INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Intrusion Detection System in WSN Using ACO

Harpreet Kaur
M.Tech Student, BBSBEC Ftg. Sahib, Punjab, India
Er. Daljeet Singh Bajwa
Assistant Professor, BBSBEC Ftg. Sahib, Punjab, India

Abstract:
Wireless sensor network is most widely used technology in number of monitoring and tracking tasks. In many such cases security is major issue of concern. Security is required to avoid any kind of interference which occurs due to lack of gateways and switches. The intruder must be detected before it harms the network. In order to protect WSN from various kinds of attacks number of algorithms has been developed. In this paper we purpose a new intrusion detection scheme by using ant colony optimization technique in heterogeneous environment of sensor nodes. With varying the density in précised manner results will exponentially increases to detect intrusion in particular area. Our result shows that detection probability increases by applying ACO in heterogeneous environment.

Keywords*: Wireless sensor network, Hive, Intruders, Intrusion detection, Heterogeneous WSN's model, Homogeneous WSN's model, Ant colony optimization technique*

1. Introduction

A WSN has become most interesting networking technology since it is deployed without communication infrastructures such as gateways and switches. Wireless sensor network basically consist of large number of tiny sensor nodes and sink that collects the information from these nodes and transfer it to base station and it act as a gateway between sensor nodes and base station as powerful processing, data storage and access to all the nodes in its network are the worthy features of WSN[4].These networks have distinct characteristics as compared to other communication networks as a result of this WSN is applied to various fields of science and technology. To collect the information related to human activities such as health care, military surveillance and reconnaissance, high way traffic, to monitor physical and environmental phenomena such as wild life, earth quake, pollution, wild fire and water quality ,to monitor industrial sites such as building safety and manufacturing performance[1]. Security issues are the most important part of WSN that are taken in account there are many critical issues related to security such as authentication, encryption, network access and compromising nodes. Intrusion detection is necessary to overcome the faults present in the network [2].

Intrusion detection is the act of detection of unwanted traffic on a network or a device. An IDS can be piece of installed software or a physical appliance that monitor the network traffic in order to detect unwanted activity and events such as illegal and malicious traffic that violates the security policy. Many IDS tools will store a detected event in a log to be reviewed at later date or will combine the events with other data to make the decisions regarding policies and damage control. An IPS is a type of IDS that can stop or prevent unwanted activates. Intrusion detection systems can monitor both inside and outside attacks and these systems are very necessary as simple security systems cannot offer needed security such as cryptography it offers prevention against some type of attacks but cannot provide privacy in malicious nodes which require cryptography keys [5].

Attacks in wireless sensor networks are classified in to two main classes based on the source of attacks: insider and outsider. Insider attacks are attacks which occur due to compromised nodes within the network. Whereas, outsider attacks are created by outside parties like laptop class attacks which are initiated from outside by using high performance devices such as laptops. To provide security, prevention based security systems such as authentication, cryptography, key management have been developed. These mechanisms are considered as first defense line against attacks because these are effective only for certain kind of outside attacks but are failed to protect insider attacks as a result of this there was a need of another layer of protection. Detection systems (IDS) have been used as a second defense line against attacks in many type of sensor networks .However, their use in WSN poses many challenges due to constraint resources [3].

Solution to security attacks involves three basic components:
Prevention, Detection, Mitigation (reacting) against attacks in intrusion detection systems if first layer i.e. intrusion prevention is failed to prevent attacks then second layer comes into play i.e. intrusion detection. Intrusion is unauthorized activity which harms the network actively (e.g. harmful packet forwarding, packet dropping and hole attacks) or passively (e.g. information gathering, eavesdropping). Intrusion detection systems provide the information related to type of intrusion, location of intruder, date, intrusion activity active or passive to other supportive systems and this information is very useful for third layer of defense. This is the main reason behind the importance of intrusion detection [7].
WSN networks are heterogeneous and homogeneous consist of many tiny nodes which are used to monitor physical and environmental conditions by measuring temperature ,humidity ,pressure, sound, vibration at different locations. A typical model of WSN consists of sensor nodes that transfer the data to base station. In some cases aggregation points called cluster nodes are used to collect the data due to constraint resources. In sensor network a group in which all the sensor nodes have same sensing range and capability is called homogeneous group of sensor nodes. However a group in which all the sensor nodes do not have same sensing range and capability is called heterogeneous group of sensor nodes [6].

