An Ant Based Compromising Path Approach to Avoid Selfish Node Attack in Mobile Networks

Monika[1] and Nasib Singh Gill[2]

Department of Computer Science & Applications,
M. D. University, Rohtak, Haryana
E-mail : moni.ms25@gmail.com and nasibsgill@gmail.com

Abstract: **Each network suffers from different kinds of active and passive attacks. But in case of sensor network this problem is more critical as each node lose some energy on each communication and thus needs effective reconfiguration of network that minimize energy loss. In the present work we propose an ant based approach to perform the dynamic reconfiguration of network as some broken link or the attack node found over the network. The complete work is divided in three main stages. In first stage, the communication is performed through the effective shortest path. The second stage, the identification of block node or the attack node over the network is performed and in third stage, the network reconfiguration is performed as the bad nodes are detected. This paper attempts to optimize the reconfiguration process using ant optimization approach. The results obtained are encouraging and shows that the presented work is effective in terms of accuracy as well as efficiency.**

Keywords: ***Sensor Network, Block Node, Ant Optimization, Reconfiguration, Energy Efficient***

I. INTRODUCTION

Sensor network is one of the most common ad hoc network that is being used in all areas such as personal area network, body area network, vehicular area network. A sensor network is generally a vast network defined with n sensors that are defined in a mesh architecture. Each node is defined with some energy specification. With each communication over the network each node loss some amount of energy. A node that loss all its energy get dead.

A clustered network is one of the common type of sensor network. Each cluster is defined with some Cluster Head (CH). Besides, the connectivity of every sensor to a CH has to be ensured at any time. Furthermore, for data to be routed from any CH to the PN (Processing Node), all CHs have to belong to a single connected graph. Hence, for sensors' states allocation to be optimal, coverage, connectivity of sensors to CHs, and routing has to be taken into account within the same global planning process.

Besides achieving energy efficiency, clustering reduces channel contention and packet collisions, resulting in better network throughput under high load.

Generally, energy conservation is dealt with on four different levels:

1. Efficient scheduling of sensor states to alternate between sleep and active modes;
2. Energy-efficient routing, clustering, and data aggregation;
3. Efficient control of transmission power to ensure an optimal trade-off between energy consumption and connectivity;
4. Data compression (source coding) to reduce the amount of uselessly transmitted data

A) Security Attacks in WSN

The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on ad hoc wireless networks can be classified as *passive* and *active* attacks, depending on whether the normal operation of the network is disrupted or not. [2].

Passive attacks:

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is

to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overheard.

Active attacks:
An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be *internal* or *external*. External attacks are carried [25] out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication. Both passive and active attacks can be made on any layer of the network protocol stack [1]. This section however, focuses on network layer attacks only (routing attacks). Depending upon the various attacking behavior routing attacks can be classified into five categories: attacks using information disclosure, impersonation (masquerading or spoofing), modification, fabrication, and replay of packets. Among these information disclosure is a passive attack while the rest fall under the active category.

B) Secure Routing

In unipath routing, only a single route is used between a source and destination node. Routing protocols are used to find and maintain routes between source and destination. Multiple paths can provide load balancing, fault-tolerance, and higher aggregate bandwidth. Load balancing can be achieved by spreading the traffic along multiple routes. This can alleviate congestion and bottlenecks. From a fault tolerance perspective, multipath routing can provide route resilience.

II EXISTING APPROACH

The major attack to the mechanism is the man in the middle attack. The attacks could be on the routing mechanism that is being followed for communication between the two nodes. A node can be compromised at any time in the network which can also be full nodes. A node can be compromised at any time in the network. Suppose that when the two nodes are communicating to each other they had to follow the route which is of shortest length to the destination and in the route lies the malicious node. The attack by a malicious node is possible in two ways:

1. The transfer of keys takes place when the communication is needed between two nodes .So while transferring of public keys to each other. The middle node can impersonate the nodes by transferring its own public key to the nodes and can disclose the contents of communication which are not meant for it.

2. Second possibility is that the malicious nodes in the middle can disrupt the whole communication. Firstly node has to initialize the communication by sending the initialization request to the receiver which can be interrupted by the malicious node .Secondly while the communication starts then the malicious node can drop packets and sender has no way to know whether the packets are received or not.

The basis parameters that are being analyzed to generate an effective path for secure routing is given as under.

(a) maximum path length(MaxLen)

MaxLen represents the maximum acceptable length of a path defined as the sum of edge weights wi in the path. The path length may represent various physical properties, such as distance, cost, delay, or failure probability. It can be represented by i an integer or a float value. If $wi = 1$ is true for all edges, then the path length is the hop number from a source to a destination.

