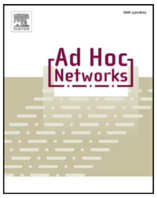
Ad Hoc Networks 37 (2016) 140–152

Contents lists available at ScienceDirect

Ad Hoc Networks

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



A mobility optimized SPRT based distributed security solution for replica node detection in mobile sensor networks

Venkatesh Manickavasagam[a], Jayashree Padmanabhan[b,*]

[a] *School of Computer Science, Carnegie Mellon University, Pittsburgh, USA*
[b] *Department of Computer Technology, Anna University, MIT Campus, Chennai -600044, India*

ARTICLE INFO

Article history:
Received 17 April 2013
Revised 19 November 2014
Accepted 19 August 2015
Available online 28 August 2015

Keywords:
Clone attack
Mobile sensor networks
Replica detection

ABSTRACT

Sensor networks are normally deployed in uncontrolled environments which may result in an adversary compromising a small number of nodes and making identical replicas of the same. This allows the attacker to launch a variety of attacks on the network, having compromised only a few nodes. Several replica detection schemes have been proposed in the literature for static sensor networks. However these schemes cannot be extended for mobile sensor networks, as they rely on static sensor locations. For mobile sensor networks, few solutions have been proposed but they are either centralized approaches or burden the network with high communication and other overheads. We propose a distributed scheme, optimized by nodes' velocities, using the Sequential Probability Ratio Test. Leveraging the intersection of message transmission paths, it can handle high mobility while at the same time guarantee uniqueness for each node without the involvement of the base station. Moreover, this scheme does not use explicit packets for the purpose of detecting replicas. Instead the periodic data packets transmitted by the sensor nodes are used. The system overheads are also reasonable and node velocities improve the system performance rather than diminish it.

1. Introduction

Autonomous mobile wireless sensor networks are used for a variety of applications [1–3] including aquatic applications, detection of intruders, border monitoring and target tracking. Each sensor node in the wireless sensor network, interacts with other sensor nodes, performing useful tasks such as static sensor deployment, network repair and event detection [4]. In malevolent environments, a small number of nodes may be captured by an adversary, and these captured nodes may be used to launch a series of attacks ranging from Denial of Service attacks,impersonation and eavesdropping.

In this paper, a particular scenario called the clone or replica node attack [5] is presented. In clone or replica node attacks, the adversary captures a node stealing all the confidential unique identifiers from it, and creates several replicas which share the same identifiers. Since a wireless sensor network is usually left unattended after being deployed due to cost constraints [5], capturing a sensor node becomes an easy task [6,7] making it vulnerable to a range of attacks [8]. The attack is considered dangerous as the adversary can compromise as few as a single node and generate several replicas with the same ID. The number is limited only by the hardware he has to generate them. The replicas need not posses the same physical characteristics as the victim node nor does it have to follow similar movement patterns. The adversary requires knowledge of only the unique identifiers and protocols required to communicate in the network, which are all available in the compromised node.

An adversary would prefer generating a large number of replicas from capturing a small set of nodes, than capturing an equal number of nodes. This is because the time and effort required to generate replicas is much lesser. Possessing

[*] Corresponding author. Tel.: +91 9444024463.
E-mail address: pjshree@annauniv.edu, pjshree12@gmail.com (J. Padmanabhan).
URL: http://www.annauniv.edu/dct/index.html (J. Padmanabhan)

http://dx.doi.org/10.1016/j.adhoc.2015.08.010
1570-8705/© 2015 Elsevier B.V. All rights reserved.

the unique identifiers of the original node, the replicas impersonate it throughout the network. They will be able to encrypt, decrypt and authenticate messages just like the captured node, thus bypassing secure communication protocols.

The adversary can take advantage of the replicas in a variety of ways. He could jam signals from benign nodes or pass fake data to damage or mislead the system. Alternatively, the adversary can simply eavesdrop on the network and monitor its data. He could even go to the extent of disturbing protocols like data gathering, data aggregation, routing and cluster formation. Thus by compromising only a few nodes, an adversary can defeat the purpose of the sensor network.