2. Literature Survey
Intrusion detection is one of the critical applications of WSN recently several approaches for wireless sensor network has been developed.
A Shakil ahmed, Dr A Rajeshwari [7] work on intrusion detection in heterogeneous environment with energy efficient node localization mechanism.WSN is employed in 2D space and analytical model is developed and it is applied to single sensing detection and multiple sensing detection. It is observed that single sensing has higher probability than multiple sensing as multiple sensing imposes strict requirements on the detection of an intruder .Simulation consist of RSS and TOA localization. The intrusion detection performed by a RSS is highly energy efficient for both type1 and type2 sensor.
Srinivasaraju Dantuluri and Poturaju [8] consider the concept of intrusion detection in two WSN models. They derive the detection possibility by using single sensing and multiple sensing. In addition, they also use the concept of network connectivity and broadcast reachablility which are necessary conditions to make detection probability in a WSN. Their simulation results validate the analytical values for both homogeneous and heterogeneous networks.
Kung and vlah[9] has taken the advantage of hierarchal tree structure to effectively track the movement of an intruder.
The intrusion detection problem has been considered from the constraint of saving network resources.
Absar-ul-hasn,Ghalib A.Shas and Ather Ali[10] describe the design and implementation of a system capable of reliable, robust and efficient monitoring for human intrusion detection. The system allows a group of sensory devices forming wireless network to detect the human presence in the deployment area and also track the positions of moving target. They evaluate their performance by using 30 nodes that includes Micaz motes and also their customer built low cost sensor nodes. Performance results show that customer built nodes operates equally well as Micaz motes and their cost is also comparatively less and these are basically designed to reduce the cost.
The detection probability can also be calculated theoretically by using underlying parameters and the analytical results has shown the improvement in on the detection probability in heterogeneous as compared to homogeneous.

3. Proposed Algorithm
In this research two type of sensor nodes are deployed i.e. type1 and type2 in 2D space. Our intrusion detection model includes following.

- WSN Network model
- Intrusion detection model for both WSN models.
- Intrusion detection model by applying ACO.

The network model specifies the WSN environment in which sensor nodes are deployed in homogeneous environment all the sensor nodes have same sensing range whereas in heterogeneous environment sensor nodes have different ranges. The intrusion detection strategy model defines the moving policy of an intruder and detection of an intruder. In order to create better results as compared to existing technique ACO is applied in heterogeneous environment.
In network model following parameters are taken.

Description	Quantity/Range
Square area(A=L*L)	1000x1000
Distribution	2D Grid distribution
Cluster Diagonal distance	200
Sensor deployment strategy	Random uniformly
Number of sensors	500 nodes
Number of intruders	100
Intrusion distance	50 meter
Battery life	5 joules

Degree of freedom	10
Packet size	64 bytes

Table 1: Reference scenario

We consider two types of sensor network models:

- Homogeneous
- Heterogeneous

In homogeneous WSN model each sensor has same sensing radius and transmission range. A sensor can only sense intruder within its sensing coverage area Parameter used for the deployment of homogeneous WSN model are:

Description	Quantity /Range
Sensors	500
Range of sensors	Vary from 10 to100 meters

Table 2: Homogeneous WSN'S Parameters

In heterogeneous WSN model, we are deploying two types of nodes:

- Type 1- sensor that has a larger sensing range, as well as longer transmission range.
- Type 2- sensor that has a smaller sensing range, as well as shorter transmission range.

Parameter used for the deployment of heterogeneous WSN model we have:

Description	Quantity and Range
Sensors	Type1 nodes 200 Type2 nodes 300
Sensor range(fix)	Type1 nodes 120 Type2 nodes 40
Grid square transaction (diagonally per cluster)	200

Table 3: Homogeneous WSN'S Parameters

Sensor nodes are deployed in 1000X1000 meters in uniformly random distribution manner.
In intrusion strategy model, intruders enter randomly and also select their positions randomly with in network domain or from any point of the network boundary of the network domain .The intruder starts from a point of network boundary and travels total distance of 50 meters and it is called intrusion distance within the network region from network boundaries. Our IDS is imposed on both homogeneous and heterogeneous WSN model.
We have taken 100 intruders in our simulation model and divided into four types i.e. type1,type2 ,type3 and type4 and randomly entered them from each side of the boundary after finding their positions .Our major task is that the intruder must be detected at very first point of the occurrence so that it will not spoil the network performance. The aim behind the use of the two types of sensor nodes is to increase the detection probability by replacing the low range sensors with high range sensors.

