Defense against HELLO Flood Attack in Wireless Sensor Network

Md. Abdul Hamid*, Choong Seon Hong*, Sang Ick Byun**
*Dept. Of Computer Engineering Kyung Hee University, South Korea
**National Computerization Agency
hamid@networking.khu.ac.kr, cshong@khu.ac.kr, sibyun@nca.or.kr

Abstract

We consider Wireless Sensor Network Security (WSN) and focus our attention to tolerate damage caused by an adversary who has compromised deployed sensor node to modify, block, or inject packets. We adopt a probabilistic secret sharing protocol where secrets shared between two sensor nodes are not exposed to any other nodes. Adapting to WSN characteristics, we incorporate these secrets to establish new pairwise key for node to node authentication and design multipath routing to multiple base stations to defend against HELLO flood attacks. We then analytically show that our defense mechanisms against HELLO flood attack can tolerate damage caused by an intruder.

12193-0) funded by the korean Government(MOEHRD) and by NCA

1. Introduction

In a large-scale sensor network individual sensors are subject to security compromise. There are several network layer attacks against sensor networks and are well described in [3]. Among them, spoofed, altered, or replayed routing information, selective forwarding, sinkhole attacks, Sybil attacks, wormholes, HELLO flood attacks, acknowledgement spoofing are well known attacks that try to manipulate sensed data. In this paper we consider routing security against HELLO flood attack.

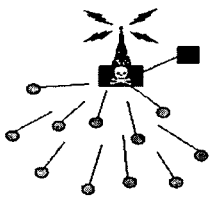


Figure 1: HELLO flood attack. A laptop- class adversary that can retransmit a routing update with enough power to be received by the entire network leaves many nodes stranded. They are out of normal radio range from the adversary but have chosen her as their parent.

As shown in figure 1, many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender [3]. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. The majority of the sensor nodes are stranded, sending packets into oblivion. There is high possibility for a mote class [3] attacker to create routing loops by spoofing routing updates.

In this paper, we present probabilistic secret sharing protocol adopted from [1] where, a small increase in the number of secrets maintained by a user substantially reduces the probability of privacy compromise. We show how these secrets can be further used to establish pairwise key and using this resulting key to implement an authenticated, encrypted link between them. To defend against HELLO flood attack, we show that it is possible for every node to authenticate each of its sender and receiver.

We provide further defense mechanism by incorporating the concept of multipath multi-base station routing to improve the tolerance caused by an adversary who has highly sensitive receiver as well as powerful transmitter.

2. Related Work

Sensor network security has been studied in recent years in a number of proposals. Kulkarni et al. [1] analyzes on the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. Fan Ye et al. [2] focused on how to filter false data using collective secrets and thus preventing any single compromised node from breaking down the entire system. In [3] Karlof et al. thoroughly discussed the problem of secure data transmission for different routing protocols and they conclude that none of them have been designed with security as a goal. Passive attacks such as cipher text attack and chosen cipher text attacks, a security protocol has been proposed in [4]. Their works requires synchronization initiated by base station and also by sensor networks. SPINS [5] implements symmetric key cryptographic algorithms

This work was supported by the Korea Research Foundation Grant (R05-2003-000-

with delayed key disclosure on motes. Reference [6] implements ticket certification services through multiple-node consensus and fully localized instantiation, and uses tickets to identify and grant network access to well-behaving nodes. Sybil and Rushing attacks are well discussed in [7, 8]. Sybil attack is a threat to WSN where a node legitimately claims multiple identities. Random pairwise key distributions are discussed in [9] and [10] to make the sensor networks resilient to security threats.

Our approach considers the routing vulnerability specially HELLO flood attack and discusses the counter measures and design considerations for secure routing in sensor networks.

3. Secret Instantiation by Tree Protocol

We present probabilistic secret sharing protocol adopted from [1]. We organize the secrets in a tree (Fig. 2). Each non-leaf node is associated with a secret and each leaf is associated with a sensor node. Each sensor node is assigned an ID that identifies its location in the tree. Finally each sensor node is provided the secrets along the path towards the root. Thus, node s_1 has the secrets, k_1, k_2 and k_4.