(b) maximum number of hops on the path *(MaxHop)*

MaxHop represents the maximum acceptable number of hops on a path. If a path contains *k* nodes, then its hop number is *k-1*. *MaxHop* is an integer value.

(c) maximum number of shared edges *(MaxSE)*

Shared edges among three paths, also called common edges, include two types of edge sharing: double- and triple-shared edges, respectively. We use integer values *MaxSEdbl* and *MaxSEtri* to denote the related maximum acceptable number of double- and triple-shared edges. This constraint is essential in cases requiring high network reliability when multiple paths are used between two routers.

III ACO

ACO is basically the optimization approach that is basically used to speed up the algorithmic process. In wireless network the ACO is basically used to optimize the communication process. According to this approach a node generate the ant to find the optimized path over the network. These ants place the pheromones on this located path so that all other nodes can follow these pheromones to communicate on this optimized path. The foremost step of ant communication is the identification of pheromone location and to place them at appropriate location. More time it takes for an ant to travel down the path and back

again, the more time the pheromones have to evaporate. A short path gets marched over faster, and thus the pheromone density remains high as it is laid on the path as fast as it can evaporate. The distinctive behavior of ants has been extensively studied and has inspired a number of methods and techniques among which the most successful is the general purpose optimization technique known as Ant Colony Optimization (ACO). ACO exploits a similar mechanism similar to that of the foraging behavior of some ant species. From the early nineties, when the first ant colony optimization algorithm was first proposed, ACO attracted the attention of increasing numbers of researchers and many successful applications are now available. Moreover, a substantial corpus of theoretical results is becoming available that provides useful guidelines to researchers and practitioners in further applications of ACO [ZHOUCHEN LIN]

AntHocNet is a hybrid multi-path algorithm, which uses the concept of ant based routing. They are based on the pheromone trial laying-following behavior of real ants and the related framework of ant colony optimization. Continuously sampling possible paths with ant-like agents and the quality of the path is indicated by the artificial pheromone variables. Ant based routing algorithms can work in a distributed, are highly adaptive, robust and provide automatic load balancing.

When a data session is started at node S with destination D, S checks whether it has up-to-date routing information for D. If not, it reactively sends out ant-like agents, called reactive forward ants, to look for paths to D. These ants gather information about the quality of the path they followed, and at their arrival on D they become backward ants which trace back the path and update routing tables. On the backward path the pheromone tables in different nodes are updates thus indicating multiple paths between S and D, and data packets can be routed from node to node as datagrams. They are stochastically spread over the paths: in each node they select the next hop with a probability proportional to its pheromone value. Once paths are set up and the data session is running, S starts to send proactive forward ants to D. These ants follow the pheromone values similarly to data packets. In this way they can monitor the quality of the paths in use. Moreover, they have a small probability of being broadcasted, so that they can also explore new paths. In case of link failures, nodes either try to locally repair paths, or send a warning to their neighbors such that these can update their routing tables. AntHocNet uses a heuristic method like Ant Colony Optimization (ACO) as compared to the other hybrid routing protocols mentioned in the literature [5].

IV METHODOLOGY

In this proposed work we have defined the network with a new intelligent protocol to perform the end to end communication over the sensor network with effect of Ant Optimization. Here each node is defined with some energy parameters. Each communication over the network give some energy is lost for the node. The basic communication is done by using path selection algorithm. But if some broken link found or the dead node found over the path. An ant optimized network reconfiguration is implemented to identify the new path over the network. The present work will give the effective solution of bad node problem over the network. The present work is effective in case of

1. Some broken link found over the network
2. When a node get dead because of heavy energy loss.
3. There is man in middle attack over the network.

The proposed algorithm of network reconfiguration is given as

1. At regular interval any node s (Source) is selected to send data to some destination node d.
2. Each forward ant selects the next hop node using the routing table information. The next node selected depends on some random scheme. If all nodes already visited a uniform selection will be performed.
3. If the selected node is some attack or damage node or it is not currently available. The forward ant waits to turn in the low priority node from the queue.
4. And it will identify any of the next non visited node and pay some delay on it.
5. If some cycle detected the ant is forced to turn on the visited node.
6. When the ant reaches the destination node a backward ant is generated to transfer all its memory.
7. Backward ant uses same path generated by forward ant.

The present work will give the benefit in terms of an optimized communication over the network. An optimized secure path will be generated to perform the reliable communication. The work is optimization based means it will give an efficient path. As the energy is main consideration, it will improve the network path. The work is dynamic it will not disturb the whole communication over the network.