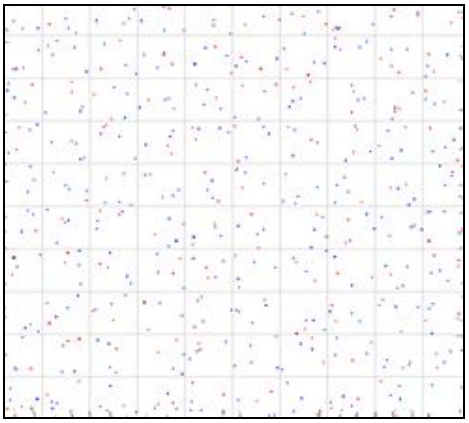

Figure 1: Heterogeneous WSN

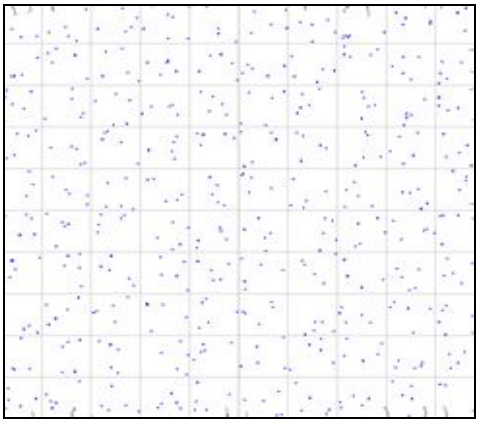

Figure 2: Homogeneous WSN

The intrusion distance is the distance that the intruder travels before it is detected by a WSN for the very first time. The maximal intrusion distance is the distance allowable for the intruder to move before it is detected by the WSN. The intrusion detection application is basically concern with how fast intruder can be detected .If all the sensor nodes that are deployed at boundary are of high

density then intruder can be detected immediately as it approaches to network area. The distance between the entrance and detection of intruder is of central interest. We have taken intrusion distance of 50 meters in our simulation model.
In order to detect the intruder it must be in the sensing range of any sensor (S). If any intruder travels the distance of 50 meters before it is being sensed by any sensor then this intrusion distance and sensor's sensing range actually determine the intrusion detection area.
The intrusion detection probability is defined as the probability that an intruder is detected within certain intrusion distance specified by WSN.
In order to give the better results we have applied ACO in heterogeneous environment of WSN .Ant colony is basically a optimization technique the one benefit of the optimization techniques is that we can get optimized results within five or ten minutes which cannot possible with mathematics operations and hit and trial operations. Nowadays these techniques are widely used and most common in various fields.
We are using the concept of degree of freedom =10 for better and effective deployment of type1 sensor in heterogeneous environment of WSN to detect the intruder at very first point of occurrence on the network boundary or within the network domain itself. At first search limits are considered to apply ACO and in this paper searching area is that area in which low range sensors are deployed so that after finding the locations low range sensors are replaced by high range sensors. Initial step is performed by initializing 500 ants and hive location is taken at the centre. According to degree of freedom =10 sensors, it means that we have to replace 10 low range sensors with high range sensors among all sensor nodes and degree of freedom means each ant has 10 locations and out of which best location is selected, best means that has longer distance from the centre as we have to place high range sensors at boundary so the location which is farther from the centre is considered as best. The parent food value is calculated by applying distance square root formula in between current node and current ant from this nearest distance is calculated from which parent food value is calculated, parent food value is the sum of all the nearest distances, all the initialized ants are called parent ants. Next step is mutation process and same steps are applied again to get more suitable values according to our requirement here child ants and child food value are evaluated. Further steps involve the selection of best fitness value and elimination of that values which are not required it means the rejection of those sensor nodes that are not suitable to deploy at boundaries. We have calculated the distance between current ants and current nodes then nearest distances are calculated and sum of all the nearest distances is obtained to find maximum parent food value and child food value. By applying selection and elimination we obtained maximum values that satisfy the basic requirements. After finding best locations low range sensor are replaced with high range sensors here we have optimized the distance and all the nearest distances are added to obtain maxima and this whole process of ACO has gone through 300 iterations to give best results. Ant colony optimization technique has following major steps:

- Initialization of population: Initialization of ants and these are called parent ants.
- Mutation process: Formation of child ants
- Selection process: Selection of best values
- Crossover process: To get better results values are cross multiplied with each other.
- Elimination process: To eliminate unnecessary values.

