An Algorithm for a Secure Path in Mobile Ad Hoc Network

Gaurav[1] Mr Mohd Sadim[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1]Al-falah School of Engineering & Technology, Faridabad, Haryana, INDIA

Abstract— Mobile Ad hoc Networks (MANETs) consists of a group of wireless mobile nodes which exchange data dynamically among themselves without based on a fixed base station or a wired backbone network. The ad-hoc network provide lack of secure boundaries. The ad-hoc network may also provide some intrusion.Ad hoc is used to describe solutions that are developed on-the-fly for a specific purpose. Computing nodes (usually wireless) in an ad hoc network act as routers to deliver messages between nodes that are within their wireless communication range. Intrusion is one of the common problems in all networks in case of ad hoc network we face the same problem. When we have a dense sensor network with number of nodes and there is some important data is transferred over the network, there is the requirement of security. But in case of "Man in Middle" it is never easy to say a network is intruder safe. Even when the Intruder knows about the routing algorithms or the algorithm implementation it is quite difficult to handle the problem. We are providing the approach to transfer data from some path other than that common path.

Key words: MANET, WSN, civilian areas, servo mechanisms.

I. INTRODUCTION

In the field of wireless networking there is another form of networking which is called as wireless sensor network. A type of wireless network which is comprised of number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors. This type of networking is called as Wireless Sensor Networking. Basically Wireless Sensor Networking is used for monitoring the physical conditions such as weather conditions, regularity of temperature, different kinds of vibrations and also deals in the field of technology related to sound.

The development of WSN was motivated by military applications such as battlefield surveillance and are now used in many industrial and civilian areas, including industrial process monitoring and control, machine health monitoring, healthcare applications, home automation, and traffic control. In surveillance applications, sensors are deployed in a certain field to detect and report events like presence, movement or intrusion in the monitored area. In the present area there are a lot of technologies which are used for monitoring and are completely based on the Wireless Sensor Networking. Wireless Sensor Networks can also be used for detecting the presence of vehicles such as motor cycles up to trains. A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from a battery [1].

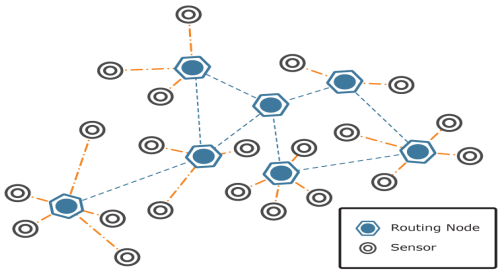

Fig. 1: Sensor network

A. Working of WSN:

Total working of Wireless Sensor Network is based on its construction. A Sensor Network initially consists of small or large nodes called as sensor nodes. These nodes are varying in size and totally depend on the size because different sizes of sensor nodes work efficiently in different fields. Wireless Sensor Network have such sensor nodes which are specially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery. The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors, a communication device (usually radio transceivers), and a power source usually in the form of a battery.
Current system solutions, protocol frameworks and paradigms typically provide the following services:

(1) Periodic Sensing (the sensor devices constantly monitor the physical environment and continuously report their sensor's measurements to a control center).
(2) Event Driven(to reduce energy consumption, sensor devices monitor silently the environment and communicate to report when certain events are realized) .
(3) Query based (sensor devices respond to queries made by a supervising control center).

Recently, new applications have been proposed, that require different approaches for disseminating sensor data to the control center, such as target tracking(where sensors exchange sensor readings in order to detect the movement pattern of a detected target) or Area surveillance(where sensors are equipped with video

capturing devices). Certainly, more services will become feasible in the near future that will allow different kinds of interaction with the surrounding environment (e.g. via actuators and servo mechanisms). It should not be surprising that the unique characteristics of this regime give rise to very different design trade-offs than current general-purpose systems. The missing elements are simple but efficient optimization strategies at the protocol level, overall system architecture and a methodology for systematic advance. Indeed, the realization of such efficient, robust and secure ad-hoc networking environments is a challenging task. Large number of such tiny and resource-constrained devices should be self-organized into an ad-hoc network under highly dynamic ambient conditions, carrying out computations locally and engaging into a collaborative computing and communication effort. The required solutions differ significantly, not only with respect to classic distributed computing but also with respect to ad-hoc networking. To further emphasize on the difference consider that

(1) The number of interacting devices in a sensor network are extremely large as compared to that in a typical ad-hoc network.
(2) Sensor networks are typically prone to faults (as a result of the low cost equipment).

