
Rakesh Sharma¹, Vijay Athavale²

¹Department of Computer Science Engg., CRM Jat College, Hisar
²Department of Computer Science and Engg., Gulzar Group of Institutes, Ludhiana

¹rakeshsharma3112@gmail.com
²vijay.athavale@gmail.com

Abstract—Wireless sensor networks (WSNs) are creating their manner from analysis to real-world preparation, body & personal-area systems, sensible homes, ecological observance or mobile communications. Wireless ad hoc networks of sensor nodes are visualized to be deployed within the physical atmosphere to observe a large kind of real-world phenomena. Wireless sensor networks (WSN’s) are getting fashionable in military and civilian applications like police investigation, monitoring, disaster recovery, home automation and plenty of others. Nearly any sensing element network application needs some kind of self-configuration and involuntary practicality. WSNs would not be with success established if security irresponsibleness and privacy problems are not self-addressed adequately. These matters become additional important as a result of WSNs are typically used for terribly crucial submissions. WSNs are terribly vulnerable and thus appealing to attacks because of their restricted charges and human-unattended preparation.

I. INTRODUCTION

Advances in technology have made possible to develop small low-cost devices, called sensors, which may be deployed in large numbers to form a wireless sensor network (WSN) that can be used in many applications [1]. The WSN technologies in a wide range of application scenarios, often with sensitive and high-valued data being communicated, the need to manage security is becoming increasingly relevant and critical [3]. Wireless sensor network has a wide range of applications such as disaster management, environment monitoring, military surveillance, habitat monitoring, health care, vehicle traffic monitoring etc [8]. WSNs are composed of small, low cost, resource-constrained devices that sense the environment and cooperate with each other in order to perform monitoring and tracking operations. Because of these specific characteristics, WSNs are vulnerable to malicious attacks, several intruders and faults [15]. The security attacks in the WSN are categorized in two ways, which are active and passive attack. In many applications, such as target tracking, battlefield surveillance and intrusion detection, WSNs are often deployed in hostile environments. Therefore, there is a great need to protect the sensing data and sensing readings from the sensors [4]. In wireless sensor networks, there are two key characteristics that make such systems prone to the security attacks. Firstly, the simplified processing capabilities and limited power resources expose them to a number of possible security attacks. Secondly, the network connectivity to the outside world, without any inbuilt protection, also leaves such systems vulnerable to security attacks [9]. Hence, the WSNs are prone to different types of attack, which can compromise reliability, integrity and availability of the sensor data traffic and sensor lifetime as well [11]. Also, the intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively (e.g., information

Gulzar Group of Institutes, Ludhiana, Punjab-141401 (INDIA)
gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks). Thus, Intrusion Detection System (IDS) plays a prominent role to the detection of any suspicious behaviour in a network performed by the network members [17]. In other words, the Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. The intrusion detection application concerns how fast the intruder can be detected by the WSN [16]. An Intrusion Detection System (IDS), which has been successfully implemented in wired networks, can detect the misbehaviour of participating nodes and notify other nodes in the network to take appropriate countermeasures [18]. Therefore, two factors are needed to ensure effective Intrusion Detection System (IDS). Firstly, the IDS should be able to deliver reliable detection outcomes. The detection methods have to be effective in identifying intrusions since poor detection performance will ruin the trustworthiness of the IDS. Secondly, the IDS should survive in hostile environments. However, maintenance of high detection accuracy is challenging [10]. Generally, the IDSs can be briefly classified into two categories: signature-based detection schemes and anomaly-based detection schemes. Both of the two categories focus on identifying behaviours of malicious nodes. They consume a large amount of energy to monitor suspicious nodes [12]. In WSNs, the use of regular IDSs [5] may be compromised by frequent detection flaws and false alarms. Improving IDS effectiveness can be achieved through by using Computational Intelligence methods [19], clustering mechanism [7], probabilistic model [13], Trust management protocol [14], etc.

II. REVIEW AND COMPARISON

<table>
<thead>
<tr>
<th>Authors</th>
<th>Intrusion detection methods</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noureddine Assad et al. [1]</td>
<td>Probabilistic model</td>
<td>The probability is increased while increasing the sensing range.</td>
<td>Affects the robustness of the connectivity due to small transmission range.</td>
</tr>
<tr>
<td>Hussein Moosavi and Francis Minhthang Bui [3]</td>
<td>Game-theoretic framework</td>
<td>Improves the security and design stability.</td>
<td>Increase the number of compromised nodes.</td>
</tr>
<tr>
<td>Mohammad Wazid and Ashok Kumar Das [4]</td>
<td>K-means clustering</td>
<td>Avoids the detection mismatch.</td>
<td>Increases the incoming traffic in the WSN.</td>
</tr>
<tr>
<td>Helio Mendes Salmon et al. [5]</td>
<td>Artificial immune inspired system</td>
<td>Enhances the efficiency of the IDS system since it achieves low false positive.</td>
<td>Incurs larger delay in the intrusion detection system.</td>
</tr>
<tr>
<td>Shahaboddin Shamshirband et al. [6]</td>
<td>Fuzzy artificial immune system</td>
<td>Enhance the detection accuracy.</td>
<td>Fails due to high volumes of real time traffic.</td>
</tr>
</tbody>
</table>
Distributed anomaly detection improves robustness against the faulty or malicious node. Due to large communication overhead, the performance gets degraded.

Probability based on network parameters significantly improves the detection probability. Critical to detect the intruder when distance between nodes and intruder is greater than sensing range.

<table>
<thead>
<tr>
<th>Sutharshan Rajasegarar et al. [7]</th>
<th>Anil Kumar Sagar and D. K. Lobiyal [8]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed anomaly detection</td>
<td>Probability based on network parameters</td>
</tr>
<tr>
<td>Improves robustness against the faulty or malicious node.</td>
<td>Significantly improves the detection probability.</td>
</tr>
<tr>
<td>Due to large communication overhead, the performance gets degraded.</td>
<td>Critical to detect the intruder when distance between nodes and intruder is greater than sensing range.</td>
</tr>
</tbody>
</table>

Table 1

III. CHALLENGES

The core weakness of wireless sensor node [6] lies in the limited resource devices, i.e. power and processing units. For this reason, vulnerability to various security threats is notably high. The main security threat [4] is that the attackers or intruders are included in the WSN since each sensor node has limited battery power, memory size, data processing capability and short radio transmission range. This leads to degrade the performance and security level.

Also, the sensors in a network are deployed in unattended environment or even hostile circumstance, and communicate with each other using wireless signal which can be eavesdropped very easily [20]. For example, bogus routing and sensed data attack, select forward attack, sink hole attack, worm hole attack, black hole attack and hello flood attack, etc.

Another important challenge [15] in WSNs is the detection of intruders, i.e., an unusual measurement that are inconsistent with the distribution of the majority of observations. The intrusion detection has several important roles in the wireless sensor network. Hence, it is important to detect and filter those erroneous measurements, to ensure the integrity of the collected data.

In [6], fuzzy artificial immune system was developed to identify the network intruders. In this C-AFAIS, the decision making capabilities face major challenges due to the poorly trained architecture and the missing of evolutionary optimization process.

REFERENCES

[7] Sutharshan Rajasegarar, Christopher Leckie and Marimuthu Palaniswami, "Hyperspherical cluster based distributed anomaly
International Journal of Advance Research and Innovation (ISSN 2347 – 3258)


