International Journal of Engineering & Technology, 7 (4.5) (2018) 657-661

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Intrusion detection using ant colony approach in wireless sensor networks

Jayashree Agarkhed [1] *, Gauri Kalnoor [2]

[1] *Professor, Department of Computer Science & Engineering, PDA College of Engineering, Kalaburagi, India*
[2] *PhD Research Scholar, Department of Computer Science and Engineering, PDA College of Engineering Kalaburagi, India*
**Corresponding author E-mail: jayashreeptl@yahoo.com*

Abstract

Design of an intrusion detection system in the sensor network to improve the behavior of the network is the major challenge is theVariety of intrusion detection mechanisms are being used now a days, to provide security in Wireless Sensor networks (WSN). Since WSN works with set of tiny nodes called as sensor nodes, there are high chances of intrusions for malicious attacks. WSN is deployed in medium open to many users wherever possible. A multiple sensing environment of WSN consists of sensors which acts as agents called as multi agents system for detecting an intruder. Ant colony is an effective approach where each agent communicate with each other for updating the information of intruder to the colony administration. The multi agents based system is best phenomenon suitable for optimization of ant colony. In this approach, the ants form a colony where it goes for search continuously until an intruder is found and once searched, it returns back with the best shortest path available with path traces stored in its database for its future reference. An optimized multi agent approach using ant colony is proposed for detection of lightweight intruders for WSN to protect against harmful malicious attacks.

***Keywords**: Intruder Attacks; Lightweight Intrusion Detection; Multi Agent System; Ant Colony; WSN, Multi Sensors.*

1. Introduction

The applications of WSN mainly consists of healthcare systems, traffic and environmental monitoring, surveillance of battlefield and so on. Some of the salient features [1] of WSN are communication and broadcast in short range, self-organizing, sensors deployed densely and co-operative, change in topology of network frequently because of fading and failure of nodes, multi-hop routing, and resources for computation are very limited mainly memory and energy.

Most of the organization's important asset and more precious is the information stored in large databases in many different forms. The information is stored and whenever required, it is processed through the systems that are based on network. WSN has become one of the most interesting research area [2] now days. To protect sensor network is the main aim of the proposed approach.

The result of an attack by intruder is information loss or damage, which is confidential, thus affecting the business or an individual user. One of the best example for intruder attack in WSN is the theft of the file or data by accessing the resources without authorization. The unauthorized user can decrypt the encryption privacy key used for securing the data in wireless network easily. After the decryption of the key, the attacker uses the access point of wireless network illegally. The hacker gets access to corporate the network resources as the entire network becomes compromised with unauthorized access.

An intruder is an unauthorized user or the activity, which is considered to be unwanted in the wireless network. The Intruder Detection System (IDS) provides detection of an intruder [3] and alerting the network or system regarding occurrence of intrusions. The IDS also detects the deviations in security violations which are non-permissible. The IDS can be a network based or host based for monitoring the logs or packets flow through network. The most common attacks in WSN are jamming of signal or eavesdropping. WSN [4] is mainly deployed and designed for detecting events and hence for the collection of data and the return back to data sensed to the users. The common mechanism for prevention of intruder is intrusion detection system. But the lightweight IDS based on multi agent system using ant colony approach can detect about 90% of the malicious attack along with detection of collision of packets. A framework for distributed IDS is designed to update, create and evaluate packets alert in WSN. Based on the knowledge of neighbors and the rules for routing [5], the attacks occurred and common problem of routing can be detected. The rate of detection under burst and strong attacks is high in this framework. By introducing reduction in alerts, less consumption of energy is achieved.

A detection model based on signatures is designed including the techniques based on signature recognition. This technique mainly depends on the matching of known patterns and thus intrusions are identified efficiently providing less complexity of implementation. Anomaly based model can also be designed for detection of an intruder based on activities of nodes observed and can also detect unknown patterns. The IDPS components for detection and prevention of intruders is shown in the figure 1[6].

