Tao JIANG, Liang-min WANG

Jiangsu University

Entropy Based Intrusion-tolerant Key Management Scheme with Updatability for Unattended Wireless Sensor Network

Abstract. *An Unattended Wireless Sensor Network (UWSN) collects the sensing data by using Mobile Sinks (MSs) which will save the battery power and prolong the network lifetime. Unfortunately, UWSNs are usually deployed in unreachable and hostile environments where MSs, who are given too much privilege, can be easily compromised. This will result in security problems. Thus, their security issues should be carefully addressed to deal with node compromise. In this paper, we present a novel key management scheme employing Blundo symmetric polynomial mechanism and the reverse hash chain to secure UWSNs. From the information entropy perspective, we prove that our scheme is intrusion-tolerant against conspiracy attack of t nodes in every group and show that our scheme is robust against node compromised attacks compared with relative schemes.*

Streszczenie *W niedozorowanych bezprzewodowych sieciach czujnikowych (UWSN) stosuje się zbieranie danych przy pomocy mobilnych stacji (mobile sink,MS). Dzięki temu uzyskuje się oszczędności w poborze mocy baterii oraz wydłużenie czasu życia sieci. UWSN są często umieszczane w niedostępnym i wrogim środowisku, gdzie MS, którym dano za dużo uprawnień, mogą być łatwo skompromitowane. To stwarza problemy bezpieczeństwa, szczególnie starannie rozpatrywane w przypadku kompromitacji węzłów sieci. W opracowaniu, w celu zabezpieczenia UWSN, przedstawiono nowy schemat zarządzania kluczem, wykorzystujący mechanizm symetrycznego wielomianu Blundo i odwrócony ciąg kodowy. Rozpatrując entropię informacji dowiedziono, że, w porównaniu do innych schematów, nasz schemat jest odporny na włamanie wobec ataków na t węzłów w każdej grupie oraz jest silny wobec ataków węzłów skompromitowanych.* ***Entropia opartego o odporny na włamanie schemat zarządzania kluczem z możliwością aktualizacji do niedozorowanej bezprzewodowej sieci czujnikowej***

Keywords: Wireless Sensor Networks, Security, Key Management, Mobile Sink, Information Entropy.
Słowa kluczowe: in the case of foreign Authors in this line the Editor inserts Polish translation of keywords

Introduction

An Unattended Wireless Sensor Network (UWSN) is a kind of hybrid wireless sensor network consisting of Mobile Sinks (MSs) and static sensing nodes [1], in which the MSs will bear most of the communication and computation overhead from multi-hop data transmissions in static WSNs and balance the network energy consumption, and hence prolong the network lifetime. Unfortunately, the introduction of the mobile nodes also brings some security concerns.

In some earlier studies, MSs are assumed to have the same capability as the base station, and the efficiency of data collection is the major design consideration [2, 3]. However, security is an unavoidable issue in UWSNs because of the unattended nature and hostile environments. Thus, the key management schemes for conventional WSNs cannot be directly applied in UWSNs for the participation of MSs.

High privileges given to MS may cause the security problems. Song, et al. [4] investigated the revocation problem of MS in their key management scheme. However, their scheme limits the flexibility of data collection. Rasheed et al. [5] proposed a new key management scheme for UWSN, however, it assigns too important role to the MS. when the MS is compromised, 90% of the pre-distributed random keys will be insecure.

To address the security over UWSNs, in this paper, we present a novel updatable key management scheme, in which the symmetric polynomial is used to generate shared keys between nodes and enables the threshold security feature of the network, while the reverse hash chain is utilized for key update or revocation to effectively restrict the privileges of MSs and at the same time for the identity generation of the newly-joined MSs. We analyze the threshold security of our scheme though the information entropy theory and compare it with relative schemes.

Network Model

A UWSN is a WSN with MSs used to help static Base Station (BS) collect data. We study the key management scheme under the network model with one MS.

There are multiple groups in our network, which contains two kinds of nodes: common nodes (Nodes) and cluster heads (CHs). At the network deployment stage, the nodes in each group are allocated to specific groups. When the MS joins the WSN, the network forms a three-layer structure.

We do not assume the MS is equipped with costly hardware security protection, which means that the adversary can obtain all confidential information pre-loaded in the MS if captured, but is costly for the adversary to perform physical capture attack. The adversary cannot capture and compromise more than t static nodes in a certain time period T_1 or capture and replicate the MS in time period $T_2(T_2>T_1)$ in every group.

