TDMA-Based Detection of Packet Modification Attacks in Wireless Sensor Networks

Hae Young Lee and Hyung-Jong Kim

Department of Information Security
Seoul Women’s University
Seoul 01797 Republic of Korea
whichmeans@gmail.com

Abstract. In a wireless sensor network, a few sensor nodes can be physically captured by a malicious adversary and then, by using the whole information they hold, skilfully modify some legitimate packets passing through the captured nodes. Such packet modification attacks (PMAs) could make real events on the field or control messages from the base stations (BSs) considered as false ones, so that some critical events, such as the enemy’s advances, may not be reported to the BSs, or BSs may lose control of numerous nodes. In this paper, the author proposes a method of detecting PMAs in WSNs, in which each PMA can be detected and notified to the BSs through a time division multiple access based collaboration among the detecting nodes. While the proposed method does not require tamper-resistant hardware, the method guarantees that a PMA can be detected unless half of the detecting nodes are collude with the PMA. The performance of the method is reviewed with simulation results.

Keywords: Wireless sensor networks, node capture, security, insider attacks, packet modification attacks

1 Introduction

A wireless sensor network (WSN) is comprised of hundreds or even thousands of small sensor nodes and some base stations (BS). In many applications, these nodes are unattended by the users since they are often deployed in hostile environments, such as battlefields [1]. Thus, by capturing a few nodes, a malicious adversary could compromise the whole of the nodes’ secret information, such as authentication keys [2]. Note that nodes are not equipped with tamper-resistant hardware due to cost constraints [3]. Using such compromised nodes, the adversary could inject fabricated sensing reports [4-7], which are technically correct, but notify the users of non-existent events. These fabricated reports may lead to real-word responses, such as dispatching patrols to some regions, or denial-of-service and energy depletion [7].

1 This research was supported by the MISP (Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW (R7116-16-1018) supervised by the IITP (Institute for Information & communications Technology Promotion). (R7116-16-1018)
Another type of potential insider attacks is packet modification attacks (PMAs) [8]. In PMAs, an adversary uses some compromised nodes to skillfully modify some legitimate packets passing through the nodes, with the goal of preventing notifications of critical events to the BSs or BSs’ control over downstream nodes. For example, a compromised node \( F_i \) shown in Fig. 1 could alter a single bit of the packet received from \( F_{i-1} \) and forward the altered packet to \( F_{i+1} \), which would result in a violation of the integrity. Thus, the packet would be dropped by a forwarding node or rejected at the destination.

![Fig. 1. A packet modification attack (PMA) in wireless sensor network.](image)

In this paper, we propose a method of detecting PMAs based on time-division multiple-access (TDMA) in homogeneous WSNs. In the proposed method, for each forwarding node, some of its neighboring nodes are chosen as the committee nodes of the node. These committee nodes overhear every packet passing through the forwarding node, and check if a packet the node received and its copy the node has forwarded match exactly at network and higher layers. If these two packets do not match, the committee considers that the node has launched a PMA against the packet. Then, the committee nodes collaboratively generate a misbehavior report (MR), which informs the users of the PMA, and forwards the MR towards the BS. The collaboration among the nodes is performed based on TDMA. The method assumes that some of the committee nodes can be also captured by the adversary. Unless half of them are collude with the PMA, the method guarantees that an MR for the PMA is forwarded towards the BS. The performance of the method is shown with simulation results at the end of the paper.

2 Overhearing-Based Detection Mechanism (OBD)

In [8], Ssu et al. proposed the overhearing-based detection mechanism (OBD) in which PMAs launched by a forwarding node can be detected in collaboration among its surrounding nodes in WSNs. For each forwarding node, some of its neighboring nodes are chosen as its committee nodes. Each of them can overhear packets from/to the forwarding node due to the broadcast nature of wireless communications. Each of the committee nodes compares packets sent to the forwarding node and those sent by
the forwarding node. When the forwarding node has just forwarded a packet, each of the committee nodes sends a voting message to the forwarding node. By collecting these votes, the forwarding node makes a decision: normal, a PMA, or invalid. Upon detecting a PMA, the forwarding node reports the PMA to the BS. However, OBD has some flaws: First, OBD assumes that the forwarding node is benign. However, the node could be also captured by an adversary, so that the node would not report PMAs to the user. Second, OBD makes every committee node send a vote for each packet. However, in terms of energy saving, this would be inefficient in peacetime.