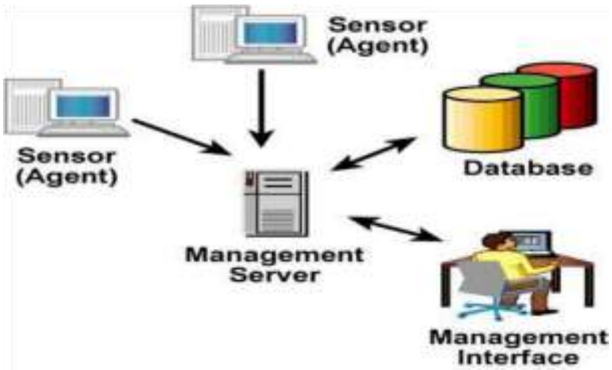

Fig. 1: Components of IDPS.

Agent mainly analyzes the events and then listens to them so that the activities of the system can be carried out. The agents are used to detect intruders. They are called as sensors in WSN. The management server analyses the information received from the activities currently in progress.

2. Related work

In this section, we will discuss the work carried on, by many researchers in WSN. Survey has been done extensively for mechanisms to detect intruder in WSN.

A model called as classification of threats is introduced in [7] by authors which explains the development of surveillance system for security by monitoring the network. Based on the behavior of the user, the anomalies are detected. The authors in [8], based on the development of IDS, statistical observation has been made, and proposed many different models based the statistics obtained.

The network based on naïve Bayesian classification is employed to develop IDS based on anomaly for detecting an intruder on bursts of traffic. This mechanism was proposed by authors in [9]. An approach based on Bayesian classifier called multisensory fusion was proposed by authors in [10], which includes the suppression and classification of false alarms. The sensor's outputs of different IDS are combined and aggregated for a single alarm production.

A Fuzzy Intrusion Recognition Engine (FIRE) technique was developed for data to be processed in the network using fuzzy logic and fuzzy sets are generated using Support Vector Machine (SVM). Once the sets are fuzzified, the process of defuzzification, fuzzification leads the result of final decision of fuzzy systems. A biological and efficiently inspired model for learning called Ant colony model for clustering is designed as discussed by the authors in [11]. An evolutionary algorithm for learning is discussed by authors in [12] known as ant colony algorithm for optimization. This algorithm can be applied for solving combinatorial problems for optimization. A task for classification in data mining is proposed by the authors in [13] which is based on the system of ant colony. The Ant Miner assigns each class to a record among the set of classes predefined mainly based on the values of predictor attributes (also called as antecedent attributes).

In [14], the authors have proposed a different ant colony approach for solving the problem energy consumption in WSN. In this modified approach, the process of many mime ants are used to determine the shortest path which in turn reduces energy consumption. This route is considered as most energy efficient. Based on the energy level, the cluster heads are selected for this modified technique.

The authors in [15], have proposed a new algorithm that determines the low power state of sensor node. The two states of sensor nodes are sleep state and active state. When there is no transmission between the nodes, the radio of sensor nodes are turned to sleep state saving power consumption. The data packets are being transmitted between nodes, and the node's state changes to active state.

In [16], an Ant Colony Optimization (ACO) algorithm is presented for WSN. This algorithm uses multipath data transmission whenever there is node failure. The error message of route is sent to the previous node whenever node failure occurs. A substituted path is then found by the previous node to reach the destination. The value of pheromone in ACO is set to zero, when the error message occurs, thus deactivating the current path.

3. Framework of lightweight intrusion detection in sensor networks

In this section, the framework for intrusion detection in sensor networks is explained with its architecture and algorithms for detection.

In sensor networks, the management of power, data dissemination and multiple protocols for routing are designed considering computational and energy resources as essential part of the design. To achieve savings of power, scalability, and redundancy in routing of data, the routing protocols for sensor networks based on clusters is developed. The two phases of routing are setup phase and steady phase. In the first phase, the clusters are organized and the heads of clusters are selected randomly, that is rotated for distribution of load of energy among the network of sensors. In the next phase called the steady phase, all the data received by the cluster heads in their clusters, is aggregated and sent to the base stations. This reduces the amount of information gathered at the base station.

