
*Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore 560 001
**Vice Chancellor, Defence Institute of Advanced Technology (Deemed University), Pune, India
email: shailak17@gmail.com

Abstract—Wireless Sensor Networks consists of tiny devices which processes and routes the sensed data. The process of detecting any external and internal intruders entering to a Wireless Sensor Network area is referred to as intrusion detection. An intruder is a moving attacker entering a particular area. In this paper, we propose an algorithm Secure and Energy Efficient Approach for Detection of Intruder (SEEDI) in homogeneous Wireless Sensor Networks. Single sensing and multi sensing intruder detection are considered in our algorithm. Simulation results showed that the proposed algorithm resulted in better performance.

Keywords- Intrusion Detection, Node Density, Sensing Range, Transmission Range, Wireless Sensor Network.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of large number of sensor nodes which are deployed in spatial environment. These nodes are capable of sensing any of the physical or environmental conditions. WSNs are widely used in military applications such as in borders for finding out the infiltrations, industrial process monitoring and control, healthcare applications etc. Sensor nodes perform sensing, data processing and communication with limited resources like power, computational capacities, memory size and low bandwidth. Therefore, utmost care has to be taken while constructing the networks under these constraints. Energy is vital for many applications in WSN since it is impossible to recharge the deployed nodes. One approach is to put some sensor nodes in sleep mode and wake them up when required to save energy.

Sensors are deployed in a variety of domains and many applications should be secure from attacks. A lot of security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, data freshness and authenticated broadcast for sensor network [1]. Localized Encryption and Authentication Protocol (LEAP), is designed to support in-network processing based on different security requirements for different types of message exchange [2]. INSENS is an intrusion tolerant routing protocol for WSNs [3]. Security solutions in the network are divided into two categories: prevention and detection. Prevention techniques, such as encryption, authentication, etc., are used to prevent attacks from outside. These preventive measures reduce the chance of intrusion, but are not able to eliminate the intrusion completely. Intrusion detection is essential to achieve longer lifetime and defend the network security by the intruders.

In WSNs, if preventive measures fail, the network can identify and resist the attacks by means of intrusion detection techniques. Thus, Intrusion Detection Systems (IDSs) are important for the security of networks. IDSs are defined as a monitoring system for detecting any malicious intruder that invades the network domain [4-6]. Detecting a moving intruder is a crucial application in WSNs. Intrusion detection is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster.

Motivation: In WSN clustering, energy utilization, routing, data aggregation, multimedia, collaborative processing, security etc., are related to each other. Whatever be the application, if WSN formed is not secure from external and internal attacks then the entire effort of data transmission is lost. There are two types of attacks: external and internal. External attacks may change the nodes to become malicious which results in abnormal behavior. So it is very important to identify the external attacks that occur in WSN.

Contribution: In his paper, we have developed SEEDI algorithm that handles internal intrusion detection and energy consumption for intrusion detection process. The internal intrusion detection includes the analysis of data sent by each node. The algorithm proposed is used for internal data analysis, it selects a set of nodes among the entire nodes and activates its IDS module. Related work is discussed in Section II, Problem Definition in Section III. The implementation and algorithm is discussed in Section IV, Mathematical analysis in Section V, Simulation results are given in Section VI and Conclusions in Section VII.

II. RELATED WORK

Zhang et al., [7] studied the problem of intrusion detection in Wireless Ad-hoc Networks. They have proposed architecture for distributed and cooperative intrusion detection system for Ad-hoc Networks, which was based on statistical anomaly detection techniques which requires much time to detect intrusion in data and during traffic.
Liu et al., [8] have explored the effects of sensor mobility on sensing, coverage and detection capability in a mobile WSN. Wang et al., [4] have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range and transmission range) under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs assuming a straight line or linear motion intrusion path for an intruder.

Yun et al., [9] proposed a novel probabilistic sine-curve mobility model to explore the effects of different intrusion paths using single-sensing and K-sensing detections in a given WSN. For intrusion detection of an object, the detection probability is determined by the object size, the number of sensors, sensing radius, the number of subsets and the size of the monitored region.

