Ad Hoc Networks 8 (2010) 345–360

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A three-tier framework for intruder information sharing in sensor networks ☆

Bin Tong *, Santosh Panchapakesan, Wensheng Zhang

The Department of Computer Science, Iowa State University, Ames, IA 50011, United States

ARTICLE INFO

Article history:
Received 4 January 2009
Received in revised form 23 June 2009
Accepted 6 October 2009
Available online 13 October 2009

Keywords:
Intruder information sharing
Bloom Filter
Quorum

ABSTRACT

In sensor networks, an intruder (i.e., compromised node) identified and isolated in one place can be relocated and/or duplicated to other places to continue attacks; hence, detection and isolation of the same intruder or its clones may have to be conducted repeatedly, wasting scarce network resources. Therefore, once an intruder is identified, it should be known to all innocent nodes such that the intruder or its clones can be recognized when appearing elsewhere. However, secure, efficient and scalable sharing of intruder information remains a challenging and unsolved problem. To address this problem, we propose a three-tier framework, consisting of a verifiable intruder reporting (VIR) scheme, a quorum-based caching (QBC) scheme for efficiently propagating intruder reports to the whole network, and a collaborative Bloom Filter (CBF) scheme for handling intruder information locally. Extensive analysis and evaluations are also conducted to verify the efficiency and scalability of the proposed framework.

1. Introduction

Due to unattended deployment environment and absence of tamper resistance, sensor networks are vulnerable to various attacks. In response, schemes have been proposed to identify intruders (i.e., compromised nodes) misbehaving in routing [2], localization [3], and other scenarios [4,5]. Once an intruder is identified, it is isolated by its detectors. However, this is inadequate. Nodes other than these detectors should also be aware of the intruder; otherwise, the intruder can be relocated or duplicated to other places to continue attacks.

To share intruder information with all sensor nodes, the detectors may generate and flood intruder reports to the whole network, directly or through trusted membership servers; other nodes receive and record the reports to maintain their knowledge of intruders. This approach, however, has following security and performance issues: (I.1) Intruders may fake false reports to revoke innocent nodes or repeatedly broadcast false reports to drain network resources; although trusted membership servers can be used to filter false reports, these servers may become attractive targets of attacks. (I.2) If the network scale is large and/or the network needs to operate for a long time (e.g., the network is deployed for long-term surveillance in a hostile area) and hence requires a large number of sensor nodes be deployed to accomplish a long network lifetime, the potential number of compromised nodes is also large, which may result in frequent flooding of intruder information even without fake reports. (I.3) If the number of intruders is large, maintaining an intruder list in each node may cause high storage overhead. To the best of our knowledge, there has not been any secure, efficient and scalable solution reported in the literature that can deal with all the above issues.

To address the intruder information sharing problem, we propose three schemes in this paper: (S.1) a verifiable

☆ The preliminary version of the work appears in IEEE SECON 2008 [1].

* Corresponding author. Tel.: +1 515 441 1702.
E-mail addresses: tongbin@cs.iastate.edu (B. Tong), santosh@cs.iastate.edu (S. Panchapakesan), wzhang@cs.iastate.edu (W. Zhang).

1570-8705/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2009.10.001

intruder reporting (VIR) scheme, which distributedly generates intruder reports that are verifiable by any node, and can prevent malicious nodes from arbitrarily accusing innocent nodes unless the majority number of neighbors of an innocent node have been compromised; (S.2) a quorum-based caching (QBC) scheme, which efficiently propagates intruder information through caching intruder information in elected nodes and infrequently updating the information throughout the network; and (S.3) a collaborative Bloom Filter (CBF) scheme, which consumes only small storage space at each node and meanwhile leverages localized collaboration to enable accurate identification of intruders.

To facilitate the execution of the above three schemes and also to integrate them together, we further propose a framework that contains three tiers of interacting entities: a dedicated membership server (DMS) on the top tier, connecting to the network occasionally at random places to avoid being tracked and attacked; a small number of sensor nodes on the second tier, acting as temporary intruder information caches (IICs); and other ordinary sensor nodes on the bottom tier. Extensive analysis and simulations are conducted to evaluate the efficiency and scalability of the proposed solution.

