Secure routing in wireless sensor network using ACO

Aishwarya Vaibhav, Ayush Jaiswal, Himani Singh and Dr. Dilkeshwar Pandey
Department of Computer Science & Engineering, ABES Institute of Technology, Uttar Pradesh, India

ABSTRACT : Wireless Sensor Network is very commonly used now a days in varying domains. It is used in defense, medical sciences, smart cities and many more places. In this paper, we discuss about the security improvement for the existing WSN by analyzing all the attacks prevailing and the best approach to minimize a vast range of attacks including Sybil attack, wormhole attack and many others. We incorporate the Ant Colony Optimization to gain energy optimized clustering and securing the network with various attacks done to compromise the network.

KEYWORDS: Wireless Sensor Network, Ant Colony Optimization and Security.

I. INTRODUCTION

The routing protocol plays a very crucial role in scheming, picking and determining the applicable path for transferring the data from the source to the destination productively. There are many routing algorithms used to determine the shortest path and increase the output of the network.

In this paper, we will explain the algorithm for selecting the shortest optimal and secure path for transferring the data packets. The aim of any network routing algorithm is to relay the packets between source and the destination enhancing the network performance. The performance measure usually taken into consideration is the output and the number of packets efficiently reaching the destination. However, we have taken the performance measure as the resistance to various attacks.

1. **Network Routing**-

Network Routing can be defined as the process of selecting a path for traffic in a network, or between or across multiple networks. Routing can be performed for different networks, like circuit-switched and packet-switched networks. The example of circuit switched network is the phone network in which the physical circuit is set up at the communication start and remains the same for the whole communication duration. Unlike circuit-switched, in packet-switched networks, also known as data networks, every one of the data packets can follow a non-identical route and no stable physical circuits are established. The example of data networks are Local Area Networks and the Internet. Here we will emphasize on data networks.

The most important function of the data networks is to make sure that there is efficient distribution of information among the users. This is done through the wringing of the network control system. One of the most important components of control system is routing. Routing refers to the scattered activity of building and using routing tables.

All routing algorithms use routing table. The table is used to withhold the information to make the local forwarding decisions. A routing table is sustained by each node in the network. It communicates with the nodes incoming data packets which are linked to use next in order to continue its movement to the destination node of that data packet.

However, one of the most important feature of the network routing problem is that it is always moving (non-stationary). Which means that, one of the routing distinctive feature is that the traffic over the network changes from time to time. Adding to that, the nodes and links of the network can instantaneously go out of the service, and the new nodes and links can be added at any moment. All these features have to be kept in mind in order to create an optimal solution to network routing problem. The problem of shortest path.

1.1 Shortest Path Routing

Shortest path routing is the implementation of the shortest path algorithm on finding a solution to the network routing problem. Its motive is to determine the shortest path (minimum cost) between two nodes, where the total sum of the costs of its constituent edges is minimized.

Till now, there have been many routing algorithms for solving shortest path that have been accepted. One of them is Dijkstra's algorithm. Dijkstra's algorithm, conceived by Dutch computer scientist Edgar Dijkstra in 1959, is a graph search algorithm that resolves the single-source shortest path problem for a graph with non-negative edge costs, producing a shortest path tree. For a defined source node in a graph, this algorithm finds the path with minimal cost (i.e. the shortest path) between that node and every other node. This algorithm can also be used for finding costs of shortest paths from a single node to a single destination node by terminating the algorithm once the shortest path to the destination node has been gained. As per example, if the nodes in the graph constitute to states and edge path costs constitutes driving distances between pair of states connected by an undeviating road, Dijkstra's algorithm is used to find the shortest route between one state and all other states. Because of this, the shortest path first is widely used in network routing protocols.

As we have stated, network routing is of similar nature and nodes and links of the network can suddenly break, as well as the new ones can be created. Therefore we have Open Short Path First, which is a determined routing protocol and keeps track of the whole network topology and all the nodes and the links within that network.
In inclusion to this, if for some time the optimum route intersects within the network, and instantaneously the link failure occurs, the Open Short Path First will recognize it very quickly in the topology and will intersect on the new loop-free routing structure. Concluding, we now have convergence as one of the probable problems to solve in the following sections as well as in the implementation we prepared.