III. SYSTEM MODEL AND PROBLEM DEFINITION

A. Network Model

Consider a homogeneous WSN in a two-dimensional (2D) plane with N sensors, denoted by a set \( N = (n_1, n_2, n_3, \ldots, n_N) \), where, \( n_i \) is the \( i^{th} \) sensor. These sensors are uniformly and independently deployed in an area \( A = L \times L \) which results in a 2D Poisson point distribution of sensors. The sensors deployed in WSN are static. In a homogeneous WSN, each sensor has the same sensing radius of \( r_s \), the transmission range \( r_x \) and node density \( \lambda \). A sensor can only sense the intruder within its sensing area i.e., a disk with radius \( r_x \) centered at the sensor. In a WSN, a point is said to be covered by a sensor if it is located in the sensing range of any sensor(s).

The WSN is divided into two regions, the covered region, which is the union of all sensor coverage disk and the uncovered region, which is the complement of the covered region within the area of interest \( A \). We have assumed that the sensing coverage area is not known to the intruder. Consider an intruder moving from the boundary as shown in Figure 1, the distance moved by the intruder is \( D \). The intruder is detected only, when there is a sensor in the area moved by the intruder. The intruder can move through a straight line or through a curved path. It follows a straight path only when it knows the exact destination, otherwise it follows a curved path. In this paper we are considering only straight path. The area moved by the intruder is,

\[
S = 2 \times D \times r_x + \pi r_x^2 / 2
\]

If the intruder is entering the WSN area from a random point, i.e., the intruder is dropped from the air, then the area moved by the intruder is shown in Figure 2 and is given by,

\[
S = 2 \times D \times r_x + \pi r_x^2
\]

Intrusion detection is defined as a mechanism for WSNs to detect the existence of inappropriate, incorrect or anomalous moving attackers. For example, while detecting an intruder in the battlefield. For this purpose, it is a fundamental issue to characterize node density and sensing range of WSN interms of a desirable detection probability [4]. Intrusion detection modules on sensor nodes try to detect the malicious action which occurs within its radio range. The monitoring technique (like watchdog, local monitoring) relies on the broadcast nature of sensor communication and takes advantage of high density sensors deployed in the sensing environment. The sensor nodes activate the intrusion detection modules called monitor nodes.

B. Problem Definition

The life span of WSN is directly dependent on the power. The power required to transfer data from a sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So, battery power of each sensor can be saved and this increases the WSN life span. There are limited external and internal intrusion detection techniques and no algorithm supports random detection of intruders.

C. Assumptions

Consider static sensors and intruder as a moving object. Each
Figure 3. Intrusion Detection by Single Sensor.

In this paper, an Intruder is defined as any moving object that enters into the WSN area. We have derived the detection probability for single-sensing and multi-sensing detection.

**Implementation and Algorithm**

Let \( n \) be the minimum number of sensors required to cover the network area. The minimum number of sensors participating in intrusion detection is equal to the minimum number of sensors required to cover the WSN area. Intrusion detection module performs two functions:

- (i) finding the intruder,
- (ii) passing the information to the base station.

The SEEDI algorithm in Phase I determine the minimum number of sensors required to cover the area depending on both sensing range and transmission range as shown in Table I. The SEEDI algorithm in Phase II determines the number of nodes required to perform intrusion detection is atleast \( n \) as shown in Phase II.

### V. Mathematical Analysis

#### A. Single Sensing Detection Model

An intruder is detected when it enters the sensing range of a sensor. When the intruder enters the area through the boundary and if the sensors are available, then the intruder is detected as soon as it enters the WSN area. Otherwise, it has to move a certain distance \( D \) before being detected by any of the sensors. The intruder is detected within the radius \( r_s \) of the circle around the sensor as shown in Figure 3.