An intuitive solution to stop replica attacks would be to protect the unique identifiers from being stolen. However, such physical shielding of nodes is avoided due to cost and other constraints. Even if the hardware is designed to resist stealing of the unique identifiers, it may still be possible for an adversary to bypass such mechanisms and in doing so, not only the compromised node but the entire network is at stake. It is therefore necessary to provide solutions assuming any secret data stored in a node can be stolen when captured.

Motivated by the increasing number of mobile sensor network applications, we propose a replica detection scheme optimized for mobility. As opposed to existing systems, the performance of the scheme increases with increase in node velocities (please refer Section 4.1). It is based on the idea that when several replicas transmit simultaneously, multiple messages with the same source *ID* but physically different sources are alive in the network. To exploit this fact, a sequence appendix is attached to every transmitted message to provide a sort of message ordering. When a forwarding node encounters an out of order message, it is possible that those messages came from different physical sources with the same network ID(replicas). The probability of messages from the same source genuinely arriving out of order [9], happened to be significantly lesser than when they were transmitted by replicas. However making decisions from only one such observation may result in a lot of false detections. To provide upper bounds for the rates of error, we collect a sequence of observations and allow the Sequential Probability Ratio Test [10] to make a decision from them. The SPRT is a hypothesis testing technique which is used to provide upper bounds for the false positive and false negative rates.

We support the efficiency, robustness and scalability of the proposed schemes through several theoretical and experimental evaluations. We analyze the attacker's risk of being detected and found that the results were similar to the birthday paradox. We prove that the system is robust to attempts of evasion by the attacker. First, we show that if the attacker synchronizes his replicas, their impact on the network will be constant with respect to the number of replicas produced. Another evasion technique, using the network's topology information, which could be employed by the attacker is also investigated and its infeasibility is proved. Through experiments, we validate the system's scalability in terms of the number of nodes and its robustness in terms of the node velocities. It has also been shown and proved that the network administrator can provide an upper bound for the false positive and false negative rates.

The rest of the paper is organized as follows: Section 2 states the network model for which the system is designed, Section 3 describes the proposed Mobile Replica Detection scheme, Section 4 performs security and performance evaluation, Section 5 calculates the system overheads, Section 6 describes the experiments performed, Section 7 describes the related work in the domain of the proposed system and compares with the same and Section 8 concludes the work.

2. System model

In this section, we describe the network model and the method the adversary uses to launch the attack. These were the models used to test and evaluate the proposed scheme.

2.1. Network model

We assume that the nodes are deployed in a two dimensional field and they are able to roam freely throughout the field, where some or all of the nodes have mobility capabilities. Every node i in the network is assigned a unique ID, ID_i. The scheme does not require the nodes to know their locations nor does it require them to have their clocks synchronized.

2.2. Adversary model

We assume that an adversary can compromise a small fraction of the nodes [7]. On compromising a node p, the adversary can steal any information from it including its ID, ID_p, and private cryptographic materials. He then creates a set of replicas $p_d = \{p_1, p_2, \ldots, p_r\}$ which share the same ID and cryptographic materials as p. These replicas can sign, encrypt and decrypt messages just like the original node which makes it impossible for the other nodes to verify its authenticity. The replicas are controlled by the adversaries and can communicate with each other at any time through another channel not used by the network. Having compromised a node, there is no limit to the number of replicas the adversary can generate and the damage caused to the network is normally proportional to the number of replicas. The adversary will try his best to protect his replicas.

We also assume that the adversary cannot generate new valid IDs which can be used for the replicas. He will also not be able to control or view what is stored in nodes which have not been compromised yet.

3. Mobile replica detection

In this section, we present a distributed network layer solution for replica detection in mobile sensor networks. The schemes used for detecting replicas in static sensor networks [5,11–14] cannot be extended to mobile scenarios as they revolve around the use of location claims which can be used to uniquely identify a node in the network. However, in the mobile environment the location of a node cannot be used to identify it. Although [15] presents a solution for mobile sensor networks, it holds several drawbacks (please refer Section 7). Table 1 provides a list of the notations frequently used in the following text.

Every packet sent by a sensor node is attached with a sequence appendix, details of which is described in Section 3.2. Every intermediate node and the destination node verifies