3 TDMA-Based Detection of Packet Modification Attacks

This section describes the proposed method in detail.

3.1 Assumptions

The proposed method considers a highly-dense WSN consisting of a large number of homogeneous sensor nodes and a BS. These nodes are similar to the current generation of sensor nodes, in terms of computation and communication capabilities, and energy resources. Due to cost constraints, nodes are not equipped with tamper-resistant hardware. Each node has some cryptographic keys shared only with the BS. Due to the broadcast nature of the wireless communications, packets transmitted by a node can be overheard by the surrounding nodes within the transmission range. It is assumed that a lightweight TDMA mechanism, such as [9] or [10], is employed within the network, so that the nodes’ clocks are synchronized locally and loosely.

A malicious adversary can capture a few nodes without being detected. However, the adversary cannot capture a large number of nodes and the BS. The goal of the adversary is to interrupt the delivery of some packets passing through the captured nodes. To prevent being detected, the adversary will try to alter a very small part of each packet; such a minimal alteration would invalidate the integrity of the packet, so that the packet would be ignored at the destination.

3.2 Initial Setup

For the sake of simplicity, hereafter, the basic mechanism of the proposed method is explained with a simple example shown in Fig. 2. Three forwarding nodes $F_{i-1}$, $F_i$, and $F_{i+1}$ along a unidirectional routing path are considered. Once $F_i$ has received a packet $P_{i-1}$ from $F_{i-1}$, the node has to send $P_i$, which is a copy of $P_{i-1}$, to $F_{i+1}$. Due to the broadcast nature of wireless communications, both $P_{i-1}$ and $P_i$ can be overheard by its neighboring nodes that are within the transmission range. The proposed method assumes a highly-dense WSN, so that the number of the neighboring nodes may reach a dozen or more. Among them, $T$ nodes are chosen as the committee nodes of $F_i$, which is a predefined value. In the example, $T = 5$ and nodes $C_1$, $C_2$, $C_3$, $C_4$, and $C_5$ are chosen as the committee nodes of $F_i$. Among the committee nodes, one is elected as the head of the committee (the committee head).
The clocks of the committee nodes are locally synchronized by a lightweight TDMA protocol. A single TDMA round is comprised of \( T + 1 \) TDMA slots; the first one is reserved for the committee head and the others are assigned to the committee nodes. Note that the slot assignment for a committee is a separate issue and beyond the scope. In the figure, the 2\(^{nd} \), 3\(^{rd} \), 4\(^{th} \), 5\(^{th} \), and 6\(^{th} \) slots are assigned to \( C_1, C_2, C_3, C_4, \) and \( C_5 \), respectively. A committee node can transmit packets only within its TDMA slot. For example, \( C_2 \) can transmit a packet only within the 3\(^{rd} \) slot of each TDMA round unless the node is currently the head.

A PMA can be reported to the BS through the following 4 phases.

1. PMA monitoring: The committee nodes of \( F_i \) can overhear any packets transmitted by \( F_{i-1} \) and \( F_i \), so that they can detect PMAs of \( F_i \) by comparing these packets. That is, each of the nodes compares \( P_{i-1} \), which was transmitted by \( F_{i-1} \) to \( F_i \), and \( P_i \), which was done by \( F_i \) to \( F_{i+1} \). Since \( P_i \) must be a copy of \( P_{i-1} \), the contents of \( P_{i-1} \) and that of \( P_i \) must match exactly at network and higher layers (i.e., \( P_{i-1} = P_i \)). If \( P_{i-1} \neq P_i \), the committee considers that \( F_i \) has launched a PMA against \( P_{i-1} \). Once the committee nodes have detected a PMA of \( F_i \), each of them first prepares a draft of a misbehavior report (DMR), which typically includes its ID, the contents informing the detection of the PMA, and a MAC generated over the contents using one of its keys. Since the committee consists of \( T \) nodes, at most \( T \) DMRs can be generated. These DMRs are used in the next phase. Note that some of the committee nodes can be also captured by the adversary, and thus have colluded in the PMA. However, the proposed method is resilient against them unless they account for half or more of the committee nodes.

