AN IMPROVED WATCHDOG TECHNIQUE BASED ON POWER-AWARE HIERARCHICAL DESIGN FOR IDS IN WIRELESS SENSOR NETWORKS

A. Forootaninia[1] and M. B. Ghaznavi-Ghoushchi [2*]

[1] Department of IT, Tehran University, Kish International Campus, Iran
forootaninia@ut.ac.ir
[2] School of Engineering, Shahed University, Tehran, Iran
ghaznavi@shahed.ac.ir (*Corresponding Author)

ABSTRACT

Preserving security and confidentiality in wireless sensor networks (WSN) are crucial. Wireless sensor networks in comparison with wired networks are more substantially vulnerable to attacks and intrusions. In WSN, a third person can eavesdrop to the information or link to the network. So, preventing these intrusions by detecting them has become one of the most demanding challenges. This paper, proposes an improved watchdog technique as an effective technique for detecting malicious nodes based on a power aware hierarchical model. This technique overcomes the common problems in the original Watchdog mechanism. The main purpose to present this model is reducing the power consumption as a key factor for increasing the network's lifetime. For this reason, we simulated our model with Tiny-OS simulator and then, compared our results with non hierarchical model to ensure the improvement. 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 2611.492 seconds for a network with 100 sensors.

KEYWORDS

WSN, Intrusion Detection System (IDS), Watchdog, Improved Watchdog, Low-Power, Hierarchical Model

1. INTRODUCTION

The recent progresses in electronics and wireless telecommunication allow us to design and develop sensors with low consumptive power, small size, and reasonable price for various applications. These small sensors are able to receive different environmental information (based on the sensor type), process and transmit them.

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 IDS came from examining the behavior patterns of ordinary users and identifying the abnormal behavior patterns of the users. Intrusion detection system 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].

Establishing security in wireless sensor networks due to its changing nature and non-concentrated typology has increased the vulnerability in these networks. Moreover, as a result of energy limitations in wireless sensors, the consumptive power has always been a challenging issue to be considered in designing these wireless sensor networks. In spite of the high volume of researches and studies which tried to propose an efficient intrusion detection system, none of