Fitness value is the actual result that consist of maximum food value .To find the best fitness function, values are arranged in ascending or descending order in order to find maxima and minima in this paper we obtain maxima to get better results.
The benefit of this approach is that Type1 sensor with long sensing range ,transmission range and long battery life can effectively deploy at the boundaries of square area A=(LXL) and intruder can be detected more fast at the entry point of region.
The mathematical formula is given below.

$$\mathbf{D=}\sum_{j=1}^{j=nodes}\sqrt{(\mathbf{Pxi}-\mathbf{Nxj})\text{^}2+(\mathbf{Py}-\mathbf{N}}$$

Here, P_x and P_y are the position of current ant and N_x and N_y are the positions of current nodes.
In this way distance between current ant and current nodes is calculated from which all the nearest distances are created which helps in changing the location of the sensor nodes i.e. high density sensor nodes are placed at boundaries..
Hence, intrusion detection can be made fast and maximum food value is calculated.

4. Results

Our IDS is imposed on both homogeneous and heterogeneous WSN models. In homogeneous WSN range of sensors is varied from 10 to 100 meters to generate results and results are given below: We have calculated detection probability in terms of range of sensors.

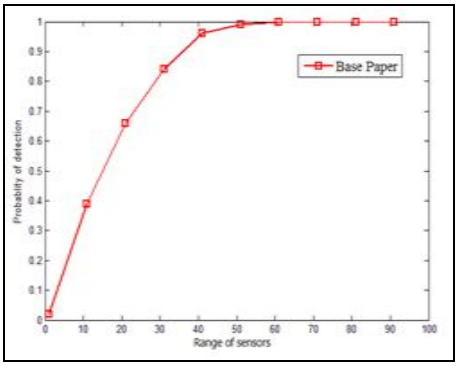

Figure 3: Detection probability in Homogeneous WSN

On the other side for heterogeneous environment range of sensors is varied from 10 to150metres .It is the graph related to new technique applied to improve performance. Here ant colony optimization technique is applied and it has shown better results as compared to previous technique in which sensor nodes near the base station replace themselves with last ten entries of low range sensors. In our work we have replaced 10 best locations among all sensor nodes and place them at boundary to make detection probability better and results are given below and also the improvement is shown as compare to previous techniques.

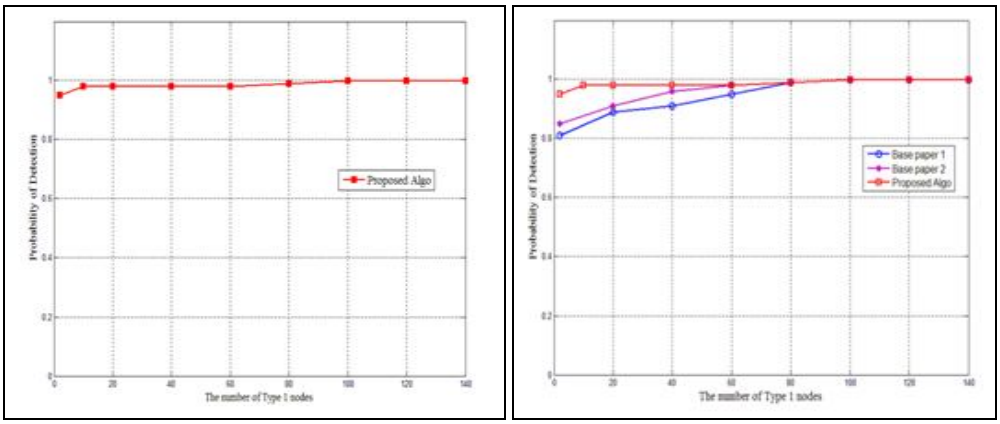

Figure 4: Detection probability in Heterogeneous WSN
Figure 5: Improvement as compared to previous work