2. **Ant Colonies**

Ant colony optimization (ACO) is an algorithm based on the behavior of the real ants in finding the shortest path from a source to the food. It uses the performance of the real ants in the process of searching for the food. We have observed that the ants accumulates a definite amount of pheromone in its path while they travel from the nest to the food. As they return to the nests, ants tend to follow the same path as marked by the pheromone and again deposit the pheromone on its path. In this way the ants following the shorter path are expected to return earlier and hence increase the amount of pheromone deposit in its path at a faster rate than the ants following a longer path.

However, the pheromone is subjected to evaporation by a certain amount at a constant rate after a certain interval and therefore the paths visited by the ants frequently, are only kept as marked by the pheromone deposit, whereas the paths rarely visited by the ants are lost because of the lack of pheromone deposit on that path and as a result the new ants are intended to follow the frequently used paths only.
Now, all the ants starting their journey can learn from the information left by the previously visitor ants and are guided to follow the shorter path directed by the pheromone deposit. In ACO, a number of artificial ants (which mimic the data packets) build solutions to the considered optimization problem and exchange information on the quality of these solutions via a communication scheme that is pheromone deposit on the path of the journey performed.

II. OBJECTIVE

We aim to enhance the security measures currently prevailing to ensure proper functioning and secured data transmission between the nodes and base station while keeping in mind all the constraints existing in the Wireless Sensor Network nodes.

III. PROBLEM DOMAIN

A wireless sensor network contains a large number of sensor nodes which are inherently resource-constrained. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These limitations are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. If we have to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes.

IV. METHODOLOGY

ACO algorithms is applied in the network routing problems to find the shortest path. In a network routing problem, a set of ants (packets) are simulated from a source location to the destination. The ants that are in the front chooses the next node randomly gathering the information from the routing table and the ants who are successful in reaching the destination are updating the pheromone deposit at the edges visited by them by an amount (C/L), where L is the total path length of the ant and C a constant value that is adjusted according to the experimental conditions to the optimum value. This will help the coming set of the ants learn from the pheromone deposit feedback left by the previously visited successful ants and will be guided to follow the shortest path.

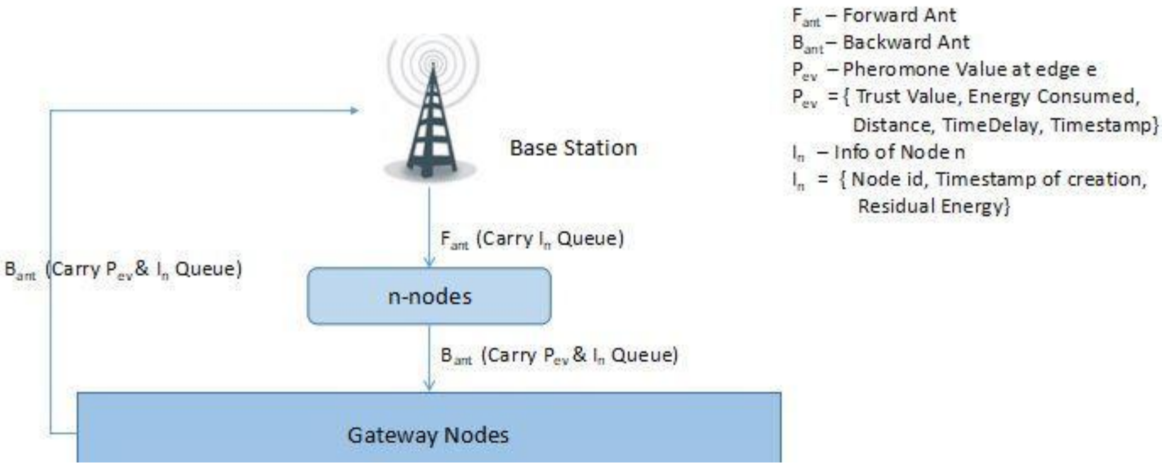

Fig 1 - Setting up the cluster and routing table

The probability that the ant will select a node y from node x is given by the following formula:

$$P_{xy} = \frac{T_{xy}^{a} . n_{xy}^{b}}{\sum T_{xy}^{a} . n_{xy}^{b}}$$

Now if here, if the link created between two nodes exists, otherwise the $P_{xy} = 0$. Here, Txy is the pheromone value of each edge which connects the nodes x and y. $n_{xy} = (1/d_{xy})$, here d_{xy} is the total distance between the nodes x and y. a and b are two stances which determine the relative influence of the pheromone trail and the heuristic information.