V RESULTS

The proposed work is about to introduce an Ant based compromising path to transfer data from some safe route if there are some chances of occurring of any intrusion or the congestion in the route of the basic routing algorithm. The work is implemented in Matlab 7.8.

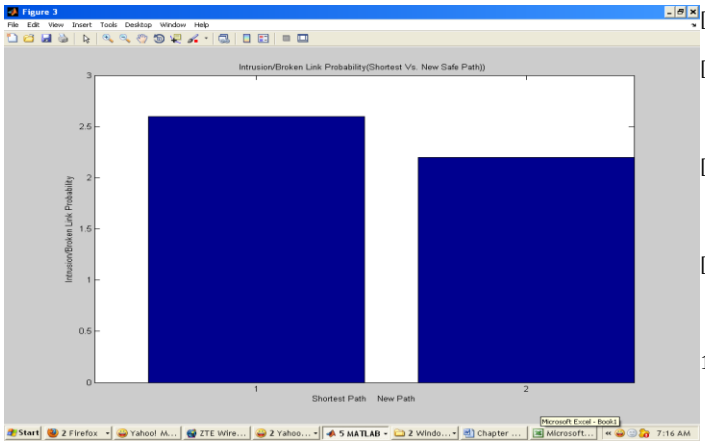

Figure 1 : Optimized Path Cost

Here figure 1 shows the results obtained from this reconfiguration network. The obtained results show that the presented effective path is much efficient the static reconfiguration of the network.

VI CONCLUSION

We are providing the solution for the problems where we can save the ad hoc network from the active attack of Intruders that are on the basis of algorithmic implementations. Generally the path selected for data transfer in ad hoc network is the shortest path because of this intruder attack is also in same area. We have defined an Ant Optimized path in which no node from the shortest path will be included.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci , "A Survey on Sensor Networks", in Proc. of the IEEE Communications Magazine, vol.40, Issue: 8, pp. 102-114, August 2002.

[2] Qiangfeng Jiang and D. Manivannan, "Routing Protocols for Sensor Networks", in Proc. of the IEEE Conference, 2004, pp. 93-98.

[3] Nam N. Pham, Jon Youn and Chulho Won, "A Comparison of Wirless Sensor Network Routing Protocols on an Experimental Testbed", in Proc. Of the IEEE International Conference on Sensor Networks, 2006, pp.35-42.

[4] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, Tech. Rep. F33615-01-C-1895.

[5] A.Perrig, R.Szewczyk, V.Wen and J.D. Tygar, "SPINS: Security Protocols for sensor networks", International Conference on Mobile Computing and Networking (Mobicom 2001), 2001, pp.189-199.

[6] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer 35 (10), 2002, pp. 54-62.

[7] Lewis, F.L., "Wireless Sensor Networks Smart Environments: Technologies, Protocols, and Applications", New York: ed. D.J. Cook and S.K. Das, John Wiley, 2004, pp.1-18.

[8] J. Deng, R. Han and S. Mishra, "INSENS: Intrusion-Tolerant Routing in WSN", in Proc. Of the Second International Workshop on Information Processing in Sensor Networks (IPSN 03), April 2003, pp. 349-364.

[9] Dijkstra E. A note on two problems in connection with graphs. Numerical Mathematics 1959;1:269-271.

[10] T. Korkmaz, M. Krunz, and S. Tragoudas, "An efficient algorithm for finding a path subject to two additive constraints", in Proceedings of the ACM SIGMETRICS '00 Conference, June 2000, vol. 1, pp. 318–327.

[11] Thierry Rakotoarivelo , Patrick Senac , Aruna Seneviratne and Michel Diaz , "Enhancing QoS through Alternate Path: An End-to-End Framework", in Proc. of the IEEE INFOCOM, Conference on Computer Communications, pp. 14-22, 2000.

[12] Dr. Sami S. ,Al-Wakeel and Eng. Saad A. AL-Swailem , "PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks", in Proc. of the IEEE Communications Society, pp. 4159-4163, 2007.

13] Wei Wang, Sylvani Gombault, " Efficient Detection of DDoS Attack with Important Attributes", 3rd International Conference on Risks and Security of Internet and System :CRiSIS'2008, IEEE, 2008.

[14] Yinan Jing, Xueping Wang, Xiaochun Xiao, Gendu Zhang, "A Logless Fast IP Traceback Scheme Against DDos Attacks in wireless Ad-hoc Network.