A Practical Inter-sensor Broadcast Authentication Scheme

Joon Wan Kim, Yong Ho Kim*, Hwaseong Lee, and Dong Hoon Lee

Center for Information Security Technologies(CIST), Korea University
{lechorok,optim,hwasaeong,donghlee}@korea.ac.kr

Abstract. For inter-sensor broadcast authentication in wireless sensor networks, Chen *et al.* proposed a bootstrapping scheme which enables to save only neighboring nodes' hash-chain commitments, much fewer than whole network size, before deployment [2]. However, the scheme lacks scalability and is not tolerant for node isolation. Therefore, we suggest new mechanism providing scalability and present its modified version with node-redemption which makes most of nodes participate in broadcast authentication with a little additional memory.

Keywords: security, authentication, wireless sensor network.

1 Introduction

For broadcast authentication(BA) in wireless sensor networks, μ-TESLA based on delayed disclosure of verification keys and multi-level μ-TESLA enlarging life time of system were suggested [8,11]. But these approaches were useful only in a specific model where sensors verifies packets from base station(BS). For authentication between sensors, it requires verification keys which can check mutual signs. As we consider random deployment, however, each node should pre-install $n-1$ keys nearly to n, size of entire network excluding each node itself. For dealing with this impractical situation successfully, Chen *et al* proposed a bootstrapping scheme for the first time, which enables to save only nearby nodes' hash-chain commitments, much fewer than $n-1$, before deployment [2]. This approach is very significant, for it realized inter-sensor broadcast authentication(ISBA), which overcame traditional BA in which BS becomes signer and sensor becomes verifier. Unfortunately, the scheme lacks scalability and does not suggest a solution to problems of node isolation caused by some error such as initialization failure because of packet loss which may occur after random deployment. Thus we suggest new mechanism providing scalability and node-redemption.

* "This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement)" (IITA-2006-(C1090-0603-0025)).

C. Stephanidis (Ed.): Universal Access in HCI, Part I, HCII 2007, LNCS 4554, pp. 399–405, 2007.

1.1 Related Works

Perrig *et al.* proposed a μ-TESLA mechanism that is optimized to WSNs from original TESLA [11]. Liu *et al.* suggested enhanced version of multi level μ-TESLA which enlarges the life time of network and provides efficient updating algorithm for commitments [8]. By enlarging hash-chain level and delaying time, their scheme is weak to such DoS attack. Chen *et al.* claim that ISBA is essential in WSNs and proposed a bootstrapping scheme to achieve it based on the multi level μ-TESLA mechanism [2]. They have assumed random deployment of sensor nodes and targeted the distribution of hash-chain commitment and authentication. According to their approach, each node just needs commitments of nearby nodes after deployment without entire $n-1$ commitments. As a result, every node broadcasts their own commitments and stores commitments of the sensor nodes within a broadcast transmission range. By this optimized transmission mechanism for the distribution of hash-chain commitments, each sensor needs small storage portion as nearby density.

Contributions. Our contribution is as below.

- We proposed a first *scalable* inter-sensor broadcast authentication scheme using only symmetric primitives.
- We suggested a concept of multi-session in network lift time for enabling controlled network scalability.
- The proposed node-redemption guarantees the nodes that are isolated in bootstrapping period to participate in already organized network.
- Our schemes are *perfect resilience* under selective node capture attack in the all session.

2 Preliminary

2.1 Inter-sensor Broadcast Authentication

Traditionally in WSNs, referring to BA, many researchers have focused on verifying validity of packet which is mainly sent when BS orders specific commands to nodes or sends data. It is no wonder that forgery by malicious adversary, wrong orders, and no authentication would threaten so much usability and security of network. What is remarkable is that most of proposed methods using μ-TESLA are designed for these models. In other words, when those approaches want to broadcast to nearby nodes, not to BS, they requested that BS would broadcast through hop by hop route [8,11,13]. Intuitively, these ways lay a burden on all nodes in routes to BS due to too much communication overheads whenever nodes broadcast. Especially damage of nodes near BS participating in transmission so often is much more serious. Therefore when a node broadcasts to nearby nodes, it would be better to broadcast itself. It is ISBA that enables a certain node to authenticate itself to its nearby nodes when the node wants to broadcast to its nearby nodes. In next subsection, we consider necessity of ISBA and its application models.

