Secure and Reliable Knowledge-Based Intrusion Detection Using Mobile Base Stations in Smart Environments

Ambika N.
https://orcid.org/0000-0003-4452-5514
Department of Computer Applications, SSMRV College, Bangalore, India

INTRODUCTION

Wireless sensor network (Yick, Jennifer, Mukherjee, & Ghosal., 2008) (Akyildiz, F., Su, Sankarasubramaniam, & Cayirci, 2002) is an assembly of low cost nodes which can capable of self-configuration. These nodes communicate with each other forming a convenient topology. Smart home (Erol-Kantarci, Melike, & Mouftah, 2011), military surveillance (Lee, Hyuk, Lee, Song, & Lee, 2009), health monitoring (Kim, et al., 2007), habitat monitoring (Mainwaring, et al., 2002) are some of the applications where these nodes play a primary role. These unsupervised nodes are liable to get compromised and launch different kinds of attacks. Hence the malicious nodes have to be detected (Butun, Ismail, Morgera, & Sankar, 2014) at an early stage to minimize the attacks in the network.

The mobile base station (Sun, Osborne, Xiao, & Guizani, 2007) (Djamel, Khelladi, & Badache, 2005) provides flexibility to the system to move to any corner of the network. They are capable of authenticating the other nodes but they require more security than the static ones. The proposed work is using the mobile base station that adds reliability to the data transmitted. The work is compared with (mehmood, et al., 2018). The work considers two different kinds of nodes in the network. Assistance nodes are the watchdogs in the work. They aid in selection of cluster head and provide information on any malicious activity in the respective cluster. The mobile agent is used in the work to cross-verify the malicious activity of the node deployed in the cluster.

The work is divided into six sections. The section 2 details the work done by various authors. The section 3 explains the proposed work in detail. The role of different deployed nodes is described in this section. Section 4 provides details of analysis of the work. The details of simulation of the work are provided in section 5. Section 6 details the future directions. The work is concluded in section 7.

BACKGROUND

Many authors have provided their own insights (Butun, Ismail, Morgera, & Sankar, 2014) and suggested different ways to detect an intrusion in the sensor network. The details of the same are explained in this section.

In (mehmood, et al., 2018) the network is divided into clusters and each cluster is headed by the cluster head. The base station has a blank knowledge database installed. The cluster heads are provided with inference engines. The heads monitor node-related events and data transmission in the respective clusters. The data monitored is considered as events and the same is transmitted to the base station. This

DOI: 10.4018/978-1-7998-3479-3.ch036

received data is analysed to detect suspicious activity. Routine and redundant events are eliminated and same is notified to the respective cluster heads. The threats detected in the received message are notified to the cluster heads. The same is broadcasted to the other cluster members. Any unknown event is analysed and alerted to the cluster heads to avoid transmission. The cluster head is rotated among the members of the cluster for effective and energy consumption of the nodes.

Three stages are proposed by the authors in (Silva, et al., 2005) to detect an intrusion in the network. Filtered messages are collected by the promiscuous node in data acquisition phase. Using this approach the energy is saved. The array storage structure is used to store the discarded messages. In the rule application phase the rules are applied to stored data in array. If the tested data again results in failure, the data is discarded. The approach reduces detection latency. Failure alert is raised if the stored data does not obey the stated rules. An intrusion detection alert is raised if the failure alert is raised beyond a threshold. The failure history is maintained by the respective node. The previous and the present cumulative failure value are combined to obtain new cumulative value. The approach follows deviation failure.

The authors have suggested a security scheme to detect intrusion in (Onat & Miri, 2005). Node impersonation and its effect are addressed in this work. Node impersonation is where the intruder steals the identification of the legitimate node. It provides itself with the same identity credentials. It gains the trust of the other surrounding nodes and gets into depleting the resources or provides false alarms. In the proposed work data and control packets are directional. Tree based forwarding structure is used to route the packets from one end to another. The anomaly report is generated by the neighbours. If more than one node declares illegitimate activities w.r.t its neighbour, the suspicious node is concluded to be guilty.

A Light weight scheme is proposed by the authors in (Ioannis, Krontiris, Dimitriou, & Freiling, 2007) to detect the illegitimate node in the network. The system is focussed to detect blackhole and selective forwarding attacks based on specification based detection. The watchdogs are into cooperative decision making process where the selective forwarding attack is detected to take appropriate actions. The system is into gaining the information from the neighbouring nodes to ward off the guilty node. The nodes are into auditing and aid in building intrusion treat level. This report is shared to bring in collective report. To achieve the success in detection, four conceptual models are utilized. Local packet monitoring, local detection engine, cooperative detection engine and local response are building and the work is divided among the nodes of the network to increase success rate of detecting intruder.

A game theoretic approach is suggested by authors in (Agah, Das, S. K., & Asadi., 2004) to detect intrusion in the network. The authors have suggested three different approaches to detect the compromised node in the network. In the first approach, attack-defence scenario is created. The sensor nodes and the attacker are in non-cooperative mode. The game achieves Nash equilibrium for the attacker and the Intrusion Detection system. This resultant provides an advantage to the Intrusion detection system. Second scheme Markov decision process is used. The system is into learning mechanism. The Intrusion Detection system observes the system and tries to understand the behaviour of the intruder. Using this analogy it tries to analyse which node requires protection. Third scheme uses intuitive method. The node that has the highest traffic load is given the higher priority of protection.

A hierarchical trust based scheme is proposed by the authors in (Chen, Guo, Bao, & Cho, 2014) to detect intrusion in the network. The nodes are evaluated for their honesty, energy and cooperativeness. Sensor node level and cluster head level trust is maintained in the system. The sensor nodes observe other nodes of the cluster for their legitimacy. The cluster head maintains the trust level of other cluster heads in its vicinity. The trust evaluation based on either direct or indirect methodology. The direct evaluation is evaluated for their activity when they communicate with other nodes of the network. The trust level generated by the nodes of the cluster is exchanged by each other. The trust level related to other cluster