When the intruder starts from a point on the network boundary, as shown in Figure 1 and if intrusion distance \( D > 0 \), the corresponding intrusion detection area \( A \) is almost an oblong area. The area includes a rectangle of length \( D \) and a half circle of radius \( r_s \) and the area is,

\[
A = 2r_s D + \frac{\pi r_s^2}{2} \tag{3}
\]

According to the definition of single-sensing detection, the intruder is detected if and only if there exists atleast one sensor within this area \( A \). i.e., the intruder is detected if it comes in the sensing range of any of the sensors, else the intruder is not detected. Similarly, when the intruder starts from a random point in the network domain, the corresponding intrusion detection area is given by equation (4). The sensing area includes two half circles and that of the rectangle. The radius of the circle is \( r_s \) and the length of the rectangle is \( D \).

\[
A = 2r_s D + \pi r_s^2 \tag{4}
\]

Initially, assume that the intruder starts from the boundary of the network.

**Theorem 1:** The probability \( P(D) \) indicates that an intruder can be immediately detected once it enters a homogeneous WSN with node density \( \lambda \) and identical sensing range \( r \). \( P(D) \) is given by,

\[
P(D = 0) = 1 - e^{-n}
\]

**Proof:** According to Poisson distribution

\[
P(m, A) = \frac{(A \lambda m^e)^{A \lambda}}{m!} \tag{5}
\]

where, \( m \) is the number of sensors, \( A \) is the area, \( \lambda \) is the probability of sensors responsible for intrusion detection. In this paper, only \( n_1 \) sensors are performing intrusion detection at a time. So \( \lambda = n_1 / A \). If there are no sensors in the area \( A \), then the probability is equal to \( P(0, A) = e^{-A \lambda} \).

Based on complement of the probability, the probability that

---

**Table I**: Secure and Energy Efficient Approach for Detection of an Intruder (SEEDI) Algorithm

<table>
<thead>
<tr>
<th>Phase I</th>
<th>MinNode(tr,rs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>if ( tr \geq rs ) then</td>
<td></td>
</tr>
<tr>
<td>( n ) ( \left\lfloor \frac{rs^2}{k} \right\rfloor \equiv k \mod \left\lfloor \frac{r^2}{2} \right\rfloor )</td>
<td></td>
</tr>
<tr>
<td>where ( k = {0 \text{ to } \left\lfloor \frac{rs^2}{2} \right\rfloor - 1 } )</td>
<td></td>
</tr>
<tr>
<td>if ( tr &lt; rs ) then</td>
<td></td>
</tr>
<tr>
<td>( n ) ( \left\lfloor \frac{tr^2}{k} \right\rfloor \equiv k \mod \left\lfloor \frac{r^2}{2} \right\rfloor )</td>
<td></td>
</tr>
<tr>
<td>where ( k = {0 \text{ to } \left\lfloor \frac{tr^2}{2} \right\rfloor - 1 } )</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

**Phase II**: At sink node

- Assign \( U = \{R\} \) the set of nodes in the WSN area.
- Let \( N(i) \) is the set of neighbors of node \( i \). repeat
  - If \( N(i) \neq \emptyset \) Find min \( N(i) \)
  - Put \( i \) in Stack
  - \( I = \{a / \text{the distance between } i \text{ and } N(i) < (rs/2)\} \)
  - if \( N(i) > 1 \) then \( U = U - [i U I] \);
  - else \( U = U - I \);
- Until \( U \) is Null

---

At the sink node, the algorithm sends a packet to the selected node to activate its IDS module.
there is at least one sensor in the area $A$ and the intruder is detected by any of these sensors is,

$$1 - P(0, A) = 1 - e^{-n_1} \quad (6)$$

Hence the theorem is proved.

**Theorem 2:** Suppose $\eta$ is the maximal intrusion distance allowable for a given application, then the probability $P(D)$ that the intruder can be detected within $\eta$ in the given homogeneous WSN can be derived as,

$$P(D \leq \eta) = 1 - e^{-n_2} \quad (7)$$

where, $n_2$ is the number of sensors participating in intrusion detection.