2.2 Application Models

ISBA can be used conveniently and practically in *interior network process* excluding BS [2]. For example, when there is some information all the nodes within broadcast range should know, ISBA makes nearby nodes broadcast only once without unicasting as many as nearby nodes, achieving purposes they want. And when new routing is needed because of node capture or isolation, nearby nodes can inform node searching for routes or isolated node of route information rapidly. Especially ISBA is very suitable for voting mechanism researched recently. That is, existing voting approaches for logical revocation of node suspected a malicious was dependent on unicast between nodes or broadcast from BS. However, if ISBA is used, instant and local voting can be available and the length of packet will be shorter and the transmission frequency will be lower so that communication costs(very large portion of entire costs) can be reduced.

3 The Proposed Schemes

3.1 The Basic Scheme

The basic scheme consists of five phases; initialization phase, broadcasting phase, waiting phase, reveal phase, and node addition phase. All the commands of BS (e.g. START and STOP) are authenticated by BS-node μ-TESLA mechanism. In this case, storage overhead of network is very small, since every node is forced to store just only one commitment of BS to authenticate his signs on each packet. We suppose that we may say session counter s increases when it happens physical changes of network topology by system organizer. In contrast, for any changes by attacker such as node capture or isolation of some nodes in bootstrapping period, we may not call them session increasing despite of logical change of topology. In addition, we also assume that all the sensor nodes are spread randomly over a target field so that any node does not predict who will be nearby.

I. Initialization (before nodes deployment)

- For entire network size n, number all sensors by unique IDs such that $ID_1, ID_2, ..., ID_n$
- Choose GMK_m at random and then create a GMK hash-chain as following $GMK_i = hash(GMK_{i+1})$ $(i = 1, 2, ..., m-1)$ (where m is the length of session) and call GMK_1 a GMK hash-chain commitment.
- Create unique secret keys as following and store them to each sensor nodes one by one.

$$K_{ID_j} = hash(ID_j||s||GMK_s) \quad (1 \leq j \leq n)$$

  where s is session counter starting from 1

II. Broadcasting Phase (after nodes deployment)

- BS broadcasts a START command to all sensor nodes.
- Each node $ID_j (j = 1, 2, ..., n)$ encrypt following value using their secret keys that already are stored at themselves and broadcast it to nearby nodes with IDs.

$$Auth = E_{K_{ID_j}}(ID_j||s||F_{ID_j})$$

(where F_{ID_j} is μ-TESLA hash-chain commitment of ID_j for general using of ISBA. Signer has this value and entire hash-chain information, and verifiers authenticate all broadcast messages from the signer using that commitment and the μ-TESLA mechanism.)

- After nodes deployment, BS broadcasts STOP command to all sensor nodes, each nodes can neither broadcast messages nor buffer received messages.

III. Waiting Phase

- Wait for time of δ.

IV. Reveal Phase

Base station

- Broadcast GMK_s to all sensor nodes.

Sensor nodes

- ID_v can construct K_{ID_j} with GMK_s, ID_j, and session counter. After that he can decrypt $Auth$ and authenticate $(Auth, ID_j)$ comparing ID_j with inside ID.
- If verification is successful, ID_v will accept F_{ID_j} as μ-TESLA hash-chain commitment of ID_j, else discard it.

V. Node Addition Phase (After session s)

- In session $s + 1$, for node addition, store following values to each sensors before nodes deployment.

$$K_{ID_j} = hash(ID_j||s + 1||GMK_{s+1})$$

- After deployment, each additional node ID_a computes following value and broadcasts $(Auth, ID_a)$ to every nearby node.

$$(Auth, ID_a) = (E_{K_{ID_a}}(ID_a||s + 1||F_{ID_a}), ID_a)$$

- Similar with phase IV, BS reveals GMK_{s+1} to all sensors, and each node computes as following

$$K_{ID_a}(ID_a||s + 1||F_{ID_a}\ D_{K_{ID_a}}(E_{K_{ID_a}}(ID_a||s + 1||F_{ID_a})))$$

If verification is successful, F_{ID_a} will be accepted as μ-TESLA hash-chain commitment of ID_a else discard it.