The limitations in energy, computational power and memory are much more severe in sensor networks.

II. LITERATURE SURVEY

Rajaravivarma, Yi Yang, and Teng Yang[2] provided detailed information about networking and applications of the Wireless Sensor Networks. They represent a new generation of real-time embedded systems with significantly different communication constraints.

Xiang-zhong Meng, Bing Wu [4] explained the problem of determining the node locations through a wireless sensor special algorithm. Only knowing the right location of network and brings forward a new locating algorithms of nodes. we can determine the exact location of fake nodes . In WSN, right location of WSN node is the basic to information in advance, then we realize the position of node by clock-locating algorithm.

Akramul Azim and Mohammad Mahfuzul [13] provided a new robust relay node based hybrid Low Energy Adaptive Clustering Hierarchy (LEACH) which incorporates the recently developed energy comparison. LEACH is a node relay based technique that helps to make the network still operates, in the presence of nodes having low energy to communicate. The proposed scheme also maintains the efficiency of energy utilization through controlling the size of cluster in a distributed manner for the first time.

Stefan Funke[6] provided the hole detection algorithm and also gave procedure to identify nodes near the boundary of the sensor field as well as near hole boundaries. ZHAN YING[9] performed research on physical storage mechanism that is proper for the migration of Data Flow in Storage Node in order to associate physical storage resources with logical data resources. By establishing autonomous storage management model to meet demand of continuing availability and data integrity, we put forward to an autonomous algorithm which can support sustainable and intelligent management for data flow. Storage Management Control optimization is an effective method that will reduce the working time to large scale data storage management.

Hang Qin and Zhongbo Wu [12].This paper investigates the load balancing in sensor nodes and wireless link based on the performance of wireless sensor networks. With an optimized model, the dynamic scheme of data collection and forwarding scheduling between grid-quorum is derived to evaluate the benefits of load balancing in order to access the profitability. The load balancing method in this paper outperforms load in the terms of balancing factor, different nodes number and data scales of various applications.

III. SECURE ROUTING PATH

One of such an algorithm is generally followed by a user over the network is the shortest path problem, When intruder want to hack some information by acting man in middle, it is not easy for him to trace all the nodes over the network because the sensor network contains large number of nodes.

A. Existing System:

In such case instead of tracking each node intruder will follow a route or the pattern to perform the attack. One of such method is to trace the shortest path. Generally each routing algorithm follow the concept of shortest path to transfer the data over the network with minimum time requirement. In other words we can say the shortest path route nodes are the most unsafe nodes for transferring data as they are generally targeted by an intruder.

Fig. 2: Distance from one node to another

The general possibility of error is man in middle attack. The attack can be performed by the intermediate node i.e. malicious node and have the unwilling effects on the ongoing process. In order to make secure transmission the complete network must be analyzed for the security breach so that secure transmission can take place with in the network. The solution to the attack is given by finding an alternative route to the destination node and by getting the proper acknowledgement from the destination node.

Due to insecure nature of the wireless links and the dynamically changing topology, wireless ad-hoc networks require a careful and security oriented approach for designing the protocols.

B. Proposed System:

Alternate paths may significantly improve security and reliability of source routing. We develop a fast alternate path-finding algorithm for authentication purpose. This algorithm is based on the Dijkstra's shortest path algorithm. Three partially disjoint paths can be calculated in time complexity O (N*logN*logW0), where N and W0 represent the number of nodes and the sum of the weights of all edges in a graph, respectively. We use simulation tests to compare

the performance of our algorithm and the shortest paths algorithm that uses the deviation approach. Based on the results of simulation, our algorithm is proved to be an efficient alternate path-finding method with several advantages such as simpler implementation, faster execution time, better stability and fewer shared edges in a selected path set.