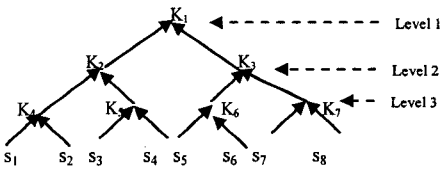


Figure 2: Single Tree Key Assignment

When two nodes, say, s_1 and s_2, want to exchange messages during their effective communication, they first exchange their identities. Then, they identify their least common ancestor and based on the secret distribution mechanism, the common secret associated with this ancestor will be available to both s_1 and s_2. So, the secret associated with the ancestor will be used for communication between s_1 and s_2. For example, two nodes s_1 and s_2 want to communicate then they will use secret key k_4 whereas if s_1 and s_5 want to communicate then they will use secret key k_1.

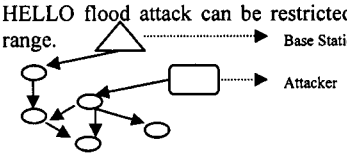
To reduce the probability of node compromise, calculated in [1] that, given T secret-trees (Multiple Tree Protocol), each with degree d, the probability that x knows secrets from all the trees is $(d/(d+1))^T$.

4. New Key Setup During Communication

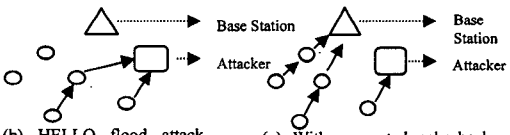
According to the secret distribution protocol described earlier, we know that every pair of nodes shares some number of initial secrets n. Let's assume node x and y shares initial secrets $k_i(i=1,2,....,n)$. Prior to communicate with each other, these tow nodes can generate a new key using those initial secret on demand. This can be done using some mathematical function e.g. RC5 [16] to generate MAC. So, we say that new key $E_{new\text{-}key} = MAC(k_1, k_2, ..., k_n)$. This MAC is calculated and used for node to node authentication prior to their communication.

5. Counter Measure Against HELLO Flood Attack

If each sensor node constructs a set of reachable neighbor nodes, and is only willing to receive REQ messages from this set of neighbor nodes, then REQ messages from an adversary transmitted with larger power will be ignored. Thus, the damage from a HELLO flood attack can be restricted within a small range.



(a) Attacker advertises REQ message with large transmission power, legitimate nodes think that attacker is their initiator.



(b) HELLO flood attack, legitimate nodes think that attacker is their initiator

(c) With encrypted echo-back mechanism, message exchange won't be blocked by the

Figure 3: HELLO flood attack and defense

Fig. 3 gives a pictorial view of how HELLO flood attacks can be initiated and the defense against the attack. We see that some nodes will not be blocked by the attack. Each node locally broadcasts an echo message to its neighbor with format:

$s_1 \rightarrow$: ECHO||$E_{new\text{-}key}$ (IDs_1||nonce)

Where, ECHO is the message type, ID is the ID of the sensor node s_1, $E_{new\text{-}key}$ is the new key as we have mentioned earlier and nonce is the random number. If a node, say, s_2 receives this message; it sends echo reply with format:

$s_2 \rightarrow s_1$: ECHOBACK||$E_{new\text{-}key}$ (IDs_2||nonce)

When node s_1 receives this message, it records node s_2 as its verified neighbor. If an attacker obtains the shared secrets after a node has received its new encrypted key, it can not know the new pairwise key. However, if an attacker obtains the new key, it can initiate echo-back many times by sending several echo messages. The attacker can generate false identities and can initiate Sybil attack, adding new nodes with

false identities. To prevent such attacks, node should destroy its new key from memory after a certain time that is long enough to set up pairwise keys with all its neighbors.

