Computer Systems Science & Engineering
DOI:10.32604/csse.2022.023609
Article

Tech Science Press

Gray-Hole Attack Minimization in IoMT with 5G Based D2D Networks

V. Balaji* **and P. Selvaraj**

Department of Computing Technologies, College of Engineering and Technology, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, 603203, Tamilnadu, India
*Corresponding Author: V. Balaji. Email: bv0089@srmist.edu.in
Received: 14 September 2021; Accepted: 15 October 2021

Abstract: Reliable transmission is vital to the success of the next generation of communications technologies and Fifth Generation (5G) networks. Many sensitive applications, such as eHealth and medical services, can benefit from a 5G network. The Internet of Medical Things (IoMT) is a new field that fosters the maintenance of trust among various IoMT Device to Device (D2D) modern technologies. In IoMT the medical devices have to be connected through a wireless network and constantly needs to be self-configured to provide consistent and efficient data transmission. The medical devices need to be connected with sophisticated protocols and architecture to handle the synergy of the monitoring devices. Today, one of the commonly used algorithms in D2D communication is the Optimized Link State Routing protocol (OLSR). The OLSR is considerably good at effectively utilizing the bandwidth and reserving the paths. One of the major attack against the OLSR is the Node isolation attack, also known as the Gray hole denial of service attack. The Gray hole attack exploits the vulnerabilities present with sharing the topological information of the network. The attackers may use this topological information to maliciously disconnect the target nodes from the existing network and stops rendering the communication services to the victim node. Hence, considering the sensitivity and security concerns of the data used in e-Health applications, these types of attacks must be detected and disabled proactively. In this work, a novel Node Authentication (NA) with OLSR is proposed. The simulation experiments illustrated that the proposed protocol has an excellent Packet Delivery Ratio, minimal End-End delay, and minimal Packet loss when compared to the Ad-hoc On-Demand Distance Victor (AODV) protocol and the proposed authentication scheme was able to protect the OLSR protocol from a node isolation attack.

Keywords: 5G; AODV; D2D; IoMT; OLSR; security issues

1 Introduction

The Internet of Things (IoT) is a network of devices that includes mobile devices, wearable electronics, and other things. They have a unique Internet address (IP) that allows them to communicate with neighbouring network entities (e.g., smart home users). The sensors and sophisticated Application

Programming Interfaces (APIs) are used to connect and share data over the Internet [1]. The Internet of Medical Things (IoMT) is another sort of IoT communication ecosystem. In contrast to traditional function-specific embedded devices, an IoT device is a domain-specific microcomputer. It consists of medical devices/sensors and software that are required to connect them with the servers/virtualized storage arrays. In [2] IoT based smart healthcare systems, the monitoring devices needs to be connected over the Internet. The support for the wireless communication technologies (such as the 5G network) are also integrated into protocols that are operating the medical devices, to enable smoother Device-to-Device (D2D) communication, which is the IoMT communication environment's base.

The D2D communication network is one of 5G's core technologies (D2D), a collection of medical devices that can communicate wirelessly with one another without relying on a centralised infrastructure or authority. A chain of intermediate nodes is used to transport data packets from one device to another. For UDP (User Datagram Packet) based network packet transfer, a variety of routing methods is available. The majority of these algorithms can be classified as proactive and reactive routing protocols.

1.1 Concerns in Reactive Routing Protocols

AODV and Dynamic Source Routing protocol (DSR) are the reactive protocol which finds a route only when it is needed. Regardless of the routing technique, the ability of all nodes to be recognised by other nodes, even while in motion, is one of D2D's most significant needs and a key component of its success. Because of the frequent topological changes, these methods differ from normal routing algorithms used in traditional networks. At times the route that was persistent between the two medical devices can be broken. This may happen due to the mobility of the intermediate nodes. With the various other reasons, the medical nodes can be connected and disconnected from the network at any time, which might disrupt the network connectivity and the expected level of network performance. These are the major security breaches that possibly affect the performance of the internet connected medical applications.

1.2 Concerns in Proactive Routing Protocols

Every medical node in a proactive protocol, such as OLSR (Optimized Link State Routing Protocol) and Destination-Sequenced Distance Vector Routing protocol (DSDV) keeps track of all possible network destinations and the best routes to reach. This is one of the major concerns when accounting the security breaches available for the internet connected medical applications.

One of the most often used algorithms presently is the OLSR. Although OLSR is very effective at utilising bandwidth and calculating paths, it is vulnerable to a variety of attacks like black hole attack, gray hole attack, Denial of Service (DoS) attack etc. Because OLSR relies on network node collaboration, it is vulnerable to a few collaborating malicious nodes. However, in some cases the route might be disrupted merely by a single intruder node that causes route failure. Communication delay, link spoofing, flooding, wormhole, replay, black-hole, collusion mis-relay, and denial-of-service attacks are all instances of attacks.

