Algorithm Application for A Secure Path in A Mobile AD HOC Network

Sone Lal Patel[1] Sumiran Daiya[2]
[1]Research Scholar [2]Assistant Professor
[1,2]Department of Electronics & Communication Engineering
[1,2]Sat Kabir Institute of Technology & Management, Bahadurgarh, Haryana, India

Abstract — Mobile Adhoc Networks (MANETs) are made up of a collection of wireless mobile nodes that communicate with one another on a dynamic basis without the need for a wired backbone network or a stationary base station. Ad hoc networks don't offer safe boundaries. Additionally, the ad-hoc network might offer some incursion. Solutions created on the spot for a particular goal are referred to as ad hoc. In an ad hoc network, computing nodes—which are typically wireless—serve as routers, sending messages between nodes within their wireless communication range. One of the typical issues with all networks is intrusion; in the case of an ad hoc network, we encounter the same issue. Security is necessary when there are many nodes in a dense sensor network and some critical data is being transmitted over the network. However, it is never simple to declare a network to be intruder secure when there is a "Man in the Middle." It is challenging to solve the issue, even if the hacker is aware of the routing methods or how they are implemented. We offer a method for moving data from a different way than the typical one.

Keywords: Mobile Ad Hoc Networks (MANETs), Wireless Communication, Intrusion Detection, Ad Hoc Routing, Man-in-the-Middle Attack, Network Security, Dynamic Topology, Sensor Networks, Data Transmission Security, Alternative Routing Methods

I. INTRODUCTION

Wireless sensor networks are another type of networking that falls under the umbrella of wireless networking. This kind of wireless network is made up of many different sensors that are connected to one another and work together to accomplish a common task in order to verify and balance environmental conditions. Wireless Sensor Networking is the name given to this kind of networking. Wireless sensor networking is mostly used to monitor physical factors, including weather, temperature, vibrations, and other types of vibrations. It also deals with sound-related technology.

Military uses like battlefield surveillance spurred the development of WSN, which are currently employed in a wide range of commercial and residential domains, such as traffic management, home automation, healthcare applications, machine health monitoring, and industrial process monitoring and control. Sensors are placed in specific fields for surveillance applications in order to identify and report events such as presence, movement, or trespass in the monitored area. Many of the methods utilized for monitoring in the current field are entirely dependent on wireless sensor networking. Additionally, wireless sensor networks can be utilized to detect the presence of motorbikes, trains, and other vehicles. A sensor network is made up of several small, portable detecting units known as sensor nodes.

Each sensor node has a power source, transceiver, microcontroller, and transducer. Electrical signals are produced by the transducer in response to perceived physical occurrences and effects. The sensor output is processed and stored by the microprocessor. The transceiver, which can be wireless or hard-wired, sends data to a central computer after receiving commands from it. Each sensor node is powered by either a battery or the electric utility.[1].

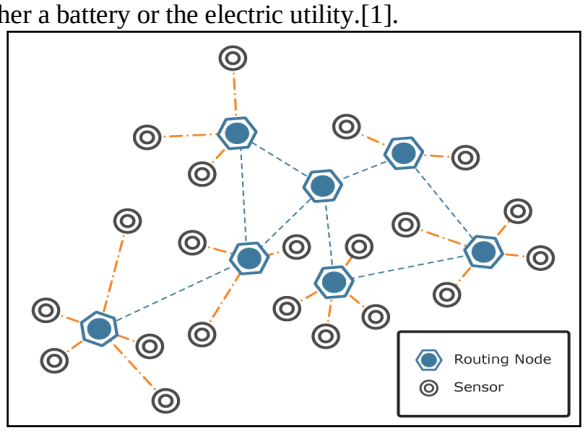

Fig. 1.1: Sensor network

A. *Working of WSN*

The foundation of a wireless sensor network's overall operation is its design. Initially, a sensor network is made up of sensor nodes, which might be tiny or huge. Since different sensor node sizes function well in various fields, these nodes vary greatly in size and are entirely dependent on it. Sensor nodes in wireless sensor networks are specifically made in such a way that they have a radio transceiver to generate radio waves, a microcontroller to control the monitoring, various wireless communication devices, and an energy source like a battery.

