Available online at www.sciencedirect.com

ScienceDirect

Computer Communications 30 (2007) 2385–2400

computer communications

www.elsevier.com/locate/comcom

Adaptive security design with malicious node detection in cluster-based sensor networks

Meng-Yen Hsieh [a], Yueh-Min Huang [a,*], Han-Chieh Chao [b]

[a] *Department of Engineering Science, National Cheng Kung University, No. 1, Ta-Hsueh Road, Tainan 701, Taiwan, Republic of China*

[b] *College of Electrical Engineering & Computer Science, National Ilan University, 1, Sec. 1, Shen-Lung Road, I-Lan 260, Taiwan, Republic of China*

Available online 29 April 2007

Abstract

Distributed wireless sensor networks have problems on detecting and preventing malicious nodes, which always bring destructive threats and compromise multiple sensor nodes. Therefore, sensor networks need to support an authentication service for sensor identity and message transmission. Furthermore, intrusion detection and prevention schemes are always integrated in sensor security appliances so that they can enhance network security by discovering malicious or compromised nodes. This study provides adaptive security modules to improve secure communication of cluster-based sensor networks. A dynamic authentication scheme in the proposed primary security module enables existing nodes to authenticate new incoming nodes, triggering the establishment of secure links and broadcast authentication between neighboring nodes. This primary security design prevents intrusion from external malicious nodes using the authentication scheme. For advanced security design, the proposed intrusion detection module can exclude internal compromised nodes, which contains alarm return, trust evaluation, and black/white lists schemes. This study adopts the two above mentioned modules to achieve secure communication in cluster-based sensor networks when the network lifetime is divided into multiple cluster rounds. Finally, the security analysis results indicate that the proposed design can prevent and detect malicious nodes with a high probability of success by cluster-based and neighbor monitor mechanisms. According to the performance evaluation results, the proposed security modules cause low storage, computation, and communication overhead to sensor nodes.

Keywords: Sensor network; Dynamic authentication; Alarm return; Trust values

1. Introduction

Distributed sensor networks comprised of many low-energy sensors monitor various environments, such as oceans and wildlife, manufacturing machinery performance, building safety and earthquakes, and many military applications. Homogeneous sensor nodes are often deployed in open and unattended environments without physical protection. Hence, security design is vital for various sensor network applications, because a sensor network is vulnerable to active and passive attacks owing to the wireless nature of link connections among sensor nodes. Many sensor networks in real scenarios are organized hierarchically to lower the energy consumption of communication overhead [3,4,15–17], and to raise network security and connectivity [10–13,40]. However, most security research in cluster-based sensor networks does not mention authentication issues for new incoming sensor nodes, and does not efficiently prevent attacks of compromised nodes. To achieve adaptive security schemes in hierarchical sensor networks, this study proposes *SecCBSN* (*Secure Communications of Cluster-Based Sensor Network*) with three modules to establish secure links and broadcast authentication between neighboring nodes, and to detect and eliminate malicious or compromised nodes from the network.

[*] Corresponding author. Tel.: +886 6 2757575; fax: +886 6 2766549.
E-mail addresses: tab.hsieh@mail.hku.edu.tw (M.-Y. Hsieh), huang@mail.ncku.edu.tw (Y.-M. Huang), hcc@mail.ndhu.edu.tw (H.-C. Chao).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.04.008

Hierarchical sensor networks have cluster heads (CHs), which gather, aggregate, and relay sensed data from localized member nodes (MNs) to a base station (BS). In homogeneous sensor environments, CHs are chosen from ordinary sensor nodes with limited energy. Sensor nodes constitute a hierarchical architecture and work with self-organization management mechanisms to reduce the energy overhead. A well-known cluster-based network, LEACH [10], rotates CHs during different cluster rounds when CHs are specified from homogeneous sensor nodes. Rotating CHs have the advantage of averaging energy consumption among sensor nodes, thus reducing the opportunity for attack. The cluster-based structure is vulnerable to various attacks [23] in which the intruder imitates or compromises CHs. Communication attacks can happen during two phases: one is from MNs to CHs; the other is from CHs to the BS. The SLEACH [21] and SecLEACH [22] provide modified versions of LEACH, supporting secure cluster-based communication protocols with cryptographic protection against malicious attacks. The SLEACH provides CHs-to-BS authentication using simply shared keys. SecLEAH increases MNs-to-CHs authentication using random key pre-distribution (RKP) solutions. However, the two above mentioned security schemes in LEACH cannot resist vicious attacks from compromised nodes. Some sensor nodes with key pre-distribution schemes may not always report their sensed data to the BS due to the lack of secure links shared with neighboring CHs. *SecCBSN* develops a dynamic authentication scheme in which new nodes deployed during network lifetime can establish secure links with their neighboring nodes. This scheme eliminates the security disadvantages of the above mentioned networks. *SecCBSN* also extends the LEACH architecture with security consideration, and equips each node with two network interfaces (NIFs) for different transmission ranges, instead of using adjustable radio in the network interface.