2. Draft broadcast: In this phase, the committee head broadcasts its DMR, \( DMR_{H_i} \), within the first slot of a TDMA round, to ask the other committee nodes for agreements on reporting the detection of the PMA. Each of them then checks if \( DMR_{H_i} \) addresses the same PMA detected by it. If so, the node generates an agreement message (AM), which typically includes its ID and a MAC generated over the contents of \( DMR_{H_i} \) using one of its keys. These \( T - 1 \) AMs will be
broadcasted and collected by all the committee nodes, excluding the head, in the next phase. The committee head can be also captured by the adversary, and thus have colluded in the PMA. The captured head may not broadcast a DMR or broadcast an incorrect DMR. However, this can be simply detected by the other committee nodes. Once the head’s misbehavior has been detected, the node assigned to the next ‘valid’ slot of the round broadcasts its DMR, $DMR_i (i \neq H)$. $DMR_i$ can be also checked by the remaining committee nodes.

3. Agreement broadcast: In this phase, each of the committee nodes, excluding the node who had broadcasted a ‘legitimate’ DMR in the previous phase, broadcasts its AM within its slot of a TDMA round. Meanwhile, each of the committee nodes, including the head, collects these $T - 2$ AMs, compiles a misbehavior report (MR) that typically includes its ID, the contents of the legitimate DMR, and $T$ MACs: one from the DMR and the others from the AMs. Some of the committee nodes can be also captured by the adversary, and thus have colluded in the PMA. They may not broadcast an AM or may broadcast an incorrect AM. However, unless half or more of them are captured, the majority of the MACs would be legitimate.

4. Report forwarding: In this phase, the committee head forwards its MR, $MR_H$, towards the BS within the first slot of a TDMA round. Since the head can be captured by the adversary, $MR_H$ is verified by the other committee nodes; each of them checks if $MR_H$ and the node’s MR match exactly. If so, $MR_H$ is considered to be legitimate. But if not, or the head broadcasted nothing, the node assigned to the next valid slot of the round broadcasts its MR, $DMR_i (i \neq H)$. Note that $MR_i$ can be also checked by the remaining committee nodes.
Fig. 3. (a) resilience against node capture and (b) energy efficiency.

4 Simulation Results

The performance of the proposed method against PMAs has been also evaluated through simulation. For each forwarding node, 5 nodes were chosen as its committee nodes. Fig. 3(a) shows the percentage of PMAs reported to the user when, for each committee, the committee head was captured by the adversary and the number of captured committee nodes, excluding the head, is between 0 and 2. As shown in the figure, the proposed method (filled rectangles) could make every MR reported to the user unless 3 or more of the nodes in each committee were captured. But OBD (empty circles) could not report any MRs even though all the other committee nodes were benign. Fig. 3(b) shows the energy efficiency of the proposed method. As shown in the figure, the proposed method could save extra energy resources since a committee node needed not send a message to the head in peacetime. But OBD made the node send a message for each packet, which resulted in energy-inefficiency in peacetime.

5 Conclusions and Future Work

In this paper, we proposed a method for the detection of PMAs in homogeneous WSNs. By using the broadcast nature of wireless communications and a lightweight TDMA mechanism, a PMA launched by a forwarding node can be detected by its committee and reported to the user. Unless half or more of the committee nodes are
captured by an adversary, the method guarantees that an MR informing the user of the PMA can be forwarded towards the BS. In contrast to OBD, the proposed method is resilient against captured heads and can save extra energy resources. The performance of the method was shown with the simulation results. We will investigate algorithms for committee selections with the consideration of energy efficiency and security. Also, we will do detection methods that can detect PMAs without the use of TDMA.

References