Due to dynamic topology any node can join or leave the network at any time. This is the point of security breach as the joining node can be a malicious node and can have unwilling effects on the network performance. So it is very important to authenticate the joining nodes from the establishment of the network. Cluster based architecture is used because it is easily manageable and more secure than other architectures. In cluster based architectures gateways are used for inter cluster communication.

The network establishment takes place from the starting i.e. there is initially no nodes in the network. The authentication of the joining new nodes is done by using hash functions. As the network grows the architecture enables the network to be divided into number of clusters and each cluster having a cluster head. The cluster head has the responsibility for managing the whole cluster. After the different nodes being divided into number of clusters, there is secure communication mechanism for inter and intra cluster communication. Finally the we will address the attack possibility in the network .

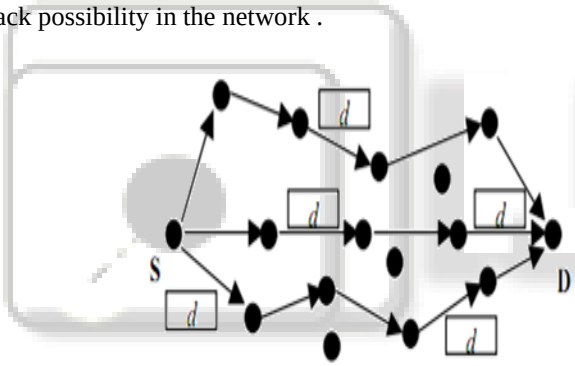

Fig. 3: Nodes in a WSN

The possible attack in such a network is man in middle attack.The possible solution for such types of attacks is to find an alternative route to destination. The technique uses the method to find the alternative route which is not the shortest and which doesn't involve any node that resides in the shortest path. We simulate the proposed solution using our own simulator known as Network Simulator(NS-2).

C. Research Methodology:

In this section, we present our mechanism(Secure Data Transmission using alternate Path in Ad hoc Network). At every round the network establishes a new routing topology by setting up new alternate routing paths. When we find the alternate path, we have to fulfill the following constraints:

1) 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 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.

2) Maximum number of hops (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.

3) (c) Maximum Shared Edges (MaxSE):

Shared edges among the paths, also called common edges, include two types of edge sharing: double-shared edges and triple-shared edges. 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.

D. Secure alternate path algorithm Description:

(1) Establish a network for any number of nodes.
(2) Generate an N x N matrix and initialize all the elements of matrix with 0.
(3) Calculate the distance from one node to all other nodes and store in an N x N matrix.
(4) Give the range of the network node and set all other elements that are outside the range to 0.
(5) Encrypt the Message with Public Key of Destination Node
(6) Message=Public_Key(Message,Di)
Here Di represents the Destination Node

i. for (i = 0 ; i <n ; i++)

```
{
for (j = 0 ; j < n ; j++)
{
        if j is neighbour of i
        neighbour_array[i][j] =1;
        }
}
```

(7) Selection of shortest path from source to destination
(8) Initialize the source node and put it in another array. Name the array as array [ ].
(9) Search the neighbour list and pick a random node from the list and put that node in the array. Compare the random node with all the elements of the shortest path array.
(10) If the array [top] element matches with any of the elements in the list then put array [top] = 0 and top = top-1.Make the entry corresponding to that node in neighbour array as 0 and Go to step 5.
(11) Compare the neighbour list of the generated node with all the elements of array.If all the neighbour matches then put array [top] =0 and top = top-1 also make the entry of that node in neighbour array as 0 and Go to step 5 else Pick a random node from the list and put it in the array.
(12) If array [top] = destination then *Message=PrivateKey(Message,Di)*

Decrypt the message using Private Key of receiver side and terminate the process with success message. return route and exit else Go to step 6.