In the proposed architecture, each node belongs to a single allocated cluster among the set of clusters that are distributed geographically across the entire network. The main objective is to share the information, thus improving the capability of detection of an intruder for each nodes participating in the network.

Every IDS agent is designed in the sensor node individually classified as local agent and global agents. The multi-agent based system consists of IDS agents that are active only whenever needed, to save the battery life of the sensor nodes. An internal database is exists in every node to store the data that is monitored for sending and receiving of data. This database is called as the blacklist that contains malicious nodes specifically in the network. Once the initial configuration of the network takes place, the knowledge of malicious nodes lacks in the sensor nodes. Once the WSNs are deployed, the database consisting of signatures is constructed. An entry made in the database of malicious nodes, is constructed and then propagated by the cluster heads to individual nodes. The communication between neighboring nodes is monitored by the global agents, because WSN has the nature of broadcasting every packets within its communication range. A mechanism called as watchdog monitoring is used and the rules for predefined routing so that the packets can be monitored using the knowledge of two-hop neighboring nodes. An alert is created and sent to the CHs, whenever the monitoring nodes realizes that the potential breach for security is going to take place in their range of communication network. Figure 2 shows the agents of intrusion detection on protocol stack of a sensor.

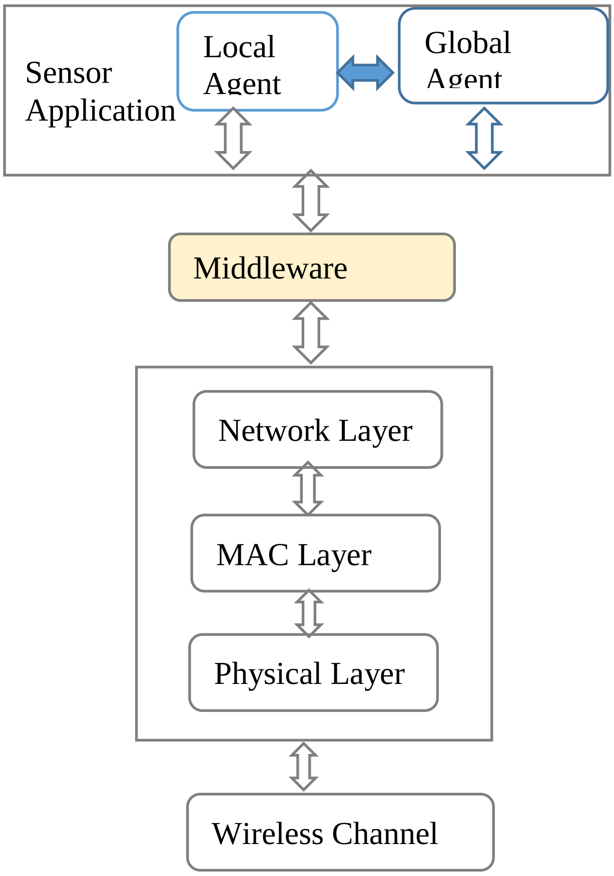

Fig. 2: Intrusion Detection Agent on Protocol Stack.

In figure 2, the sensor application consists of local and global agents. An algorithm is designed for detection of an intruder using a framework of lightweight IDS in sensor networks.

```
Algorithm: Intrusion detection algorithm (at monitoring nodes)
$\text{Detection\_Global}(\text{packet}_i)$
$\text{if detecting}(\text{packet}_{i_{ID}}, \text{buf})$
$\text{then \{ if verify}(\text{node}_{ID}, 2 - \text{hop} - \text{neighbor's list})$
else
$\text{verify}(\text{rules}_{\text{predefined}}, \text{packet}_i)$
{
$\text{generate}(\text{alert});$
 $\text{send}(\text{alert}, \text{cluster}_{\text{head}});$
}
```