Updatable Intrusion-Tolerant Key Management

In our scheme, key distribution consists of three phases, namely key material pre-distribution, key agreement, and key update as well as MS revocation.

Key Material Pre-distribution Phrase: For every group, the BS chooses a random symmetric bivariate polynomial $f(x, y)$ of degree t with coefficients over a finite field F_q, where q is a prime number large enough to accommodate a symmetric key:

(1) $$f(x,y)=\sum_{0\le m,n\le t} a_{mn}x^m y^n \qquad (a_{mn}=a_{nm})$$

Equation (1) is also called Blundo symmetric polynomial [6]. BS pre-loads the polynomial $f_{MS\text{-}Node}(ID,y)$ for MS and CHs. At the same time, BS chooses different polynomials $f_{CH_i\text{-}Node}(ID,y)$ for every group and pre-loads CHs and Nodes with different one referred to as $f_{MS\text{-}Node}(ID,y)$ and $f_{CH_i\text{-}Node}(ID,y)$. BS randomly selects an initial value S_n and calculates a reverse hash sequence $\{S_i\}_{i=0}^{n}$:

(2) $$S_{i-1}=h(S_i)(1\le i\le n)$$

In Equation (2), $h(\cdot)$ is a collision-free one-way hash function and $\{S_i\}_{i=0}^{n}$ is called the reverse hash chain [7].

Similarly, BS chooses a random value r_{MS} and then uses formula (3) to calculate the reverse hash sequence with $MS_n = r_{MS}$.

(3) $$MS_{i-1}=h(MS_i)(1\le i\le n)$$

At the beginning of the network deployment, BS pre-loads MS and CHs with polynomial $f_{MS\text{-}CH}(ID,y)$ and hash value S_0, in which the ID in $f_{MS\text{-}CH}(ID,y)$ represents the node identity and S_0 represents the first value of the reverse hash chain. Meanwhile, BS pre-loads the CHs and Nodes in different group with polynomial $f_{CH_i\text{-}Node}(ID,y)$ and hash S_0.

Key Agreement Phrase: We consider the key agreement between peer nodes u and v which are pre-loaded with $f(v,y)$ and $f(v,y)$ respectively. Let the current hash values stored in u and v are S_i and S_j, respectively. Then, u and v can carry out key agreement protocol KAP and key update protocol KUP as shown in Figure 1.

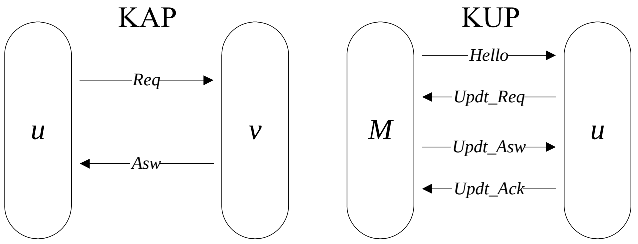

Fig.1. Key management protocol in our scheme

The node u firstly sends a request message Req to v

$$Req = \{u, i, seq, MAC\ (\ Key_{u\text{-}v}\{S_i\}, Msg\ )\} \tag{4}$$

where the $Key_{u\text{-}v}\{S_i\}$ is the shared key calculated by u independently through (5).

$$Key_{u\text{-}v}\{S_i\} = h(\ f\ (u, v), S_i) \tag{5}$$

Upon receiving Req, only when $i = j$ can v calculate $f\ (v, u)$ and $Key_{u\text{-}v}\{S_i\}$. Thus, we have

$$f\ (v,u) = f\ (u,v) \tag{6}$$

From the definition of $Key_{v\text{-}u}\{S_j\}$ and (6), we have

$$Key_{u\text{-}v}\{S_i\} = Key_{v\text{-}u}\{S_j\} \tag{7}$$

Hence, we obtain

$$MAC(Key_{v\text{-}u}\{S_j\}, Msg) = MAC(Key_{u\text{-}v}\{S_i\}, Msg) \tag{8}$$

For legitimate node u, v will reply with Asw

$$Asw = \{v, j, seq+1, MAC(Key_{v\text{-}u}\{S_j\}, Msg)\} \tag{9}$$

Upon receiving Asw, u will carry out the same procedure to verify the legitimacy of v.When $i \neq j$, u and v cannot forge $MAC(Key_{u\text{-}v}\{S_i\},v \mid i \mid seq+1)$ in Asw and cannot pass the authentication

Key update phrase: Let M be pre-loaded with $f(M,y)$ and hash value S_i. Let u be pre-loaded with $f(u,y)$ and hash value S_j. M notifies u that it comes to update the hash value and conduct key agreement through Hello message. Upon receiving the Hello message, u sends the update request message $Updt\_Req$ to update its key materials.

$$Updt\_Req = \{u, i, seq, MAC(Key_{u\text{-}M}\{S_i\}, Msg)\} \tag{10}$$

The elements u, i, seq, and Msg in (10) are similarly defined as in (4) and the updated shared key $Key_{u\text{-}M}\{S_i\}$ between u and M is calculated through equation (5).