Using various sensor sizes, the complete network operated concurrently, experimenting with the multirouting algorithm phenomena, also known as wireless ad hoc networking.

Sensor nodes can be thought of as little computers with very simple components and interfaces. They typically include sensors, a communication device (often radio transceivers), a processing unit with limited memory and computational capability, and a power supply, typically a battery.

The following services are generally offered by current system solutions, protocol frameworks, and paradigms:

1) Periodic Sensing: The sensor devices continuously communicate their measurements to a control center while also monitoring the physical environment.
2) Event Driven (sensor devices passively monitor the surroundings and communicate to report when specific occurrences are realized) (to reduce energy use).
3) Query-based (a supervising control center asks questions, and sensing devices reply).

Target tracking (where sensors exchange sensor readings to detect the movement pattern of a detected target) and area surveillance (where sensors are equipped with video capturing devices) are two recent applications that call for

different methods for sending sensor data to the control center. In the near future, other services that enable various forms of contact with the environment (e.g. via actuators and servo mechanisms) will undoubtedly become possible.

It should come as no surprise that the distinct features of this regime result in design trade-offs that are significantly different from those of general-purpose systems today. Simple yet effective protocol-level optimization techniques, a comprehensive system architecture, and a methodical advancement methodology are the missing components. It is difficult to create ad-hoc networking infrastructures that are this effective, reliable, and secure. Under extremely dynamic environmental conditions, a large number of these small and resource-constrained devices should self-organize into an ad hoc network, performing calculations locally and participating in cooperative computing and communication efforts. There are substantial differences in the necessary solutions between ad-hoc networking and traditional distributed computing.

To further highlight the distinction, take into account the following:

1) A sensor network has a far higher number of interacting devices than a conventional ad-hoc network.
2) Due to the inexpensive equipment, sensor networks are usually prone to malfunctions.

Sensor networks face far more severe energy, computational, and memory constraints.

II. LITERATURE SURVEY

Rajaravivarma, Yi Yang, and Teng Yang [2] provide comprehensive details on networking and Wireless Sensor Network applications. With radically differing communication restrictions, they constitute a new generation of real-time embedded systems.

The difficulty of identifying the node positions using a unique algorithm for wireless sensors was described by Xiang-zhong Meng and Bing Wu [4]. Just being aware of the network's correct location introduces new node locating techniques. We are able to pinpoint the precise position of phony nodes. The correct location of a WSN node is the foundation for knowledge beforehand, and the clock-locating algorithm is used to determine the node's position.

A new, reliable hybrid Low Energy Adaptive Clustering Hierarchy (LEACH) based on relay nodes was presented by Akramul Azim and Muhammad Mahfuzul [13]. It integrates the recently created energy comparison. A node relay-based approach called LEACH helps the network continue to function even when there are nodes with insufficient energy to communicate. By regulating the cluster size in a distributed fashion for the first time, the suggested plan also preserves energy efficiency.

The hole detection algorithm and a method for locating nodes close to the sensor field's edge and hole borders were both supplied by Stefan Funke [6].

In order to link physical storage resources with logical data resources, ZHAN YING[9] conducted research on physical storage mechanisms that are appropriate for the movement of Data Flow in Storage Nodes. We propose an autonomous algorithm that can assist intelligent and sustainable data flow management by building an autonomous storage management model to satisfy the demands of data integrity and continuous availability. Optimizing Storage Management Control is a useful technique for cutting down on the amount of time needed to handle large-scale data storage.

Zhongbo Wu and Hang Qin [12]. Based on the effectiveness of wireless sensor networks, this study examines load balancing in sensor nodes and wireless links. To assess the advantages of load balancing and determine profitability, a dynamic data gathering and forwarding scheduling scheme between grid-quorum is constructed using an optimal model. In this work, the load balancing approach performs better than the load in terms of the balancing factor, the number of nodes, and the data scales of different applications.

III. SECURE ROUTING PATH

The shortest path problem is one such algorithm that users typically utilize over networks. Because sensor networks have a lot of nodes, it is difficult for an intruder to track down every node in the network when he wants to steal information by posing as a man in the middle.