**Proof:** The volume moved by the intruder is,$$
\begin{align*}
A &= 2\pi r_s + \left(\frac{1}{2}\right)\pi r_s^2 \quad (8)
\end{align*}
$$

So if there is no sensor in that area, then the probability of detection is $P(0, A)$, then complement of $P(0, A)$ will give the probability of detecting intruder within the distance $\eta$.

**B. Multi-Sensing Detection Model**

Some applications require more than one sensing information about the intruder, i.e., the case of finding intruder position. In this case we need the intruder to be detected only when it is within a sensing range of $K$ sensors as shown in Fig. 4.

**Theorem 3:** Let $P_m(D = 0)$ be the probability that an intruder is detected immediately once it enters a WSN with node density $\lambda$ and sensing range $r_s$ in multi-sensing detection model. Then $P_m(D = 0)$ is given by,

$$P_m(D = 0) = 1 - \sum_{i=0}^{m-1} e^{-n_1}$$

where, $n_1$ is the number of selected sensors within the area $A = \pi r_s^2 / 2$.

**Proof:** This theorem can be proved based on Poisson distribution. The area is only one half circles with radius $r_s$. $P(i, A)$ gives the probability of detecting the intruder with $i$ sensors. $\sum_{i=0}^{m-1} P(i, A)$ gives the sum of the probabilities of detecting the intruder with less than $m$ sensors. So the complement will be the multi-sensing probability. The analysis for intruder detection less than maximum allowable distance can also be determined as in Theorem 2.

**VI. SIMULATION AND VERIFICATION**

Our analytical results are verified through simulation using MATLAB for single-sensing and multi-sensing detection models in WSN. The simulation was carried out using 500 sensors which were uniformly distributed in a square network domain. The sensors are uniformly distributed in a two-dimensional space of 1000*1000 meters. The node density is set as $\lambda = 0.0005$ per square meter. The sensing range is varied from 0 to 50 meters and maximal allowable intrusion distance is 50 meters.

The simulation results are obtained by changing node parameters such as density, transmission range and sensing range. The intruder is allowed to move through the WSN area starting from any point. Monte-Carlo simulation is performed and each data point shown in Figure 5 is the average of the simulation results. The analytical results are calculated by using the Theorems 1, 2 and 3. For successive simulation runs, the sensors are uniformly redistributed in the network domain.

The simulation results showed that the detection probability. It is found that the detection probability remains
same as in the case of analytical results, thus proving the correctness of the analytical model. Fig. 5 shows Single-Sensing Detection probability and Multi-Sensing Detection probability. It shows that Single Sensing Detection probability is higher than that of Multi-Sensing Detection probability. This is because Multi-Sensing Detection impose a stricter requirement on detecting the intruder (i.e., at least 3 sensors are required).

The graph is obtained by changing the sensing range from 0 to 40. Each point in the graph is a result of 100 simulations. i.e., to get each point we need to execute our simulation and find out the probability from the result of 100 executions. Here we can see that single sensing is possible at lower ranges also. But multi-sensing takes time to get the results, since it requires more than one sensor (in this simulation three sensor information were considered) information to detect the intruder.

Fig. 6 demonstrates the average number of nodes selected by using SEEDI algorithm. The density of nodes is varied to check how many nodes are activating its IDS module. From the graph it is evident that even if the density of nodes in the area increases the number of nodes selected for intrusion detection remains within a small range. In order to plot the graph the sensing range and transmission range is fixed to 45 and the density is varied. The energy consumption by the network using SEEDI algorithm is analyzed in the Fig. 7. The assumption made is that the energy used by one node for a unit time is one unit. The results showed that the energy consumption is less compared to the previous work.

VII. CONCLUSIONS

In this paper, the external intrusion detection is minimized in an energy efficient way and probability of space. This probability gives an insight into the required number of sensors in a given deployment, their sensing and transmission range to securely detect an intruder in a WSN. We have developed an analytical model for intrusion detection and applied the same into single-sensing detection and multiple-sensing detection scenarios for homogeneous WSNs. The correctness of the analytical model is proved by simulation.

REFERENCES