When M gets message $Updt\_Req$ with $j \neq i\text{-}1$, M records u as a potential malicious node; Otherwise, when $j = i\text{-}1$, M calculates $S_j = h(S_i)$ to obtain S_j and verify the message through processes (5), (6) and (7). After passing the verification, M will send u the message

$$Updt\_Asw = \{M, i, S, seq+1, MAC(Key_{M\text{-}u}\{S_i\}, Msg)\} \tag{11}$$

From which M can send S_i to u securely with $S = E_{key_{M\text{-}u}\{S_{i-1}\}}\{S_i\}$. Upon receiving $Updt\_Asw$, u calculates S_i = $D_{key_{u\text{-}M}\{S_j\}}$ (S) and verifies the legitimacy of S_i. Finally, u sends $Updt\_Ack$ message (12) to confirm the establishment of the shared secret key between M and u.

$$Updt\_Ack = \{u, i, seq+2, MAC(Key_{u\text{-}M}\{S_i\}, Msg)\} \tag{12}$$

Through the above analysis, we observe that our scheme can carry out key agreement and key update to realize securely shared keys establishment and authenticated node revocation.

As a final remark, the MS may be subject to capture. To fight against this attack, effective node revocation and authentication node update are necessary. BS firstly generates a number of identities for MS as shown in (3). All CHs are pre-loaded with MS_0 firstly. After a period of time, the current identity of MS is supposed to be MS_i. If MS_{i+1} is needed, BS will pre-load MS_{i+1} with the relevant symmetric polynomial $f(M_{i+1},y)$ and a new hash value. In this case, MS_{i+1} can send CHs its identity through *Hello* message and CHs can authenticate MS through $MS = h(MS_{i+1})$. If MS_{i+1} is verified, CHs will store it as a legitimate one. Finally, we conclude that the use of reverse hash chain to generate the MS identity, can not only reduce unnecessary storage overheads, but also is resistant to the collusion attacks.

Entropy-based Intrusion tolerance Proof

In this section, we prove that the proposed key agreement protocol and key update protocol can resist t-collusion attack with the knowledge of information entropy.

Entropy Based Intrusion Tolerant KAP

Let $U = \{u_1,\ldots, u_n\}$ be a set of *n* nodes in our key agreement scheme and let *s* be the current shared hash value used in the two protocols above. At the same time, each node is pre-loaded with a t degree Symmetric polynomial $f\ (ID,y)$, in which f is a bivariate symmetric polynomial over finite field F_q and ID is the identity of the node.

We denote by X a set of any two nodes that need to calculate the shared key. Hence, $X \subseteq \{1,\ldots n\}$ and $|X| = 2$. Let $X = \{i, j\}$ be the set of any two nodes, then $u_X = \{u_i, u_j\}$ is the element consist of u_i and u_j, while U_X is the set of all possible u_X. The two nodes in u_X need to calculate $f_X = f(ID, u_X)$, $x \in X$ and according to the property of function f, we know that $f_i = f_j$ denoted by f_X. We denote F_X as

$$F_X = \{f \mid f = f(x,y), x, y \in F_q\} \tag{13}$$

For the set X, let $p_{F_X}(f)$ be the probability of $\forall f \in F_X$ when $f = f_X$, and let $H(F_X)$ be the entropy on the probability distribution $\{p_{F_X}(f)\}_{f \in F_X}$.

In our key agreement scheme, as long as the nodes in u_X obtain each other's ID, they can calculate the share value f_X between them. According to relevant proof [8], it holds that

$$H(F_X \mid U_X) = 0 \tag{14}$$

Indeed, the nodes in u_X also share an initial secret hash value s_X belonging to the reverse hash chain. According to the deterministic in Key agreement protocol, when calculating $Key_{S_X}^{u_i - u_j}$, it holds that

(15)
$$H(\{Key_{S_X}^{u_i - u_j}\} \mid U_X S_X) = 0$$

where S_X is the set of all possible known hash values in reverse hash chain.

