node.

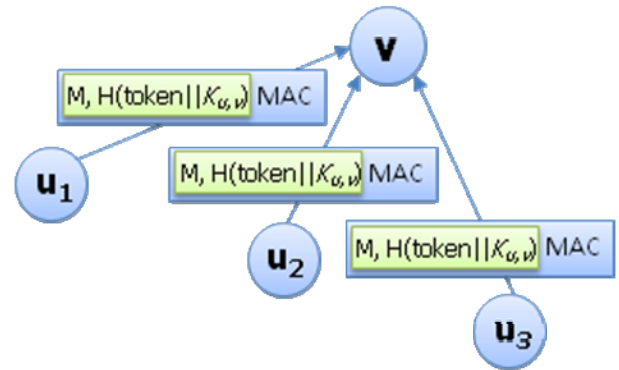
A proposed scheme does 100% misused detection frequency for assurance of data integrity. Thus this scheme reinforces security due to aggregating verified messages.



(a) Tokens generation and transmission of the detecting node i



(b) Tokens transmission of the detecting node i



(c) Data transmission of the sensor nodes

Figure 3. Operation of token misused key detection scheme

C. Scenario

In Figure 4, the sensor node u_1 is a non-compromised node and the sensor node u_2 is the compromised node by an adversary. So the adversary can know the shared key, $K_{u1,v}$,

between u_1 and v and the compromised node, u_2 , can impersonate u_1 . Finally, while the sensor node u_1 receives a token from detecting node i , the compromised node, u_2 , sends a message to cluster head v as u_1 .

But, since the sensor node u_2 does not know the token of the sensor node u_1 . The sensor node v detects misused key and cuts off message of the sensor node u_2 .

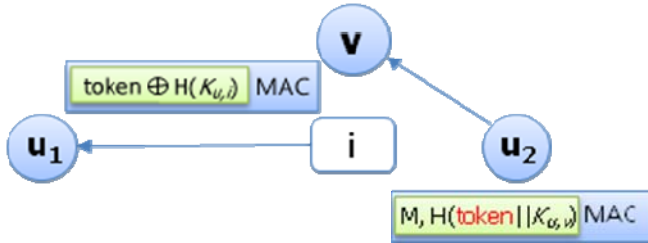


Figure 4. Example of misused key detection

IV. EVALUATION

In this section, we will compare the energy efficiency and security of our scheme with those of the Liu and Dong's scheme. For impartial evaluation, we compare the Liu and Dong's scheme with our scheme in same environment. MATLAB is used as the performance evaluation tool.

A. Energy efficiency

We simulated the energy efficiency performance by using the simulation parameters. The simulation parameters are showed in Table 1.

Table 1. Simulation parameters

Parameter	Value
E _{elec}	50 nJ
E _{fs}	10 pJ/bit/m ²
E _{mp}	0.0013 pJ/bit/m ⁴
Size of token	8 bytes
Size of token list	80 bytes
Size of message	80 bytes
Size of node ID	4 bytes
Size of MAC	8 bytes
Average of distance	6 m

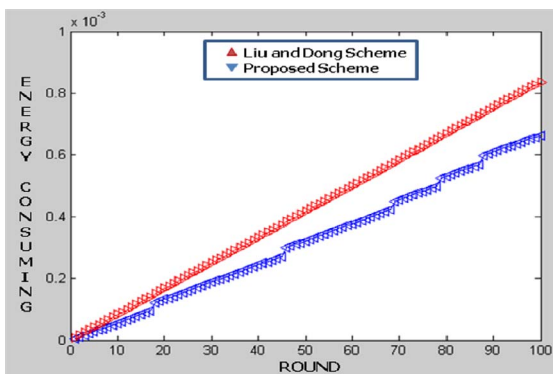


Figure 5. Energy consumption of the sensor nodes

The performance evaluation result shows that the proposed scheme consumes energy about 20% less than the Liu and Dong's scheme. It is because the overhead to detect the misused key is reduced by using the token. Figure 5 shows energy consumption of the sensor nodes.