Finally we get the list of nodes that provide a safe path in case of uni-cast , this pass is very closer to the shortest path but doest not include any node from the shortest path list because of this it provide the secure

transmission on the algorithm implementation attack of the Intruder.

IV. RESULT

In simulation, we can construct a mathematical model to reproduce the characteristics of a phenomenon, system, or process often using a computer in order to information or solve problems. Nowadays, there are many network simulators that can simulate the network. In this section we will introduce the most commonly used simulators. We will compare their advantages and disadvantages and choose one platform to implement reactive/proactive protocol and conduct simulations.

A. Network Simulator – NS-2:

NS-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (NS) contains all commonly used IP protocols. The Network Animator (NAM) is use to visualize the simulations. NS-2 fully simulates a layered network from the physical radio transmission channel to high-level applications. We have with defined scenarios to test the above work.

Parameter	Value
Number of Nodes	50
Topography Dimension	800 m x 800 m
Traffic Type	TCP
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Routing Protocol	DSR
Antenna Type	Omni directional

Table 1: Simulation Parameters

B. Simulation Scenario of 50 mobile nodes with congestion:

The mobile ad hoc network comprising of 50 mobile nodes is constructed in the NS-2 simulator with the use of ETCL script in the topological boundary area of 800 m x 800 m. The position of the mobile nodes is defined in terms of X and Y coordinates values. The given scenario shows the packet transmission with shortest path between the nodes starting from the source node 0 to the destination node 49. The red coloured nodes indicated the misbehave nodes or some intrusion nodes.

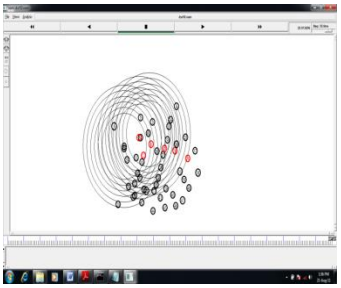

Fig. 4: Screenshot of 50 mobile nodes implementing packet transmissions with Shortest Path in DSR

C. Simulation Scenario of 50 mobile nodes Alternate path:

The mobile ad hoc network comprising of 50 mobile nodes is constructed in the NS-2 simulator with the use of ETCL script in the topological boundary area of 800 m x 800 m. The position of the mobile nodes is defined in terms of X and Y coordinates values. The given scenario shows the packet transmission without congestion between the nodes starting from the source node 0 to the destination node 49. The red coloured node indicated the packet loss and marked this node as misbehaving node. In this scenario, it will perform the delay analysis by comparing the throughput with the Expected output. If there is some weaker node that performed delayed data transmission, we need to identify that node, and eliminate the delayed node and perform the cache refresh ness dynamically. Now the data will be transferred from some compromising node.

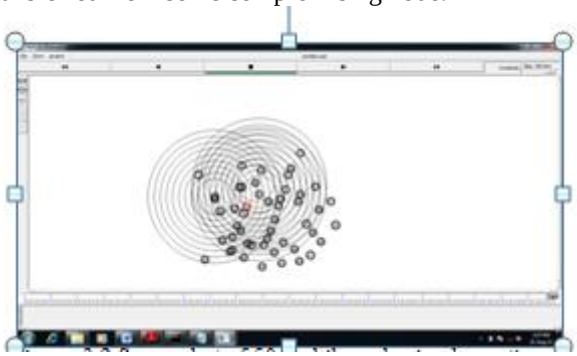

Fig. 5: Screenshot of 50 mobile nodes implementing packet transmission in case of alternate path

The trace file output is then converted into X Graph to show the results in graphical format

Fig. 6: X Graph of 20 seconds of actual simulation time for DSR

The Figure 3.3 shows the X graph of data transmission when the simulation is carried only for 20 seconds, the packet received and packet loss is initially zero at the time of start because initially there is no TCP connection. This graph represents the outputs without setting the expected simulation time.