In the following: Section 2 surveys relate work. Section 3 presents the system model. Section 4 provides an overview of the proposed framework, which is followed by description, analysis and evaluation of VIR, CBF and QBC in Sections 5–7, respectively. Section 8 discusses possible attacks on the proposed framework and countermeasures against these attacks. Finally, the paper concludes in Section 9.

2. Related work

There exist tons of intrusion detection and intruder identification systems [6–9] for traditional wired or mobile ad hoc networks. However, none of them can be directly applied to sensor networks because sensor networks cannot afford the resources required by these schemes. For instance, SWATT [9] requires the verifier to keep the memory content of the verified node, which may be infeasible given constraint storage in sensor nodes. Consequently, researchers have been attracted to develop intruder detection and identification schemes that are suitable for sensor networks, which results in a number of schemes [10,7,11]: For example, Parno et al. [7] proposed two schemes for detecting node replication attacks, and both of the schemes are probabilistic solutions. Ye et al. [11] proposed schemes for identifying malicious nodes that inject bogus traffic into the network. However, these works either do not address how to disseminate intruder information or simply broadcast intruder information after intruders are identified. Without intruder information dissemination, intruder detection and identification schemes have to be run again and again when intruders are relocated or duplicated. On the other hand, simple broadcast of intruder information will cause performance issues (I.1–I.3) in Section 1.

Researchers [12,13,10] have also proposed schemes for intruder revocation and membership management in mobile ad hoc networks. Yang et al.'s [12] solution requires each node to maintain a same list of malicious nodes. In other words, all the nodes have the same opinion regarding maliciousness, and thus a revoked node is completely isolated from the rest of network. On the other hand, the other two solutions [13,10] allow each node to maintain its own rating on other nodes, and deal with them accordingly. However, these schemes require each node to maintain a complete list regarding malicious nodes, which is prohibitive in a sensor network due to the energy and storage constraints.

Recently, Zhang et al. [14] proposed a distributed access control scheme in sensor networks. In the work, a user needs to spend tokens purchased previously in order to gain access to the network. To prevent token reuse, any spent token should be disclosed to all sensor nodes. The authors proposed four different dissemination schemes for used tokens, which shares similarity with our proposed QBC scheme. However, significant differences also exist between these schemes and our QBC scheme: first of all, their first scheme uses network-wide flooding and thus has the performance issues of (I.2) and (I.3) as discussed in Section 1, which do not exist in our proposal. Secondly, with their other three schemes, whenever a token is spent, a request should be sent out to determine whether the token is used or not, and the request may travel a long path. This may incur a large communication overhead. But in the QBC scheme, a large portion of intruder information is stored locally at each individual sensor node, and thus in most cases intruder queries can be answered locally.

In order to reduce the storage space taken at each sensor node for storing intruder information, the proposed CBF scheme adopts the Bloom Filter data structure. Bloom Filter has been adopted in broadcast authentication in sensor networks [15]. Our CBF scheme extends the basic Bloom Filter scheme, and proposes a new application of Bloom Filter in the context of intruder information sharing.

Our scheme uses the Merkle hash tree structure for verification of intruder report. Merkel hash tree has seen applications in a number of security schemes for sensor networks. The examples include data aggregation [16], broadcast authentication [15], and countermeasures against mobile sink compromise [17].

3. System model

3.1. Network assumptions

We consider a sensor network composed of a network controller and a large number of densely-deployed resource-constrained sensor nodes. The controller connects to the network every now and then at arbitrary positions (i.e., it need not be connected to the network at all the time or be at a fixed place). In addition, the network has the following features: (i) All sensor nodes are loosely time synchronized. (ii) Each sensor node knows its own location (via GPS based or non-GPS based localization schemes). (iii) The network needs to operate for a long time and is composed of static nodes, mobile sensor nodes, or a mixture of static or mobile sensor nodes. Mobile sensor nodes