Once the sensor nodes are deployed in the needed field of environment, we assume that the adversary requires specific time to deploy his/her attack. This implies that there is no single malicious node at the time of deployment in the initial stage. Some nodes are elected as monitor node or guard node that uses the mechanism of monitoring called watchdog. A set of rules that are predefined are used with a knowledge of two-hop neighbour with the particular range of transmission. The packets are received by the monitoring nodes which are within their radio transmission range. These received packets are buffered in the database with information type of packet, packet id, source and destination. The buffer has entries with each having a tag of timestamp. Thus, the node id and lists of two-hop neighbours are verified.

The algorithm below explains the mechanism to activate the nodes while monitoring or guarding.

```
Algorithm: Activate nodes monitoring
Step 1: Listen to the tansmitted packets
Repeat
Step 2: Check the packet header
Step 3: $\text{if( ID} = \text{dest}_{id})$
$\text{if( Detection\_Local}(\text{packet}_i) \text{ then}$
drop packets
else
recieve packets
endif
Step 4: $\text{if}(\text{source}_{ID}, \text{dest}_{id}, 1_{\text{hop}_{\text{neighbour}}})$
$\text{Detection\_Global}(\text{packet}_i)$
else
drop packets
Step 5: Repeat Until no transmission
```

A two-hop neighbour list and malicious nodes stored known as blacklist are the two databases which sensor nodes maintain. Every node transmits and broadcasts the hello packet [17] before original packets that contains information are sent. The hello packet consists of fields with source-id, node-id and hop-counter. The monitoring node becomes active once it listens to the packet transmission initializing the hello packet and starts verifying the id. If malicious node is detected by local-detection agent, then an entry is made in the blacklist database. Then, the CH generates a new rule and propagates to all clusters through CHs.

4. Ant colony approach in WSN

In this section, the approach of ant colony in sensor network is discussed. It is one of the efficient approach for intruder detection for improving the accuracy of detection and its performance.

The technique using ant colony is a probabilistic method which is based on solving problems computationally and finds better paths based on the real ants strategy. An agent is considered to be each ant that is real or artificial and communicates with remaining ants directly or indirectly, thus optimizing the changes of the environment of WSN.

The initial stage of ant colony approach is to search for the best and optimal path along the graph. It can be traced based on the ant's behavior introducing the path between their colony created and the source of food [18]. The highlighting features of the ant colony are solution to high precision and optimal convergence globally.

The algorithm discussed below explains this approach for detection of an intruder in WSN.

```
Algorithm: Ant Colony algorithm
Step 1: Start
Step 2: Initialization of pheromone traces
Step 3: While (stop condition is false) do
For every ant do
Ant deposition randomly
While (incomplete solution) do
Choose randomly next element based on
Pheromone trail.
End while
End for
Pheromone trail Update
End While
Step 4: Stop
```

In the algorithm, the data set is generated as an input so that the performance is compared with other methods of intrusion detection. Next, the fuzzy based rules, if-then rule can be applied so as to increase the rate of accuracy and interpretability in the model of detection. Based on the values of training, datasets are selected among set of given data. An ant colony method is applied on the dataset. The test is applied on the collected data set. Values of Rate of detection and false alarm rate is computed. Finally the results are obtained based on the performance measure.

The framework is designed for the proposed scheme with a goal of improving the performance of WSN. The detection rate of attack is increased with accuracy and false alarm rate is decreased based on the proposed scheme. The ant colony algorithm is applied to search the best optimal path with update in counter of malicious nodes. The flowchart of the design work is shown in figure 3.