From the perspective of information entropy, (15) ensures the correctness of Theorem 1as fallows:

Theorem 1. In the key agreement protocol, any two nodes u and v are able to calculate their shared key $Key_{u-v}\{S\}$ when they are pre-loaded with the same hash value S and polynomial as shown in (1).

Theorem 2. The key agreement protocol and key update protocol are both t intrusion-tolerant.

In the following we prove Theorem 2：

Proof： Let u_X and u_Y be the subset of $U = \{u_1,\ldots, u_n\}$, $X, Y \subseteq \{1,2,\ldots,n\}$, with $|Y|=k$, $|X|=2$ and $X \cap Y = \varnothing$. Then we denote by U_X the set of all u_X, $u_X \in U_X$ and U_Y the set of all $U_Y, u_Y \in U_Y$. When $k < t$ and $k + 2 \leq n$, the nodes in U_Y can not calculate $Key_{S_X}^{u_X}$, even if they have got the secret hash value s_X and conduct collusion attack. As a result, Theorem 2 is proved. Namely, we have to prove

(16)
$$H(Key_{S_X}^{u_X} \mid U_Y S_X) = H(F_X)$$

From [8] we know that if the S_X is independently chosen from U_Y, it will not affect the conditional information entropy, and combine the deterministic calculation process of $Key_{S_X}^{u_X}$, we obtain that

(17)
$$H(Key_{S_X}^{u_X} \mid U_Y) = H(F_X)$$

From (17), we know that, to prove (16), it is enough to prove $H(Key_{S_X}^{u_X} \mid U_Y S_X) = H(Key_{S_X}^{u_X} \mid U_Y)$, namely

(18)
$$H(Key_{S_X}^{u_X} \mid U_Y) - H(Key_{S_X}^{u_X} \mid U_Y S_X) = 0$$

According to the conditional mutual information entropy formula

(19)
$$I(X;Y \mid Z) = H(X \mid Z) - H(X \mid ZY)$$

It holds that

(20)
$$H(Key_{S_X}^{u_X} \mid U_Y) - H(Key_{S_X}^{u_X} \mid U_Y S_X) = I(Key_{S_X}^{u_X}; S_X \mid U_Y)$$

From (19), we have $I(S_X; Key_{S_X}^{u_X} \mid U_Y) = H(S_X \mid U_Y) - H(S_X \mid Key_{S_X}^{u_X} U_Y)$. Then, from $I(X; Y \mid Z) \geq 0$ and (19) we obtain that $H(X \mid Z) \geq H(X \mid ZY)$, hence $I(S_X; Key_{S_X}^{u_X} \mid U_Y) \leq H(S_X) - H(S_X \mid U_Y)$. Since S_X and U_Y are independent, we have $I(S_X; Key_{S_X}^{u_X} \mid U_Y) \leq 0$. According to the property of conditional mutual information entropy we obtain $I(S_X; Key_{S_X}^{u_X} \mid U_Y) = I(Key_{S_X}^{u_X}; S_X \mid U_Y) = 0$.

By (20), it is clear that (18) is proved. Since the range of k is variable, hence theorem 2 is proved.

Intrusion tolerant Properties of KUP

In fact, we can not prove the security of our key update protocol from the perspective of entropy, because the hash function is not unconditionally secure. Suppose that the reverse hash chain and the encryption technology do not affect the security features of our protocols in the sense of entropy, then the proof of the intrusion tolerant capacity of key update protocol will be similar to theorem 2, which we do not repeat the proof here.

Network Intrusion Analysis

For the sake of discussion, we assume that the numbers of symmetric polynomials pre-loaded in the MS and cluster heads are a and b, respectively, there are b cluster heads in one subarea, and the total number of subareas is not more than t. Suppose that there are n nodes in each subarea, then the total number of nodes in the network is $N = a \cdot t \cdot n/b$. Our key agreement scheme can resist collusions among no more than t nodes in one subarea. We define the intrusion tolerance rate as the secure links probability shown in (21):

(21)
$$p_{\text{Tol}}(x) = \frac{L_{\text{All}}(x) - L_{\text{Compromised}}(x) - L_{\text{Ind\_Compromised}}(x)}{L_{\text{All}}(x) - L_{\text{Compromised}}(x)}$$

where x is the number of nodes compromised by the adversary, $L_{\text{All}}(x)$ is the total number of links in the network, $L_{\text{Compromised}}(x)$ is the number of the compromised links and $L_{\text{ind\_Compromised}}(x)$ is the number of links that are potentially insecure because of captured nodes.

