Journal of Network and Computer Applications 61 (2016) 21–32

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

A comparative analysis of node replica detection schemes in wireless sensor networks

Alekha Kumar Mishra*, Ashok Kumar Turuk

Department of Computer Science and Engineering, NIT Rourkela, Rourkela 769008, Odisha, India

ARTICLE INFO

Article history:
Received 18 October 2014
Received in revised form
14 June 2015
Accepted 5 December 2015
Available online 17 December 2015

Keywords:
Wireless sensor network
Security
Node replication attack
Replica detection

ABSTRACT

Wireless sensor networks are exposed to various kinds of security threat. The node replication attack is application-independent and can be launched by an adversary just by capturing a single sensor from the network. The post-capture impact of this attack is serious as an adversary can launch various insider attacks with the help of replicas that are deployed in the network. Counter-measures for node replication attack have drawn the attention of many researchers in this field. The first step towards handling a node replication attack is to detect the existence of replicas and remove them from the network. A number of replica detection schemes have been proposed in the literature. However, only a few survey articles exist based on replica detection schemes. Most of these survey lacks comparative analysis on the existing schemes, and are limited only to a few referred schemes. In this paper, we have classified the existing replica detection schemes considering a higher number of parameters than the existing schemes, and highlighted advantages and disadvantages of the contributions. A detailed comparative analysis of the existing schemes are made based on their communication cost, message overhead, storage requirement, and number of replica detectors per node. We have simulated a few mostly referred detection schemes using Castalia and analysed their performance in terms of detection probability, average number of packets sent/received, detection time, and energy consumption.

Contents

* Corresponding author.
E-mail addresses: alekha@gmail.com (A.K. Mishra), akturuk@nitrkl.ac.in (A.K. Turuk).

http://dx.doi.org/10.1016/j.jnca.2015.12.001
1084-8045/

1. Introduction

Wireless sensor networks (WSN) (Zungeru et al., 2012; Rezazadeh et al., 2012; Tanwar et al., 2015) provide a low-cost, efficient, and feasible solution for remote-monitoring applications. A WSN consists of a large number of tiny sensor nodes that are deployed in higher density around or inside the target area to acquire data. Each node senses and transmits the processed data to a dedicated node, which is commonly known as base station (BS). Unlike sensor nodes, BS has abundant resources and higher computational capability. Applications of WSN include healthcare, military, habitat monitoring, traffic monitoring, rehabilitation and many more (Buratti et al., 2006; Sohraby et al., 2007; Hadjidj et al., 2013).

Sensor nodes are exposed to unattended and sometime unknown environment. In such environments, sensor nodes are susceptible to various kind of security threats such as hello flooding, sybil, wormhole, node replication attack, etc. Claycomb and Shin (2011), Modares and Salleh (2011). Among these security threats, node replication attack is of major concern in WSN (Yu et al., 2012; Huang and Teng, 2014). In node replication attack, an adversary can reprogram a captured node, and generate a number of replicas to be deployed back into the network. Moreover, node replication attack also provides a scope for the adversary to launch other insider attacks in the network (Zin et al., 2014). In this attack, a replica has the identity of a genuine node and participates in all the network activities. One of the solution to overcome the node replication is to deploy tamper-resistant nodes. But, the deployment of tamper-resistant nodes are cost prohibitive (Karlof and Wagner, 2003; Wang et al., 2006). Therefore, detection of replica is the most efficient way to handle node replication attack.

Though, there are many kind of replica detection schemes reported in the literature, only a few number of surveys on node replica detection are available. Recently published works include the articles by Xie et al. (2011), Zhu et al. (2012), and Khan et al. (2013). However, the above articles lack a comprehensive analysis of the existing node replica detection schemes. Xie et al. (2011) have focused mainly on anomaly detection in WSN. Zhu et al. (2012) and Khan et al. (2013) have discussed various replica detection techniques. However, we found that their survey lacks the following: (i) inclusion of a larger number of detection schemes, (ii) critical analysis of communication complexity and storage overhead, (iii) classification of replica detection schemes using various parameters, and (iv) performance evaluation through simulation.

In this paper, we have made a comprehensive survey of node replica detection schemes reported in the literature. Our contributions to this paper are as follows: (i) The existing schemes classified not only based on detection types such as centralized, distributive, etc., but also using additional parameters such as geographical location dependency, claim-forwarding strategy, and message routing type; (ii) a critical analysis is presented on the communication, storage, and message overhead of each scheme, and (iii) a few detection schemes are simulated and their performance is compared. The metrics considered for the evaluation are: detection probability, average number of packets sent/received, energy consumption, and detection time.

The rest of the paper is organized as follows: classification of existing schemes and discussion of their detection techniques are given in Section 2. Analysis of the detection schemes is performed in Section 3. Comparison of a few detection schemes through simulation is made in Section 4. Finally, the conclusion and future work are presented in Sections 5 and 6 respectively.

2. Replica detection schemes

In this section, first we explain the classification of existing schemes based on various characteristics such as detection type, claim forwarding strategy, etc. Next, we briefly discuss the existing