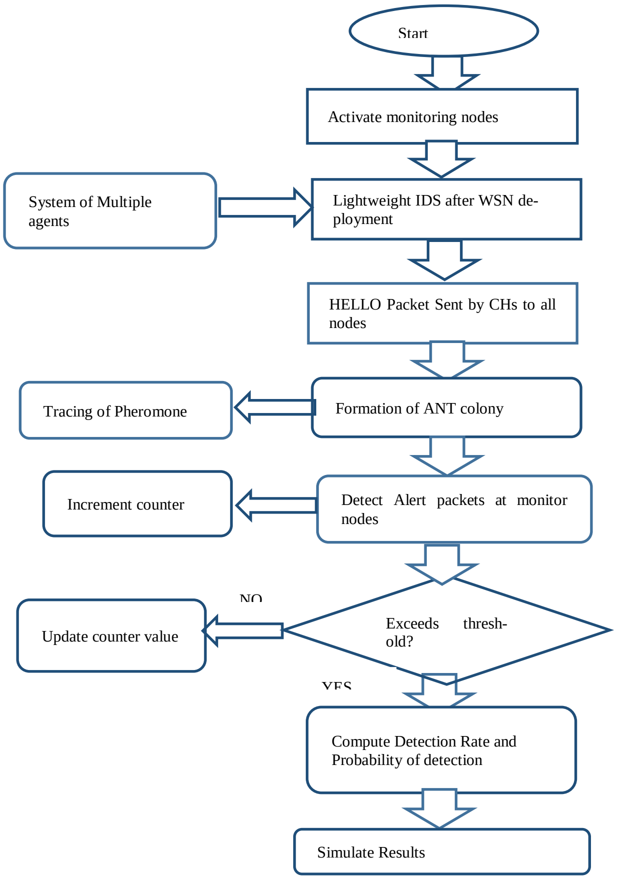
Start
Activate monitoring nodes
System of Multiple agents
Lightweight IDS after WSN deployment
HELLO Packet Sent by CHs to all nodes
Tracing of Pheromone
Formation of ANT colony
Increment counter
Detect Alert packets at monitor nodes
NO
Update counter value
Exceeds threshold?
YES
Compute Detection Rate and Probability of detection
Simulate Results

Fig. 3: Framework of Proposed Work.

5. Performance analysis

The aggregation and the detection computation is performed by CHs for each cluster in WSN. The alert messages are also aggregated and counter for alert is computed every time in each malicious node. A threshold value is set for malicious counter, and if the value in the monitor node exceeds this threshold, the revoking of sensor nodes takes place from the respective cluster and finally from WSN. The parameters $(\alpha, \beta, \delta, \varphi)$ are associated with the packet of alert that are incoming at monitoring nodes of WSN. The different levels of trust of alert packet entering at node that monitors at $\lambda = 0$ is designed. The counter of an alert at a malicious node can be computed using equation 1.

$$MC_{node} = \beta \sum_{j=1}^{i} i + \delta \sum_{k=1}^{k} j + \varphi \sum_{i=1}^{l} k \qquad (1)$$

Where, $0 < \beta < \delta < \varphi < 1$
i, j, k are the number of alert packets
The probability that attack occurred by an intruder can be detected is based on the factors: number of nodes monitoring, probability that the detection may be missed by a monitoring node, and the counter for malicious nodes with its threshold value as shown in equation 2.

$$P_D = P_X + P_{X+1} + \cdots P_K \qquad (2)$$

Where,
P_D : It is the probability of events being detected out of K nodes, at most more than X number of nodes sends and alert packet to CH.
Probability of detecting an attacker using Ant Colony approach designed in lightweight intrusion detection is computed using equation 3.

$$P_D = (1 - P_C)^X {P_C}^{K-X} + \cdots + (1 - P_C)^K {P_C}^{K-K} \qquad (3)$$

6. Results

In this section, the results are discussed that contains Detection Rate (DR) and False Alarm Rate (FAR) of individual values of data samples using Ant Colony (AC) approach. Performance results is compared with other methods such as Support Vector Machine (SVM) and Naïve Bayesian Classifier (NB).