It is clear that, if $n < t$, no matter how many nodes are compromised, they will not affect the communications security among normal nodes. If $n > t$, the attacker could compromise more than t nodes in one subarea, leading to completely security breach in the subarea. With some mathematical manipulations, we obtain the network intrusion tolerance rate as in equation (22),

(22)
$$p_{\text{Tol}} = \begin{cases} 1 & 0 \leq n \leq t+1 \\ g(x) & t+1 < n \leq N \end{cases}$$

where $g(x)$ is given by:

(23)
$$g(x) = \frac{\left[\frac{N}{n} - \left\lceil \frac{x}{t+1} \right\rceil\right]\binom{n}{2} + \binom{n - [x \bmod (t+1)]}{2}}{\left[\frac{N}{n} - \left\lfloor \frac{x}{t+1} \right\rfloor - 1\right]\binom{n}{2} + \left\lfloor \frac{x}{t+1} \right\rfloor \binom{n-t-1}{2} + \binom{n - [x \bmod (t+1)]}{2}}$$

(In Figure 2, we show the network intrusion tolerance rate for $n < 101$, $n = 200$ and $n = 400$, when the network parameters are $a = 2$, $b = 2$, $t = 100$ and $N = 10000$. We also compare our scheme with those in [4], [5] and [9].

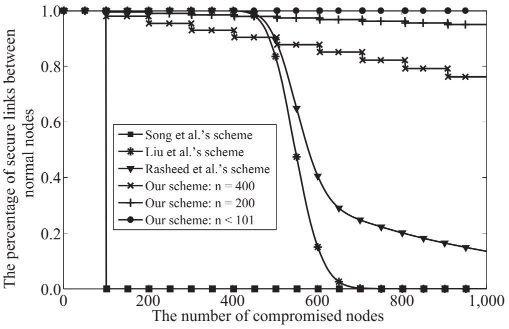

Fig.2. Network intrusion tolerant rate

We observe that, in Song et al.'s scheme [4], when the number of compromised nodes exceeds the threshold t, the entire network will be completely controlled by the attacker. The polynomial key pool scheme [9] can guarantee that when the number of compromised nodes is not more than 400, the whole network is secure.

Conclusions

In this paper, we propose an updatable and intrusion-tolerant key management scheme for UWSN which uses the Blundo symmetric polynomial and the reverse hash chain technology for key agreement and key updating to prevent compromised mobile nodes from communicating with static nodes. We conduct detailed security analysis and compare our scheme with related outcomes in intrusion tolerant rate.

Acknowledgments *We would like to acknowledge that this paper is supported by Natural Science Foundation of Jiangsu Province under No.BK2011464, and Natural Science Foundation of China under No.61003300. The author Liang-min Wang is supported by Special Funding Scheme of China Postdoctoral Science Foundation under No.200801357, QingLan Project of Jiangsu Province and Talents Foundation of Jiangsu University under No.07JDG080.*

REFERENCES

[1] Ma D., Tsudik G., Security and privacy in emerging wireless networks. IEEE Wireless Communications. 17 (2010) 12–21.

[2] Anastasi G., Conti M., Di Francesco M., Reliable and energy-efficient data collection in sparse sensor networks with mobile elements. Performance Evaluation. 66 (2009) 791–810.

[3] Rao J., Biswas S., Network-assisted sink navigation for distributed data gathering: Stability and delay-energy trade-offs. Computer Communications. 33 (2010) 160–175.

[4] Song H., Zhu S., Zhang W., Cao G., Least privilege and privilege deprivation: Toward tolerating mobile sink compromises in wireless sensor networks. ACM Transactions on Sensor Networks. 4 (2008) 1–30.

[5] Rasheed A., Mahapatra R., Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks. IEEE Transactions on Parallel and Distributed Systems. 23 (2011) 176–184.

[6] Blundo C., Santis A.D., Herzberg A., Kutten S., Vaccaro U., Yung M., Perfectly-secure key distribution for dynamic conferences. Advances in Cryptology-Crypto'92. (1992).

[7] Lamport L., Password authentication with insecure communication. Comm. of ACM. 24 (1981) 770-772.

[8] Merkle R.C., A certified digital signature. In CRYPTO. 435 (1989) 218–238.

[9] Liu D.Q., Ning P., Establishing pairwise keys in distributed sensor networks. Proc. 10th ACM Conf. Computers and Comm. Security. (2003) 52–61.

Authors: *Dr. Liang-min Wang (corresponding author), Department of Computer Science Jiangsu University, Zhenjiang, 212013, P.R. China, E-mail: jiangt2009@gmail.com; Mr Tao Jiang, E-mail: jiangt2009@gmail.com;*