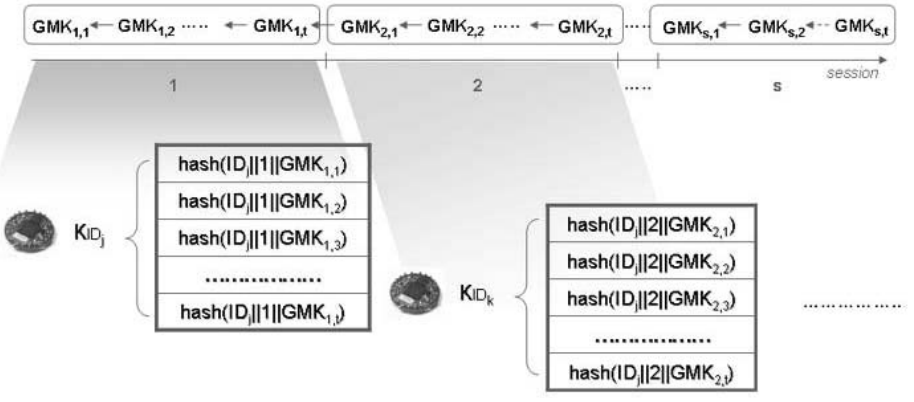

Fig. 1. Assigning GMK hash-chain key blocks for each session to provide node-redemption in deployed network

3.2 The General Scheme

The general scheme is identical to the basic scheme except that it stores hash-chain as a block unit as many as t hash-chain per every session like Fig. 1. Even if some nodes are excluded in initial authentication that uses the first key, just after deployment, the second or other keys remain secretly because they have elements of GMK that is not revealed yet. For example, after ID_j is excluded in first chance, Fig. 2 shows us authentication phases are newly started using $K_{ID_{j,1,2}}$ that includes $GMK_{1,2}$. In this way, nearby nodes can authenticate commitment of ID_j with revealed $GMK_{1,2}$. The size of t is important and we can guess practical size by following equation. It supports a node-redemption. That is, it is possible for most of nodes to be authenticated with a little additional memory unlike the basic scheme where nodes can be authenticated only within a specific time.

n: entire network size, τ: isolation rate
Φ: available authentication channel size

$$\Phi(n) = n(1-\tau)(1+\tau+\tau^2+...+\tau^{t-1})$$
$$t \longrightarrow \infty, \Phi(n) \longrightarrow n$$

If we suppose that $\tau = 0.02$ and $t = 3$, the general scheme can cover 99.9992%.

4 Analysis on Proposed Schemes

4.1 Security Analysis

Proposed schemes are secure against the following attacks.
Impersonation Attack:

- **Case 1:** All the commands to control the distributed sensor nodes are broadcasted by BS and authenticated by nodes with μ-TESLA mechanism. Since

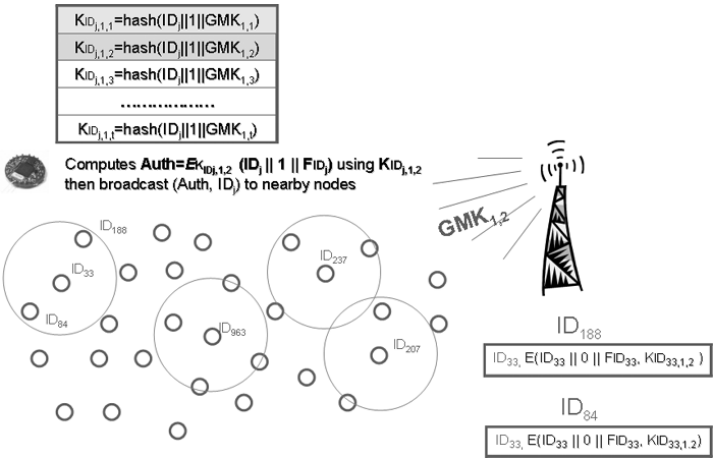

Fig. 2. An example of node-redemption

that reason, an attacker can fabricate the commands and impersonate BS with probability of forging hash values.