A. Existing System

In this scenario, the attacker will follow a path or pattern to carry out the attack rather than monitoring every node. Tracing the shortest path is one such technique. The shortest path principle is typically used by all routing algorithms to move data across networks in the smallest amount of time. To put it another way, since shortest path route nodes are frequently targeted by hackers, we can conclude that they are the most dangerous nodes for data transfer.

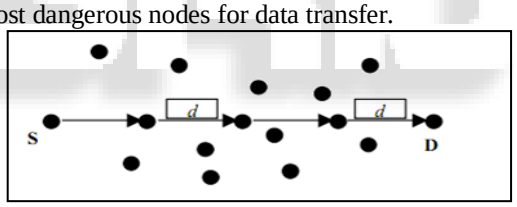

Fig. 1.2: Distance from one node to another

The most common mistake is a man-in-the-middle attack. The malicious node, or intermediate node, can carry out the attack and unintentionally impact the running process. Secure transmission can only occur within the network after the entire network has been examined for security flaws. The assault can be stopped by figuring out another way to get to the destination node and by receiving the appropriate acknowledgement from it. The continually changing topology and unsecured nature of wireless communications necessitate a cautious and security-focused approach to protocol design in wireless ad-hoc networks.

B. Proposed System

Alternative routes have the potential to greatly increase source routing's security and dependability. For the purpose of authentication, we create a quick alternative path-finding method. The Dijkstra's shortest path algorithm serves as the foundation for this approach. In time complexity O (N*logN*logW0), where N and W0 are the number of nodes and the total weights of all edges in a graph, respectively, three partially disjoint pathways can be computed.

We compare our method's performance with that of the shortest routes algorithm that employs the deviation technique using simulated testing. Simulation results demonstrate that our approach is an effective alternative path-finding technique with a number of benefits, including easier implementation, quicker execution time, improved stability, and less shared edges in a chosen path set.

Any node can join or exit the network at any time because of the dynamic topology. Since the joining node may be malevolent and have unintended consequences for the network's performance, this is the point of security breach. Therefore, it is crucial to authenticate the joining nodes at the network's creation. Because it is easier to manage and more secure than other systems, cluster-based architecture is adopted. Gateways are used for inter-cluster communication in cluster-based designs.

The dynamic topology allows any node to join or leave the network at any moment. This is the point of security breach since the connecting node could be malicious and have unforeseen effects on the network's functionality. Authenticating the joining nodes during the network's formation is therefore essential. Cluster-based architecture is used because it is more secure and easier to maintain than other systems. In cluster-based systems, gateways provide communication between clusters.

Finally, the we will address the attack possibility in the network.

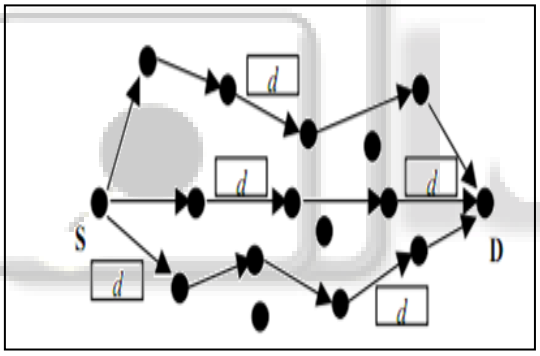

Fig. 1.3: Nodes in a WSN

Man-in-the-middle attacks are a potential threat in such a network.Finding a different path to the target is one potential defense against these kinds of attacks. The approach is used to determine a different route that is not the shortest and does not pass via any nodes that are part of the shortest path. We use Network Simulator (NS-2), our proprietary simulator, to model the suggested solution.

C. Research Methodology

Our method (Secure Data Transmission utilizing Alternate Path in Adhoc Network) is presented in this part. The network creates new alternate routing paths at each cycle to create a new routing topology. The following requirements must be met while determining the alternate route:

1) Maximum Path Length (MaxLen)

The maximum allowable length of a path is represented by MaxLen, which is the total of the path's edge weights. A number of physical attributes, including distance, cost, delay, and failure probability, can be represented by the path length. Either a float or an integer can be used to represent it. The number of hops from a source to a destination equals the path length if wi = 1 is true for every edge.