Because of inherent memory constraints, a sensor node cannot store all possible pairwise keys shared with other nodes. Additionally, owing to the lack of post-deployment geographic configuration information, a deployed node is not equipped with the right pairwise keys shared with its neighboring nodes. Hence, key distribution affects the establishment of pairwise keys between sensor nodes, and influences the degree of secure communication in sensor networks. Although key pre-distribution schemes [7] reduce the overhead of key establishment, they do not support network scalability. Random pre-distribution methods (RKP) [18–20] might be appropriate for the designers of sensor networks to consider available storage and security demand. However, the connection availability of neighboring nodes is not absolutely guaranteed. In some research papers [8,9], sensor nodes have to on-line establish pairwise keys between neighboring nodes after they are deployed. However, these methods bring communication overhead because of the flooding of pairwise key requests, and are dangerous for new incoming sensor nodes in open environments without any authentication service. *SecCBSN* combines the establishment of pairwise keys with the proposed dynamic authentication in a primary security module. An authenticated node can share a key commitment for broadcast authentication with its neighborhood in the network.

Many previous security schemes defend against packet forwarding misbehavior [11], produced by compromised nodes or selfish nodes. Compromised nodes not only drop forwarding packets, but also forward fake or duplicated ones. A survey of security issues [1] classifies security schemes into detection and preventive solutions. The detection methods against data dropping include end-to-end feedbacks (ACKs) [27,28,33], watchdog [29], activity-based overhearing [30], admission in neighborhood [31], reputation [32], and probing [33,34]. The preventive methods to avoid data dropping include nuglets [35,36] and data dispersal [37]. A number of studies have focused on intruder-detected and intruder-tolerant schemes [2,22–25]. Related papers [2,24,38,39,43] always adopt trust value and blacklist schemes for discovering insecure locations or compromised nodes. A location-centric sensor network is proposed in [2] to isolate misbehavior and establish trusted routing. This research chooses trusted routes without misbehaving nodes by identifying insecure locations, embedded blacklists, and modified geographic or trajectory routing. The broadcast of blacklists in this research brings the low overhead of control packets, since blacklists are embedded in the headers of routing or data packets, and advertised to the network. A security scheme [24] for distributed denial of service (DoS) attacks has been proposed by limiting the number time of broadcasting routing request packets and blacklists. Although the above schemes use different techniques to discover misbehaving nodes, they both have disadvantages, and are not always suitable for sensor networks. Sensor nodes with limited resources cannot constantly monitor other node behaviors, and report alarms to their base station or neighborhood. A compromised node can return a false alarm, which is difficult to detect. Building effective detection mechanisms to discover compromised nodes will reduce significant overhead in sensor nodes. *SecCBSN* provides an intrusion detection module, consisting of alarm return protocols, trust value evaluation, and black/white lists, to detect and evaluate malicious or compromised nodes.

Two certificates for sensor networks, known as ECC Certificate [5] and TESLA Certificate [4], have been presented. The ECC Certificate is a public-key certificate that is designed for use in constrained sensor networks, due to their small ECC key size. The hybrid authenticated key establishment scheme, proposed in [14], combines elliptic curve cryptography (ECC) and symmetric-key operations to authenticate the identities of sensor nodes, and solve key distribution and resource-constrained problems. However, ECC is not always suitable for all sensor nodes with restricted energy. The TESLA Certificate is a new type certificate that is driven using the TESLA [6] technique. This technique, which does not depend on public-key cryptography, performs entity authentication and achieves asymmetric security properties with low-energy sensor nodes. *SecCBSN* adapts the TESLA Certificate scheme for dynamic authentication in the primary security module, since symmetric cryptography is most applicable to sensor nodes.