From the above results it is noticeable that there is a significant rise in the detection probability of an intruder so this is an interesting technique which provides better results as compared to previous work.
To evaluate the energy consumption we have developed an energy simulation model. In our simulation model for both homogeneous and heterogeneous sensor nodes are randomly deployed with same battery life in square area of 1000X1000 meters in 2D grid pattern. Each cluster has diagonal distance of 200 meters. The sensors which are placed near the boundary they have to detect the intruders and then send the information to base station.
We have calculated the energy consumption of a sensor node to in terms of intruder motion. Sink position is taken at the centre.

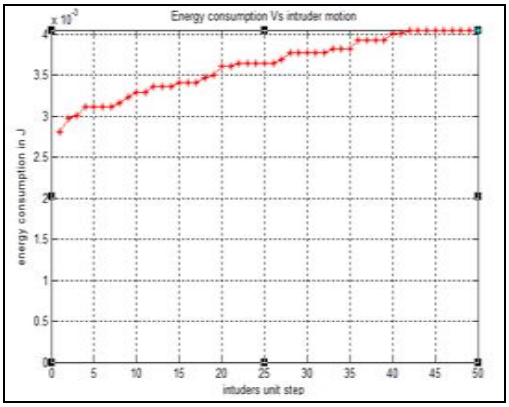

Figure 6: Energy consumption

5. Conclusion

It is clear from the grid pattern deployment is that better results are obtained from this approach. A n intrusion detection model is implemented and evaluated for both homogeneous and heterogeneous network models .It was programmed in matrix laboratory programming language and intruders coming towards network domain are identified from that detection probability in terms of range of sensors is evaluated. By applying ACO the detection probability gives better results as compared to other previous work. It gives better performance by applying this new technique and detection probability is increased.

6. References

1. Kazem Sohraby Danial Minoli Tyab Znati " wireless sensor network technology ,protocol and application".
2. Dekan Refernt Korrefernt "Intrusion prevention and detection in wireless sensor networks"2008.
3. Murad A Rasam Mohd . Aizaini maroof and Anazida Zainal "A novel intrusion frame work for wireless sensor network".
4. Dilip Kumar Trilok C. Aseri R.B.Patel "Energy efficient heterogeneous approach for wireless sensor network".
5. Bhaskar Krishna machari "Introduction to wireless sensor network"
6. K.Thanigaivalu Dr D Morgin "Impact of sink mobility on network performance".2009
7. A Shakil ahmed, Dr A Rajeshwari "Intrusion detection in heterogeneous environment with energy efficient localization algorithm".2012
8. Srinivasaraju Dantuluri and Poturaju "Intrusion detection in single sensing and multiple sensing domain"
9. Kung and vlah "Intrusion detection by using hierarchical tree structure"
10. Absar-ul-hasn Ghalib A. Shas and Ather Ali "Intrusion detection system using wireless sensor network"
11. Deying Li Hai Liu"Sensor coverage in wireless sensor network"
12. Hanif D Sherali Scott F. Midkiff "Energy provisioning and relay node replacemaent"
13. Hossin Jadidoleslamy "High level intrusion detection for heterogeneous wireless sensor network"2009
14. Ismail Butan Salvatore D. Margora and Ravi Shankar "A survey of intrusion detection systems in wireless sensor network".
15. Saber Banihashemian Abass Ghaemi Bafgi "A new key management scheme in heterogeneous sensor networks."
16. Sandeep kumar Nishant Chaorasia Pragaya Sharma "Intrusion detection using datamining."2013
17. Ajay Jangra Richa, Swati, Priyanka "Wireless Sensor Network (WSN): Architectural Design issues and Challenges" 2010.
18. Jenifer Yich Bishwanath Mukharjee Dipak Ghosal "Survey on wireless sensor network".
19. Chris Karlof David Wagner "Secure routing in wireless aensor netqorks security against attacks".
20. Souma benerjee Crina Grosan Ajit Abrahm and P.K Mahanti "Intrusion detection in wireless sensor networks using emotional ants"