Data Values	DR (%) for AC	FAR (%) for AC	DR (%) for SVM	FAR (%) for SVM
0.22	95.01	1.72	90.97	5.10
0.40	96.11	1.76	91.03	5.04
0.55	98.20	1.79	91.80	5.50
0.68	99.50	1.82	92.04	6.01

7. Conclusion

The sensor network is deployed in an unattended environment and thus the main goal is to detect an intruder using the best possible approach. The ant colony approach is used by searching the best trace of pheromone. This approach is used in lightweight IDS where number of monitoring nodes are elected in each cluster of WSN along with the CHs. A multi agent system is proposed as local agents and global agents while activating all the guard nodes of the network. The results are computed with improving performance of the network. The detection of an intruder can be estimated up to 99.99% accuracy.

References

[1] J. Han and M. Kamber, (2011) "Data Mining:Concepts and Techniques Slides for Textbook — Chapter 7 " Intelligent Database Systems Research Lab School of Computing Science Simon Fraser University, Canada ,October 15.
[2] Md. S. Abadeh, J. Habibi, (2010) "A Hybridization of Evolutionary Fuzzy Systems and Ant Colony Optimization for Intrusion Detection", Volume 2, Number 1 (pp. 33-46), Department of Computer Engineering, Sharif University of Technology, Tehran, Iran.
[3] Y. Shi, ;(et.al.), (2011) "Optimization Based Data Mining:Theory and Applications" Chengdu, China, Springer- Verlag London Limited, pp 18-134.
[4] M. Glick, A. Klon, P. Acklin, and J. Davies, (2011) "Enrichment of Extremely Noisy High-Throughput Screening Data Using a Naïve Bayes Classifier", Journal of biomolecular Screening, Published by:http://www.sagepublications.com, in August 6.
[5] LK. Behera and A. Sasidharan, (2011) "Ant Colony Optimization for Co-operation in Robotic Swarms", Pelagia Research Library Advances in Applied Science Research, 2 (3): 476-482.
[6] HA. Zurba T. Landolsi, Md. Hassan and F. Abdelaziz, (2011), "On the Suitability of Using Ant Colony Optimization for Routing Multimedia Content over Wireless Sensor Networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks Vol.3, No.2, June.
[7] Mei-Ling Shyu and Varsha Sainani, ―A Multiagent-based Intrusion Detection System with the Support of Multi-Class Supervised Classification.
[8] Marco Dorigo and Thomas Stützle ―Ant Colony Optimization
[9] T. Singh, (2010) "Thesis work on: Ant Colony Optimization (ACO) based Intrusion Detection System" CSE dept Thapar University, patiala, India.
[10] Vijay Srinivasan, John Stankovic, Kamin Whitehouse,"Using Height Sensors for Biometric Identification in Multi-resident Homes", Pervasive Computing, eighth International Conference, Pervasive 2010, pp. 337-354, Helsinki, Finland, 2010.
[11] A.P.N Fahmi, "Hey Home, Open Your Door, I'm Back! Authentication System using Ear Biometrics for Smart Home, "International Journal of Smart Home, Vol. 7, No. 1, 2013.
[12] M. Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification," Department of Computer Science, Purdue University, 2011.
[13] Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energyefficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, vol. 1, no. 1, pp. 57-65.

[14] Swati Bartariya, Ashutosh Rastogi, and Security in Wireless Sensor Networks: Attacks and Solutions, IJARCCE, Vol.5, Issue 3, March 2016.

[15] Rajevv Arya, S.C. Sharma, Analysis and optimization of energy of sensor node using ACO in wireless sensor network, Science direct, 2015.

[16] Kamaldeep Kaur, Parneet Kaur, Er. Sharanjit Singh, Wireless Sensor Network: Architecture, Design Issues and Applications, IJSER, Volume 2, Issue 11, November 2014.

[17] Rodrigo Roman, Jianying Zhou, and Javier Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks".

[18] S.V. Sheela and P.A Vijaya, "Iris Recognition Methods - Survey" International Journal of Computer Applications, Vol. 3, No.5. pp. 19 25, June 2010.