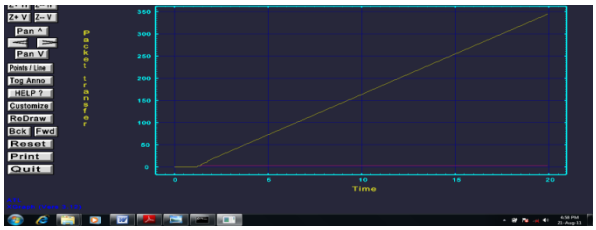

Fig. 7: X Graph of 20 seconds of expected simulation time for DSR

The Figure 3.4 shows the X graph of DSR when the simulation is carried only for 20 seconds, the packet received and packet loss is initially zero at the time of start because initially there is no TCP connection. This graph representing the outputs by setting the expected simulation time.

V. CONCLUSION

Importance of WSN cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, WSN pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities.

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 generated such a path in which no node from the shortest path will be included. It will give an secure and efficient approach of data transmission in ad-hoc network in uni cast.

REFERENCES

[1] Proceedings of IEEE GLOBECOM '01, 2001-11.K Whitehose, D Culler. Calibration as Parameter Estimation in Sensor Networks [C]. In: First ACM International Workshop on Wireless Sensor Networks and Application, Atlanta GA, 2002-09.
[2] An Overview of Wireless Sensor Network and Application V. Rajaravivarma, Yi Yang, and Tang Yang Computer Electronics, School of Technology 0-7803-7697-8/03/$17.000 2 008 IEEE
[3] Ye W, Heidemann J, Estrin D, applications of wireless sensor networks. In: Proc 21St Int'l Annual Joint Conf IEEE Computer and Communications Societies (INFCOM 2002), New York, NY, June 2002.
[4] Low Power Locating Algorithms For Wireless Sensors Network , Xiang-zhong Meng, Bing Wu, Hui Zhu and Yao-bin Yue Xiang-zhong Meng Proceedings of the 2006 IEEE
[5] Node Sensing & Dynamic Discovering Routes for Wireless Networks Arabinda Nanda, Amiya Kumar Rath and Saroj Kumar (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010
[6] Topological Hole Detection in Wireless Sensor Networks and its Application Stefan Funke Computer Science Department Gates Bldg. 375Stanford University, CA 94305, U.S.A.
[7] Energy Aware Routing for Low Energy Ad Hoc Sensor Networks Rahul C. Shah and Jan M. Rabaey
[8] Route Aware Predictive Congestion Control Protocol for Wireless Sensor Networks Carl Larsen, Maciej Zawodniok, Member, IEEE, and Sarangapani Jagannathan, Senior Member, IEEE Singapore, 1-3 October 2007
[9] Research on Management of Data Flow in the Cloud Storage Node Based on Data Block ZHAN Ying 978-0-7695-4047-4/10 $26.00 © 2010 IEEE DOI 10.1109/ICIC.2010.355
[10] A Survey on Sensor Networks Ian F. Akyildiz,Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci Georgia Institute of Technology 0163-6804/02/$17.00 © 2002 IEEE
[11] Alternate Path Routing for Multicast Daniel Zappala IEEE INFOCOM, CONFERENCE ON COMPUTER COMMUNICATIONS, MARCH 2000
[12] Analysis and Improvement of the Dynamic Load Balancing of Overlay-based WSN Hang Qin1,2,Zhongbo Wu1,2 978-1-4244-2358-3/08/$20.00 © 2008 IEEE
[13] Hybrid LEACH: A Relay Node Based Low Energy Adaptive Clustering Hierarchy for Wireless Sensor Networks Akramul Azim1 and Mohammad Mahfuzul Islam2 Proceedings of the 2009 IEEE 9th Malaysia International Conference
[14] Dynamic Route Diversion in connectionless Mobile Ad Hoc Networks Yao H. Ho1, Kien A. Hua1, Ning Jiang2, and Fei Xie1 978-0-7695-3187-8/08 $25.00 © 2008 IEEE