– **Case 2:** In many actual environments, our system may be eavesdropped by an attacker. Especially, if BS reveals the GMK in phase IV, any attacker can easily compute some node's value of Auth because of knowing his secret key used in encryption step. This result, however, dose not lead the attacker to authenticate his own hash-chain commitment successfully to nearby nodes. The reason is that any node(even malicious one) has no chance of giving his commitment to nearby nodes after the end of the broadcasting phase, except for this phase II so that one receives or accepts Auth packets.

Collusion Attack: This condition of attack can be done when one or more malicious nodes collude each other to compute another secret key using their known keys. Even if the conspirators know a number of K_{ID_j}, they can not compute any proper secret key K_{ID_m} because of unknowing GMK as pre-image part of the hash value.

Selective Node Capture: Proposed schemes construct hash-chain and its commitment independently for each sensors. So, although an adversary knows secret information of some sensors, she never knows about secrets of any other nodes.

4.2 Efficiency Analysis

Our scheme needs only one broadcast in order to send the each node' own hash-chain commitment to the neighbor nodes. And a sender stores only keys as much as the size of nearby nodes, not $n-1$. Since GMK or commitments nearby nodes are continually updated, it is needed just current one instead of whole values.

5 Conclusion

We proposed two ISBA schemes based on the initial distribution mechanism for the μ-TESLA hash-chain commitments of each neighbor nodes. Simultaneous using of the proposed two schemes provides scalability and node-redemption for isolated nodes during the initial broadcasting phase. In all the phases, we just need symmetric primitives such a hash function and block cipher algorithm. Our schemes guarantee a property *perfect resilience* under selective node capture attack for all the network sessions.

References

1. Chang, S., Shieh, S., Lin, W., Hsieh, C.: An Efficient Broadcast Authentication Scheme in Wirless Sensor Networks. In: Proc. ASIACCS06, pp. 311–320 (March 2006)
2. Chen, W., Chen, Y.: A Bootstrapping Scheme for Inter-Sensor authentication within Sensor Networks. In: IEEE Communication Letters, vol. 9(10) (October 2005)
3. Chen, H., Perrig, A., Song, D.: Random key distribution schemes for sensor networks. In: Proc. IEEE Symposium on Security and Privacy, pp. 197–215.(May 2003)
4. Deng, J., Han, R., Mishra, S.: A performance evaluation of instrusion-tolerant routing in wireless sensor networks. In: Zhao, F., Guibas, L.J. (eds.) IPSN 2003. LNCS, vol. 2634, pp. 349–364. Springer, Heidelberg (2003)
5. Eschenauer, L., Gligor, V.: A key-management scheme for distributed sensor networks. In: Proc. the 9th ACM conference on Computer and Communications security, pp. 41–47 (November 2002)
6. Menezes, A., Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997)
7. Hwang, J., Kim, Y.: Revisiting Random Key Pre-distribution for Sensor Networks. In: ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04) (2004)
8. Liu, D., Ning, P.: Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In: Proc. Annual Network and Distributed System Security Symposium(NDSS), pp. 263–276 (February 2003)
9. Moon, H., Lee, S.: Efficient Broadcast Authentication in WSNs. In: Proc. of IEEK vol. 43(6), pp. 683–689 (2006)
10. Perrig, A., Stankovic, J., Wagner, D.: Security In Wirless Sensor Networks. Communication of the ACM 47, 53–57 (2004)
11. Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J.D.: SPINS: Security Protocols for Sensor Networks. Wireless Networks 8, 521–534 (2002)
12. Zhang, Y., Liu, W., Lou, W., Fang, Y.: Location-Based Compromise-Tolerant Security Mechanism for Wirless Sensor Networks. In: IEEE Journal on Selected Areas in Communications, vol. 24(2), (February 2006)
13. Zhu, S., Setia, S., Jajodia, S.: LEAP: efficient security mechanism for large-scale distributed sensor networks. In: Proc. Symposium on Information Processing in Sensor Networks (IPSN), pp. 259–268 (April 2004)