Advances in Electrical and Telecommunication Engineering (AETE)

AETE is a peer review journal of the Department of Electrical & Electronics Engineering, Ambrose Alli University, Nigeria

Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks

Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G. & Ajao, L. A.

Department of Computer Engineering, Federal University of Technology, Minna, Nigeria

agajojul@gmail.com

ARTICLE INFO

Article history:

Received 30 April 2018

Accepted 29 May 2018

Published 31 May 2018

Keywords:

Energy level

Intrusion detection system

Network performance

Trust value

Wireless sensor network

ABSTRACT

Security of a wireless sensor network is aimed at ensuring information confidentiality, authentication, integrity, availability and freshness is an important factor considering the criticality of the information being relayed. Hence, the need for an intrusion detection/prevention system. Conventional intrusion avoidance measures, such as encryption and authentication are not sufficient because they become useless in the event of a sensor node being compromised, hence, can only be seen as a first line of defence in the network after which intrusion detection schemes follow. In this paper, two layers trust-based intrusion detection system was developed for wireless sensor networks. A trust-based model is presented to detect intrusions to the network. Scenarios were created by using different set of weights. By injecting 2%, 5% and 10% malicious nodes from the 100 nodes considered, the results obtained were carefully observed. For scenario 2 (S2) with 2% and 5% malicious nodes injected, the model achieved the best result in all cases with an average detection accuracy of 97.8% while scenario 3 (S3) with 10% of malicious nodes introduced recorded the best performance with an average accuracy of 96%. Hence, the model will be suitable with combination of weights in S2 with small networks but when the scale of the network increases, the set of weights in S3 are best with the model.

1. Introduction

Wireless sensor network (WSN) can be referred to as a network of nodes (also known as motes) that work cooperatively to sample and control the parameters of the environment that surrounds them. Nodes in the network supportively route their data to a sink otherwise known as base station (BS) where the data can be logged and analysed (Matin & Islam, 2012). These nodes communicate wirelessly with one another and with the BS employing transceivers (Lagkas & Eleftherakis, 2014). WSN application is fast growing, as the distributed architecture among other attributes make them suitable for a variety of functions. However, wireless sensor nodes are constrained in terms of transmission range, memory, energy and computational power (Agajo *et* al., 2015; Rajeshkumar & Valluvan, 2016).

A major concern of researchers is whether the WSN can actually be secured, considering its fragile nature, as the network can be attacked to intercept messages/information (Iwendi & Allen, 2012). Passive attacks can be launched against the network privacy by unauthorised persons with the goal of monitoring and listening to the communication channel to extract meaningful information. The passive attacks include eavesdropping, traffic analysis and camouflage adversaries. When the packets contain control information, eavesdropping becomes very effective to the adversary than getting the information through the location

Please, cite this article as: Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G. & Ajao, L. A. (2018). Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks, *Advances in Electrical and Telecommunication Engineering, 1*(1), 23-29.