Computers and Electrical Engineering 000 (2017) 1–15

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Unique identity and localization based replica node detection in hierarchical wireless sensor networks☆

T.P. Rani[a,b,*], C. Jayakumar[c]

[a] Department of Information Technology, Sri Sai Ram Engineering College, Anna University, India
[b] Department of Information and Communication Engineering, Anna University, India
[c] Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Chennai, India

ARTICLE INFO

Article history:
Received 30 January 2016
Revised 12 August 2017
Accepted 15 August 2017
Available online xxx

Keywords:
Replication attacks
Cloning attacks
Intrusion detection
Sensor network security
Wireless sensor network

ABSTRACT

Clustering in Wireless sensor networks (WSN) is a prevalent Hierarchical network management technique. Though disjoint clusters are generally preferred, overlapping clusters find its prominence in some applications of inter-cluster routing, time-synchronization and node localization. Replica node detection is a major challenge in overlapping clusters. This paper aims at replica node detection in overlapping clusters based on two methods, Replica detection based on RFID (RDBRFID) and Replica detection based on Localization techniques (RDBLT). The first method uses RFID for unique node identification and the second method detects replica by identifying its locality based on received signal strength (RSSI) and Triangulation method. These methods are implemented and their performance is compared with Multicast and non clustered methods: Randomized multicast (RM), Line selected multicast (LSM), Fault tolerant virtual back bone tree (FTVBT) and K-coverage WSN. It is observed that RDBRFID exhibits better detection rate and lesser communication overhead due to its deterministic approach.

1. Introduction

A wireless sensor networks (WSN) is a group of specialized autonomous sensors or sensor node with communication framework. They are deployed to monitor and record any physical or environmental conditions at diverse locations. Commonly monitored parameters are temperature, humidity, pressure, illumination intensity, pollutant level, vibration, sound, and voltage. The architecture of WSN may be a partial peer to peer system (P2P) or clustered system. In partial P2P systems, nodes are peers which have similar type of operations and simple configurations [1]. In clustered systems, all the nodes within clusters are peers and they communicate to their cluster heads [2]. These cluster heads are elected among the peer nodes through election algorithms, and all the nodes take their turn, to be elected as a cluster head, in order to avoid a single node being encumbered. The final communication is towards a Base station, which is a powerful system like a laptop or an Access point. The un-tethered and openness of sensor network invites various types of attacks [3]. Due to the cost involved in deploying redundant number of nodes, the attack counter measures are not included physically into the single node architecture. The security attacks are broadly classified as Application Dependent and Application Independent attacks. Replication attack is a type of Application independent attack in WSN [3].

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. M. S. Kumar.

* Corresponding author.
E-mail address: rani.it@sairam.edu.in (T.P. Rani).

http://dx.doi.org/10.1016/j.compeleceng.2017.08.010
0045-7906/

Replication attack is an attempt by an adversary in which one or more nodes are compromised or added into the network and these nodes have the same id as another node in the network. It is also known as clone attacks [4]. An attack similar to replication attack is Sybil attack [5]. In Sybil attack, a node gains multiple ids of many nodes and launches an attack. Replication attack is also treated as an intrusion and is detected using intrusion detection method (IDS) [6]. Node behaviors are monitored in IDS of WSN for corresponding applications and misbehavior or anomalous activities are identified.

The paper is organized as follows. The related works on replica node detection is discussed in Section 2. The proposed system is explained in Section 3. The background requirements of the proposed method and assumptions of the adversary are discussed in Sections 4 and 5. The proposed system implementation is explained in Section 6. The algorithm analysis is made available in Sections 7 and 8. The simulation results and conclusion is given in Sections 9 and 10.

2. Related works

The replication detection methods are broadly classified as network based and radio signal based [3]. The radio signal based detection methods take into account of the radio signal strength indicator (RSSI) or the radio finger print based on the received signals to detect the node replications in WSN [7]. This method cannot be used in hostile environments and geographically widespread WSN [8]. The networks based detection methods are classified as static based and mobile based. Static based detection methods and mobile based methods are further classified into centralized and distributed methods.

2.1. Static centralized detection

Nodes of WSN do not move after deployment in static networks. In centralized detection methods, powerful base station plays the major role in decision making. The various detection methods of static centralized methods are given in the following section. The foremost method in Static centralized method is the straight forward method [3].

2.1.1. Straight forward method

If a node makes a location claim other than its intended location it is declared as a replicated node. It can simply be stated, as in this technique, that if there are more than two location claims for a node, it is a replicated node. It suffers from the drawbacks of a centralized system. A single base station processing all information might lead to single point of failure and be a bottleneck. The nodes near the base station also get overloaded as they serve as hotspot serving the base station.

2.1.2. SET

The system is based on Set operations (intersection and union), on exclusive subset of a network [3]. It collects data about neighbors in a distributed manner and the set operations on a random group of nodes are performed at the base station. The system claims to reduce overhead in comparison with RM and LSM [4]. But both RM and LSM are distributed systems and hence such a centralized method offering a trade off on availability for overhead may need more consideration in this regard.

2.1.3. Key usage based system

The method is based on random key pre-distribution [9]. If a node wants to communicate with neighboring nodes it must authenticate itself and establish a connection using a key. If there are replicated nodes and if they use the node credentials to communicate with their neighboring nodes, the key usage will be high. The key usage will be monitored randomly by the base station using counting bloom filters. The system is based on usage of keys. But if a replicated node doesn't authenticate and communicate with neighboring nodes because of its intention to monitor the network traffic (a passive attack) initially and launch a massive active attack, the system may be unable to detect it.

2.1.4. Social finger print

In a static network the neighborhood of a node is fixed. This phenomenon of neighborhood community fingerprint is maintained by the base station [3]. Periodically the nodes send their id (id_α) with their finger print which can be formed only from neighborhood nodes authenticated messages. The system claims that though there is overhead in communicating with neighbors to get the finger print formed, detection is accurate. The system also claims to be partially centralized as the node verification can be done with neighbor nodes or at the base station or by both. The static distributed detection methods overcome the drawback of the base station bottleneck. The overhead at the base station and the hot spot will be prevalent even when there are no attacks. This provokes the need for a distributed method.

2.2. Static distributed detection

2.2.1. Straight forward method

The aforementioned straight forward method can be decentralized and it is made available as a distributed algorithm, where neighboring nodes perform replicated node detection [10]. But if the replicas do not share common neighbors, the system may be unable to detect it.

Please cite this article as: T.P. Rani, C. Jayakumar, Unique identity and localization based replica node detection in hierarchical wireless sensor networks, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.08.010