B. Trustworthiness of the aggregated message

We simulated the trustworthiness of the aggregated message performance by using the simulation parameters. In the simulation, general sensor nodes transfer only message value 1 and compromised nodes transfer only message value 100. The simulation parameters are showed in Table 2.

Table 2. Simulation parameters

Parameter	Message Value
General node	1
Compromised node	100

In the simulation, probability of compromised nodes is 20% and compromised nodes transfer wrong messages continuously using misused key.

The performance evaluation result shows that by using the proposed scheme, the probability that the aggregated message does not contain the wrong messages using misused key was 100%. Also, by using the Liu and Dong's scheme, the probability that the aggregated message does contain the wrong messages using misused key was 100%. Figure 6 shows performance evaluation result of trustworthiness of the aggregated message.

Table 3. Performance evaluation result of trustworthiness of the aggregated message

	Message Value					
Proposed scheme	1	1	1	1	1	1
Liu and Dong's scheme	2377	1981	2179	2080	1783	2080

V. CONCLUSIONS

In this paper, we presented an efficient method for detecting misused keys in the wireless sensor networks. Let us explain the advantage of our scheme from three perspectives.

1. Energy efficiency: The our scheme uses token instead of $C_{u,v}$. In Liu and Dong's scheme, $C_{u,v}$ is very important factor to detect misused key. But the misused key detection method using $C_{u,v}$ high overhead. To solve overhead, our scheme is uses token.
2. Trustworthiness of the aggregated message: In our scheme, the aggregated message is trustworthiness. Because our scheme receives only verified messages. In other words, the incorrect messages using misused key of adversary are detected by the cluster head due to unknown token value and cluster head receives the correct messages. Therefore aggregated message can be trust.

3. QOS-delay: The base station can use immediately the aggregated message. Because the aggregated message can be trusted. Thus base station can offer data without delay to an application or a user. Therefore our scheme ensures QOS.

A further direction of this study will develop efficient mechanism for detect misused key. Also we will study misused key detection mechanism in wireless sensor networks using the group key.

REFERENCES

- [1] D. Liu and Q. Dong, "Detecting Misused Keys in Wireless Sensor Network", IPCCC2007, Apr. 2007.
- [2] D. M. Kang, M. W. Park, S. H. Park and T. M. Chung, "Misused Key Detection Mechanism in Wireless Sensor Network Using Group Key", KSII2009, June. 2009.
- [3] K. Zhang, C. Wang, C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management", IEEE2008, Aug. 2008.
- [4] E. Fasolo and M. Rossi, "In-Network Aggregation Technizues for Wireless Sensor Networks: A Survey", IEEE wireless communication, Apr. 2007.
- [5] 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 Volume 30, Issues 11-12, Special issue on security on wireless ad hoc and sensor networks, Sep. 2007.
- [6] M. W. Park, J. M. Kim, Y. J. Han, T. M. Chung, "A Misused Key Detection Mechanism for Hierarchical Routings in Wireless Sensor Network", NCM2008, Sep. 2008.
- [7] J. M. Kim, Y. J. Han, S. H. Park and T. M. Chung, "An Enhanced Misused Key Detection Mechanism in Wireless Sensor Networks", SENSORCOMM, 2008.
- [8] S. A. Camtepe and B. Yener, "Key Distribution Mechanisms for Wireless Sensor Networks: a Survey", Rensselaer Polytechnic Institute, Mar. 2005.
- [9] D. R. Choudhary, D. ANSHUL, S. Roy and C. S. Thejaswi, "Computationally and Resource Efficient Group Key Agreement for Ad Hoc Sensor Networks", IEEE, 2007.
- [10] M. Dustin, J. Shankarappa, M. Petrowski, H. Weerasinghe and H. Fu, "Analysis of Key Management in Wireless Sensor Networks", IEEE, 2007.