The most important characteristic of the ACO is that the pheromone values are refreshed by all the ants (packets) that have reached the end location with success. But the thing is, before affixing the pheromone values we must first perform the evaporation action. Pheromone evaporation (p) on the edge between node x and node y is implemented by the formula:

$$\mathbf{T_{xy} \leftarrow (1 - p)T_{xy}}$$

Thus, every instant of time, t = {1,2,3,4...n} represents one iteration where all the ants in the colony will perform one move towards the selected node. That is why, after we take that in the consideration, all the ants will, after n iterations, find the solution and leave the pheromone calculated by the following formula:

$$T_{v}(t+n) = P.T_{v}(t) + \Delta T_{v}$$

ΔT_{xy}^{k} is the amount of pheromone ant k deposits on the edges visit. It is calculated by the following expression:

Here c^{k} is the actual total cost of all the edges that an ant (k) has passed on its journey from the starting point of location to the destination node. This will allow for the superior ant to leave more pheromone on the edge which is the route on the shortest path.

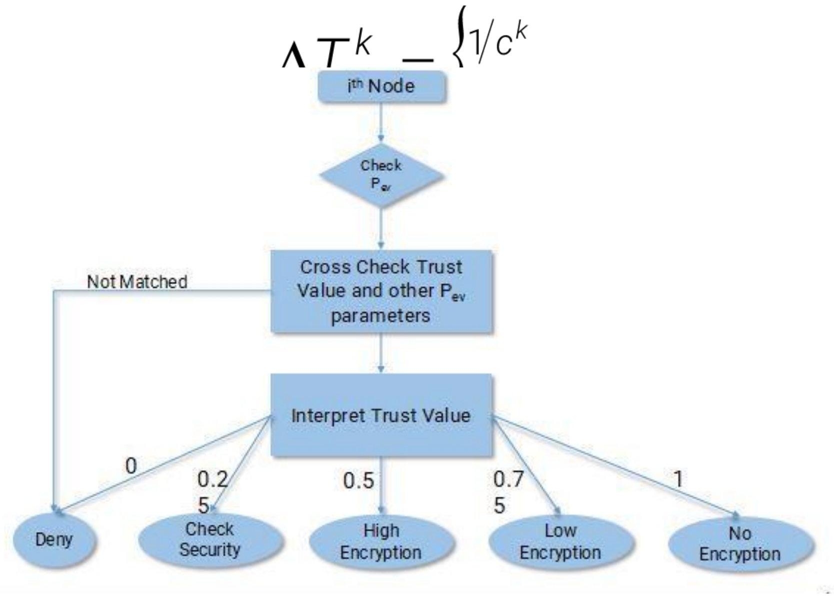

Fig 2 - Interpretation of Pheromone Value

Another advantage of the implementation of the ACO in network routing is that whenever the number of packet increases, ACO algorithm can be executed for managing crowding too. In static routing algorithm all the packets from a starting node to the destination node will after some time follow a constant path calculated by the algorithm and therefore we can have a problem with crowding. And the result would be that, some of the packets will have to wait. However, in ACO as the next node will be selected randomly, with the probability to choose the shortest path more, some packets will choose some other paths which increases the network performance and fights crowding.

With respect to this, in dynamic situations, if after a little time the shortest path converges and suddenly we get the link failure and disconnection between two nodes which are on the route of the shortest path, the ACO will quickly follow some other path and converge on it.

V. CONCLUSION

This research paper contributes a new approach to optimize and securing the existing Wireless Sensor Network. With the use of proposed methodology we can prevent most of the attacks and many other attacks which are not common at the moment.

VI. FUTURE SCOPE

For the further consideration,

- Increased security will lead to extensive use of WSN.
- Reliability, confidentiality and availability of the network will be enhanced.
- Reduce instances of false alarms by WSN.

VII. **REFERENCES**

[1] Chris karlof, Naveen Sastry, David Wanger, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Proceedings of the 2nd international conference on Embedded networked sensor systems,November 3-5, 2004, pages 162- 172,Baltimore, Maryland, USA. ISBN:1- 58113-879-2.

[2] Siva D. Muruganathan, Daniel C.F. MA, Rolly I. Bhasin, Abraham O. Fapojuwo,"A Centralized Energy- Efficient Routing Protocol for Wireless Sensor Networks", IEEE Communications Magazine. Vol. 43, no. 3, pp. S8-13. Mar. 2005.

[3] Kirk H.M. Wong, Yuan Zheng, Jiannong Cao, Shengwei Wang," A Dynamic User Authentication Scheme for Wireless Sensor Networks", IEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing (SUTC"06), 2006.