2) Maximum number of hops (MaxHop)

The maximum allowable number of hops on a path is denoted by MaxHop. A path's hop number is k-1 if it has k nodes. MaxHop is a whole number.

3) Maximum Shared Edges (MaxSE)

There are two kinds of edge sharing among the paths: double-shared edges and triple-shared edges. These are also referred to as common edges. The associated maximum allowable number of double- and triple-shared edges is indicated by the integer values MaxSEdbl and MaxSEtri. When two routers are connected via various paths and good network dependability is required, this restriction is crucial.

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
   Message=Public_Key(Message,Di)
   Here Di represents the Destination Node
6) 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.
10) Compare the random node with all the elements of the shortest path array.
    If the array [top] element matches with any of the elements in the list thenput 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)
    Use the recipient's private key to decrypt the message, then end the operation with a success message. go back and leave, or proceed to step 6.

In the end, we obtain the list of nodes that offer a secure way in the case of uni-cast; this pass is quite near to the shortest path but excludes nodes from the list of shortest

paths, thus offering secure transmission against the intruder's algorithm implementation assault.

IV. RESULT

Through simulation, we can create a mathematical model that replicates the features of a system, process, or phenomenon. This is frequently done on a computer to gather data or find solutions to issues. These days, a lot of network simulators are available that can replicate networks. We will present the most widely used simulators in this part. We will weigh the benefits and drawbacks of each platform before selecting one to use for simulations and reactive/proactive protocol implementation.

Network Simulator – NS-2

A discrete event simulator designed for networking research is called NS-2. It has strong support for simulating multicast, TCP, and routing protocols across wired and wireless networks. There are two simulation tools in it. All of the widely used IP protocols are included in the network simulator (NS). The simulations are visualized using the Network Animator (NAM). From the actual radio transmission channel to high-level applications, NS-2 accurately models a layered network. To test the aforementioned work, we have predetermined scenarios.

Parameter	Value
Number of Nodes	50
Topography Dimension	800 mx 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 1.1: Simulation Parameters

A. Simulation Scenario of 50 mobile nodes with congestion

Using the ETCL script, a mobile ad hoc network with 50 mobile nodes is built in the NS-2 simulator within an 800 m × 800 m topological boundary area. The X and Y coordinate values are used to define the mobile nodes' position. Starting at source node 0 and ending at destination node 49, the scenario illustrates packet transfer using the shortest path between the nodes. Some incursion nodes or misbehaving nodes were indicated by the red-colored nodes.

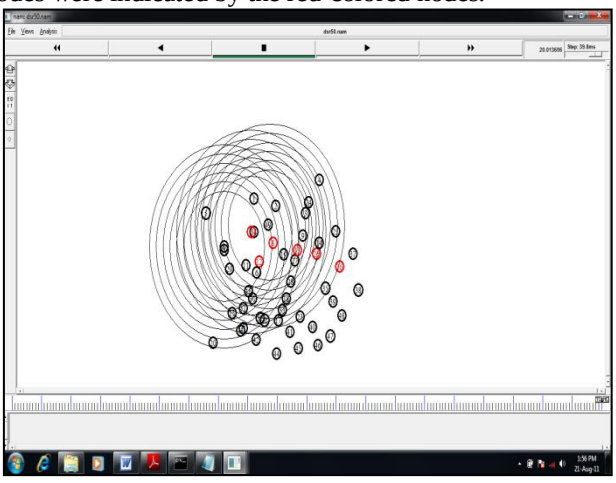

Fig. 3.1: Screenshot of 50 mobile nodes implementing packet transmissions with Shortest Path in DSR

B. Simulation Scenario of 50 mobile nodes Alternate path

Using the ETCL script, a mobile ad hoc network with 50 mobile nodes is built in the NS-2 simulator within an 800 m × 800 m topological boundary area. The X and Y coordinate values are used to define the mobile nodes' position. From source node 0 to destination node 49, the scenario illustrates packet transfer between the nodes without congestion. The packet loss was represented by the red-colored node, which was also tagged as a misbehaving node. In this case, it will compare the throughput with the expected output in order to perform the delay analysis.