6. Multi-path Multi-base Station Data forwarding

We describe how a sensor node can forward its sensed data to multiple routes. We assume that, there are a number of base stations in the network who have control over specific number of nodes and also, there are common means of communications among base stations. Each base station has all the secrets (i.e. initial secrets) those are shared by all the sensor nodes according to the key assignment protocol described earlier. Given the shared secrets and the generated new key between two sensor nodes, the operation of setting up different routing paths is as follows:

Step 1: As each sensor node shares some common keys according to the secret distribution protocol (i.e. Multiple Tree Protocol), every node uses the echo-back scheme to identify its neighbor nodes and sets up pairwise new key with its verified neighbor nodes. Then it uses its new key to exchange messages among them.

Step 2: Each base station broadcasts its request (REQ) message to its neighbor nodes with the following format:

$$REQ||ID_x||E_{key}(ID_B||HCN)$$

Here, REQ is the message type, ID_x is the ID of the sending node x, ID_B is the base station ID who generated this request message, E_{key} is the key (i.e. initial secret) that is common between any node to which base station floods the message and HCN is the base station's one-way hash chain number. Receiving node verifies that the REQ comes from the base station, then it forwards the REQ to its neighbor node, say, y, with the format:

$$REQ||ID_y||E_{new\text{-}key}(ID_B||HCN)$$

Step 3: When any ordinary node say, y, receives this REQ message, it checks the sender ID. If s is y's verified neighbor, y decrypts and authenticates the sender with computed new key $E_{new\text{-}key}$. If the message sender is valid, it replaces the HCN with the new value and encrypts the REQ message with its $E_{new\text{-}key}$ and broadcasts the newly encrypted message. In this way, flooding REQ messages securely establishes direction of routing.

7. Conclusion

This work described the defense against HELLO flood attack by introducing node to node authentication and multi-path routing using shared secret between sensor nodes. We have adopted a probabilistic key assignment protocol among sensor nodes and during communication, each node can calculate a pairwise key using these common secrets and hence improving the network resilience against security threats. We have shown that our defense mechanism can well tolerate the damage launched by the intruder. Currently we are exploring the maintenance issues such as nodes joining and leaving the network and the effect of message loss.

8. References

[1] S. S. Kulkarni, M. G. Gouda, and A. Arora: Secret instantiation in ad-hoc networks. In: Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, (2005) 1–15

[2] F. Ye, H. Luo, S. Lu, and L. Zhang: Statistical En-Route Filtering of Injected False Data in Sensor Networks. In: IEEE Journal on Selected Areas in Communications, Vol. 23, no. 4, (2005)

[3] C. Karlof and D.Wagner: Secure routing in wireless sensor networks: Attacks and countermeasures. In: Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3)(2003) 293–315

[4] R. Di Pietro, L. V. Mancini, and S. Jajodia: Providing secrecy in key management protocols for large wireless sensors networks. In: Journal of AdHoc Networks, 1(4), (2003) 455-468

[5] V. Wen, A. Perrig, and R. Szewczyk: SPINS: Security suite for sensor networks. In: Proc. ACM MobiCom, (2001) 189–199

[6] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang: URSA: Ubiquitous and robust access control for mobile ad hoc networks. In: Proc. IEEE/ACM Trans. Netw., Vol. 12, no. 6, (2004) 1049–1063

[7] J.R. Douceur,: The Sybil attack. In: 1st International Workshop on Peer-to-Peer Systems (IPTPS _02) (2002)

[8] Y. Hu, A. Perrig, and D. Johnson: Rushing attacks and defense in wireless ad hoc network routing protocols, In: Second ACM Workshop on Wireless Security (WiSe'03), San Diego, CA, USA (2003)

[9] H. Chan, A. Perrig, D. Song: Random key predistribution schemes for sensor networks. In: IEEE Symposium on Security and Privacy (2003)

[10] W. Du, J. Deng, Y. Han, P. Varshney: A pairwise key pre-distribution scheme for wireless sensor networks. In: ACM Conference on Computer and Communications Security (CCS), (2003) 42–51