A Low-Power Detection System for Wireless Sensor Networks

Ardalan Forootaninia
Dept of IT, Tehran University, Kish International Campus
Kish, Iran
Forootaninia@ut.ac.ir

M. B. Ghaznavi-Ghoushchi *member IEEE*
School of Engineering, Shahed University
Tehran, Iran
Ghaznavi@shahed.ac.ir

***Abstract*—Wireless networks are increasingly spanning the globe and so the security and privacy of these networks are of great importance. Sensor networks have their own vulnerabilities so, preventing intrusions and detecting them has become one of the most challenging issues. In this paper, we propose an approach to implement a hierarchical intrusion detection system. In this model, the network is divided into smaller units called cells and the intrusion detection program is installed on each cell representative. The main purpose to present this model is to reduce the power consumption as a key factor for increasing the lifetime of sensor nodes. In addition, an improved watchdog technique is proposed for detecting malicious nodes. This technique resolves common problems in watchdog mechanism. The proposed hierarchical model has been implemented in Tiny-OS environment and the results indicate that, our proposed model is better in performance than the original models and it has increased the lifetime of the wireless sensor nodes by around 5370 seconds for a network with 200 sensors.**

Keywords—Wireless Sensor Networks, Intrusion Detection System, Hierarchical IDS, Watchdog, Low-Power, Sensor life time.

I. INTRODUCTION

Intruding into a network refers to any activity which endangers the integrity, confidentiality and accessibility of a source and an Intrusion Detection System (IDS) is a system which detects Intrusion activities [1]. The main idea of developing intrusion detection systems came from examining the behavior patterns of ordinary users and identifying the abnormal behavior patterns of the users. An IDS which operates statistically demonstrates the network traffic like radar and detects any signal which may indicate an abnormal event or attack to the network [2].

So far, different techniques have been proposed for intrusion detection in wireless sensor networks (WSNs). In the following sections some of them are discussed.

In [3] and [4] a new technique has been proposed for identity authentication in wireless sensor networks in an interleaved manner which is called Interleaved Hop-By-Hop authentication (IHOP). IHOP guarantees to indentify all incorrect packets injected into the network. In the method [3], the wireless sensors networks are organized hierarchically and in clusters. The cluster in upper hierarchy creates a route for connection to base station and each interface node reaches a node connected to its upper level and also a node connected to its lower level. In IHOP an upper cluster collects the information related to identity authentication from its members (subordinates) and sends it to the base station in form of a report. This reporting occurs only when at least 1+t sensor observes similar results. This paper does not show how the t parameter should be adjusted to sensor network. However, IHOP guarantees that the base station will identify the incorrect packets (when more than t nodes did not agree to cooperate).

Another method [4] proposed route filtering using statistical methods which can identify and delete incorrect data. In this method, there is a key extensive pool and each sensor is allocated a part of this pool. Whenever a move in the region begins, the sensors identify this move and one of the nodes as the base station checks all the network addresses and filters all the reports en route conveying the address incorrectness. However, as mentioned in [5], this method is used for protecting the network against incorrect information injection and cannot drive away the attacks such as selective forwarding.

Also, another approach [6] was proposed based on a routing called INSESN (Intrusion-Tolerant Routing in Wireless Sensor Networks) in which the sensors collect the information related to regional typology and send it to the base station. Afterwards, the base station creates the routing table according to the collected information and sends it to the related sensors. The base station is the main control point for creating the routing table which reduces the nodes computational load. Although INSENS has been developed by a protocol based on routing table, these are base stations which collect all the information and create the routing table for each sensor. However, INSENS is not suitable for large sensor networks [6].

During the recent years, intrusion detection based on the statistical techniques has been widely under the spotlight. For example [7], uses data analysis techniques (such as clustering and neural networks [8]) using the data available