If a weaker node is responsible for delayed data transfer, we must locate it, remove it, and dynamically refresh the cache. The data will now be sent from a compromised node.

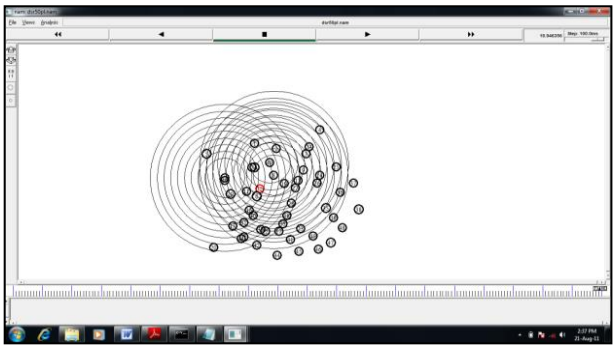

Fig. 3.2: Screenshot of 50 mobile nodes implementing packet transmission in case of alternate path

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

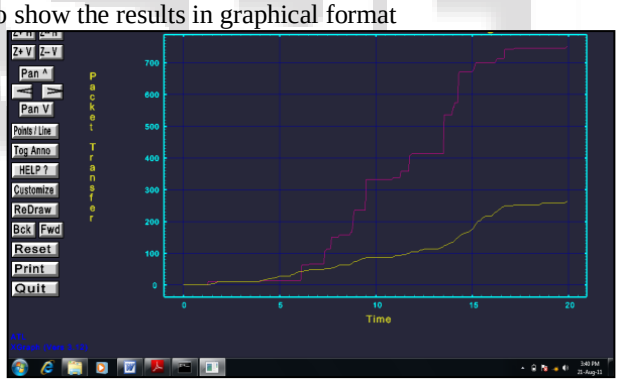

Fig. 3.3: X Graph of 20 seconds of actual simulation time for DSR

Figure 3.3 displays the data transmission X graph. Since there isn't a TCP connection at first, the packet loss and packet received are initially zero when the simulation is run for just 20 seconds. The outputs are shown in this graph without the anticipated simulation time set.

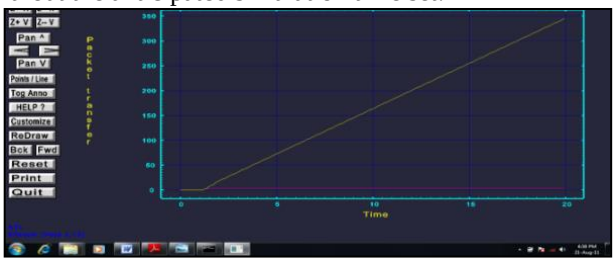

Fig. 3.4: X Graph of 20 seconds of expected simulation time for DSR

Figure 3.4 displays the DSR X graph. Since there isn't a TCP connection at first, the packet loss and packet

received are initially zero when the simulation is run for just 20 seconds. By establishing the anticipated simulation time, this graph displays the results.

V. CONCLUSION

WSN's significance is undeniable given how portable and small computers is becoming. Because of its unpredictable topology, wireless shared media, heterogeneous resources, strict resource constraints, etc., WSNs provide a variety of security solution problems in contrast to wired networks. Since many of the offered solutions were created with a small scenario size and a limited range of threats and vulnerabilities in mind, the field of security research is still open.

We are offering solutions for issues where we can protect the ad-hoc network from active intrusions by intruders using algorithmic implementations. Since this intruder attack occurs in the same location, the shortest path is typically used for data transfer in ad-hoc networks. We have created a path that excludes all nodes from the shortest path. It will provide a safe and effective way to send data in a Unicast ad hoc network.

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, 2024.
[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 2023.
[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 2022 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 2022
[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 2019
[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 © 2022 IEEE DOI 10.1109/ICIC.2010.355
[10] ASurvey on Sensor Networks Ian F. Akyildiz,Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci Georgia Institute of Technology 0163-6804/02/$17.00 © 2020 IEEE
[11] Alternate Path Routing for MulticastDanielZappala IEEE INFOCOM, CONFERENCE ON COMPUTER COMMUNICATIONS, MARCH 2022
[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 © 2018 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 2023 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 © 2020 IEEE

