Computer Networks 108 (2016) 210–222

Contents lists available at ScienceDirect

Computer Networks

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

Imposter detection for replication attacks in mobile sensor networks

Tassos Dimitriou[a], Ebrahim A. Alrashed[b,*], Mehmet Hakan Karaata[b], Ali Hamdan[b]

[a] Computer Technology Institute, Greece
[b] Department of Computer Engineering, Kuwait University, Kuwait

ARTICLE INFO

Article history:
Received 17 December 2015
Revised 13 July 2016
Accepted 22 August 2016
Available online 30 August 2016

Keywords:
Mobile sensor networks
Imposter detection
Node replication attack
Wireless network security
Node revocation
Soundness & completeness

ABSTRACT

In a node replication attack, an adversary creates replicas of captured sensor nodes in an attempt to control information that is reaching the base station or, more generally, compromise the functionality of the network. In this work, we develop fully distributed and completely decentralized schemes to detect and evict multiple imposters in mobile wireless sensor networks (MWSNs). The proposed schemes not only quarantines these malicious nodes but also withstand collusion against collaborating imposters trying to blacklist legitimate nodes of the network. Hence the completeness and soundness of the protocols is guaranteed. Our protocols are coupled with extensive mathematical and experimental results, proving the viability of our proposals, thus making them fit for realistic mobile sensor network deployments.

1. Introduction

A *Wireless Sensor Network* (WSN) is a wireless network of small sensors deployed in a specific area to sense various aspects of the environment. A *Mobile Wireless Sensor Network* (MWSN) is a special type of WSN in which sensors are mobile. MWSNs convey the sensed data to base stations or sink nodes, which can be either static or mobile, thus trying to cope with rapid topology changes that make sensing problematic in ordinary sensor networks. As a result, they extend the number of applications for which static (WSNs) are used [1]. Sensors can be attached to people for health and physiological monitoring, to animals in order to track their movements and their feeding habits, or to unmanned aerial vehicles (UAVs) for surveillance, environmental mapping and control [2,3].

In a typical WSN, where the sensor nodes are stationary, the sink or other nodes can ascertain the authenticity of a sensor node by tying its identity to its *claimed* geographic location [4]; through the help of witness nodes, location claims coming from conflicting areas in the network indicate the existence of a replication attack.

In a MWSN, however, the constant movement of nodes makes location-based detection a nearly impossible task. As a result, an adversary can assume the identity of a legitimate node and use it to communicate with the rest of the network. As sensor nodes are not tamper-resistant devices [5], the adversary can create *replicas* of nodes after compromising a node and replicating its cryptographic or other material. We refer to such replicas as *imposters* if they use the identity of existing sensor nodes to communicate with the sink or other nodes of the network.

Since the credentials of replicated nodes do not differ from those of legitimate ones, there is no easy way to distinguish between the two, thus making imposter detection a very difficult process. This type of attack, which is known as *node replication attack* in the literature, has important repercussions in wireless sensor networks security: by assuming a false identity, an imposter can send misleading information, replay old packets which could bias aggregation results or enable other types of attacks in the network, like selective forwarding, sinkhole attacks, etc. [6–8].

Contributions. In this work, we address the problem of node replication attacks by proposing a number of lightweight, *decentralized* protocols to detect imposters in MWSNs. Contrary to prior work that focuses only on imposters that can replicate only a *single* node ID, our schemes work even in those cases where imposters have assumed the identities of *different* nodes. This case is more challenging as it poses another problem: imposters can *frame* legitimate nodes, thus resulting in their dismissal from their network.

In this work, we show not only how to detect these powerful imposters but also maintain the number of false-positives (evictions of legitimate nodes) to a bare minimum. Eventually, when a sensor node is identified to be an imposter, it is prevented from communicating with other nodes in the network by means of an effective quarantining mechanism. Hence our protocols are both sound and complete. Finally, through extensive simulations, we

* Corresponding author.
E-mail address: dr_ebrahim@mac.com (E.A. Alrashed).

http://dx.doi.org/10.1016/j.comnet.2016.08.019
1389-1286/