SecCBSN is composed of primary security, cluster round, and intrusion detection modules to support secure cluster-based communication in MNs-to-CHs and CHs-to-BS against outside and inside malicious nodes. The key benefits in the design of *SecCBSN* are as follows:

- Self-organization cluster-based sensor networks (Cluster Around): *SecCBSN* adapts the adaptive clustering algorithm of LEACH. In each cluster around, a chosen CH schedules transmission and monitor periods for its members. MNs must deliver sensed data to the BS via CHs in the assigned transmission time period. However, monitoring a CH is the responsibility of localized MNs. Members in a cluster are divided into monitor subgroups to monitor communication in the delivery phase of each cluster round. At the same time, a CH is also a monitor node for its members.
- Dynamic authentication using the proposed *TCert* Certificate: *SecCBSN* allows new incoming sensor nodes, deployed into the network in one cluster round of the network lifetime, to be authenticated by their neighboring nodes in the next cluster round using the proposed certificate technique. Each of the deployed and authenticated nodes shares pairwise keys and a key commitment with its neighboring nodes for establishing trusted relationships. Malicious nodes cannot be authenticated even though they can gain secrets from deployed nodes. Dynamic authentication is performed in the primary security design of SecCBSN.
- Secure MNs-to-CHs and CHs-to-BS transmission: *SecCBSN* employs a few symmetric keys and pairwise keys to authenticate sensed data and node identities in cluster-based communication. Each sensor node has two network interfaces (NIFs) to divide secure transmission between MNs-to-CHs and CHs-to-BS, which can avoid communication collisions through different radio capabilities. An authenticated MN reports sensed data to its CH using their shared pairwise key. A CH reports aggregated data in the end of a cluster round through its individual key shared with the BS. Furthermore, MNs are scheduled with transmission and monitor time in a cluster.
- Compromised node detection and elimination: *SecCBSN* uses an intrusion detection module as an optional security function to detect and eliminate compromised nodes. The module has alarm return protocols over an alarm model. Monitor nodes can return alarm packets to the BS for accusing compromised nodes by the protocols. Alarm packets are issued from monitor nodes through monitor mechanisms. The BS can evaluate any sensor node with a trust value. Evaluated nodes with their trust values are divided to a blacklist (B-LIST) or whitelist (W-LIST). Nodes recorded in the B-LIST will be eliminated not to operate in the network. A W-LIST is organized for a cluster to record candidate MNs with trust values. In the W-LIST, the nodes with high trust values have high priority to join the cluster.

The rest of the paper is organized as follows. Section 2 describes related techniques and composed modules of *SecCBSN*. Section 3 presents that *SecCBSN* equipped with the primary security module can perform basic secure cluster-based communication protocols. Dynamic authentication in the primary security module triggers secure links and broadcast authentication of neighboring nodes. This section also introduces the Transmission/Monitoring scheduling scheme for clustered MNs. In Section 4, the security features of *SecCBSN* are further enhanced by an intrusion detection module to detect and prevent malicious or compromised nodes. *SecCBSN* with the module will perform alarm return schemes, trust value evaluation, and secure cluster-based communication protocols with black and white lists. In Section 5, the contents of security analyzes are examined. This section depicts how to secure *SecCBSN* communication by using the two proposed security modules, and explains monitor mechanisms for that monitor nodes can issue alarm packets. Section 6 evaluates the performance cost of *SecCBSN*, including energy consumption, and computation and communication overhead. Finally, conclusions are drawn in Section 7.

2. System model

This section introduces the related techniques that are applied to the proposed *SecCBSN*. This system includes two adaptive security modules, and a cluster round module to achieve secure cluster-based communication with resilience to malicious or compromised nodes.

2.1. Related techniques

- *Symmetric cryptography:* The most intuitive kind of cryptography involves the use of a secret key known only to the participants of the secure communication. If two participants have agreed on a secret key, they can communicate confidentially over an insecure channel. Each deployed node in this study has an individual key as a shared secret, sharing it with the BS. In this study, neighbor nodes can establish pairwise keys such as symmetric keys.
- *Light-weight certificate:* ECC certificate and TESLA certificate were designed to be used in constrained sensor networks. Their key sizes and amount of energy consumed are smaller than those of public-key based