The OLSR protocol follows a network overhead-reduction enhancement-based routing approach, in contrast to the traditional Link-State Routing protocol. On the other hand, the original LSR makes use of a flooded topology. Due to various inconsistencies these routing algorithms could reveal the existence of an attack but not the attacker. In Raffo et al. [3] presented a methodology for minimising the vulnerabilities and improving the security of the OLSR routing protocol from intruders and malicious nodes. The HELLO and TC messages are digitally signed by each node. These signatures will be used by the other nodes that wish to validate their own HELLO and TC messages. This technique is effective, but it comes at a cost of huge overhead; in addition to the specific OLSR overhead.

Hence signing messages takes a significant amount of computation, which becomes a cumulative component as the network expands in size for the scalability. Another concern is that the network loses its spontaneity because in order to share public keys, all nodes must know each other before hand the connection is established. This restricts the network from naturally growing to the large number of nodes at a given time and location, which is an important concern in 5G based medical D2D communication.

1.3 Concerns in Node Isolation Attack

An attacker node performs a node isolation attack by pretending to be a fictitious node and broadcasting a TC message to the victim node, claiming to have a node adjacent to reach all of the victim node's two hop neighbours. As a result, the victim node selects the attacker node as its single MPR node, to which it relays data. The packets might not make it to the destination node, though. As shown in Fig. 1 below.

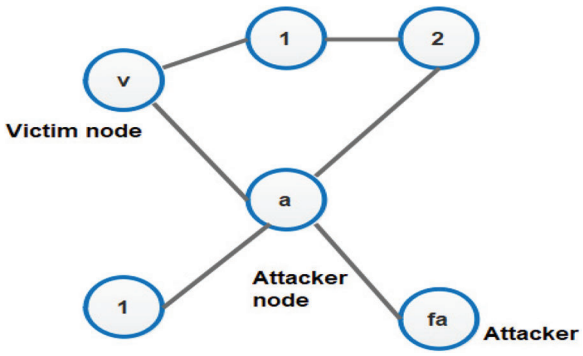


Figure 1: Node isolation attack

That the attacker node 'a' sends the TC message {v, 2, 3, 1, Fa} to the victim node 'v'. Since the message includes all of the two hop neighbours the victim node has very less possibilities to reject the attacker message. Therefore, it chooses the attacker node as its lone MPR. As a result, the attacker node can simply isolate the victim node from the rest of the network, resulting in a clusters of network partition. Because Node 2 is not identified as the MPR, it can continue to exchange data with the victim, but it will not disseminate that data.

The organization of this research article is preceded in such a way that the related research articles are analyzed in Section 2 with a detailed illustration in Section 3. The performance analysis is performed in Section 4 with a conclusion in Section 5.

2 Related Works

IoT technologies are being developed and implemented at a rapid pace, security concerns in IoT devices are only likely to get worse. In the instance of the Internet of Medical Things (IoMT), which is concerned with the communication and control of advanced medical devices, it becomes a very severe issue. Different types of IoT malware are continually being developed. These new malwares have the potential to disrupt IoMT connection and even manipulate smart medical devices. The conventional threat identification methods are insufficient for detecting and analysing the threats in IoT/IoMT networks.

2.1 Multi-Hop D2D Communication Networks: A Secure Routing Solution

In fact, the security solutions are interoperable, to promote the backward and future compatibility. The lightweight protocol proposed by Liu et al. [4] in combines end to end and digital signature authentication. This integration of authentication is carried out on the existing AODV. Because a multi-hop D2D network is

essentially an ad hoc network based on multi-hop D2D, Ad hoc network routing protocol is frequently referred to as "multi-hop D2D network routing protocol".

2.2 Device to Device Network Routing Protocol with Multiple Hops

According to Venkatesan et al. [5] operational mechanisms, ad hoc routing protocols are divided into three types: i) table-driven routing protocols, ii) passive routing protocols and iii) hybrid routing systems. Based on diverse network designs, ad hoc network routing protocols can be divided into flat and hierarchical routing systems. The majority of contemporary ad hoc network routing systems are variations on traditional ad hoc network routing approaches. Network Service Quality and resilience are two enhancement indicators. In [6] Istikmal et al. proposed an AODV Signal-To-Noise Ratio (SNR)-Selective Routing (SR) protocol in the reverse routing process, selective routing depending on the SNR threshold; In Tata et al. [7] suggested an upgraded AODV protocol that is a selective ad hoc on-demand multipath distance vector method based on load balancing. The majority of studies on reliable route in multi-hop D2D network technologies are currently focused on improving the original ad hoc routing protocol, and it focuses on specific attack strategies.

2.3 Defending Against DoS Attacks Using Secure Routing Protocols

In multi-hop Device to Device networks, denial of service (DoS) threats is widespread; As a result, DoS attacks can be mitigated using hash functions and other mechanisms for authenticating the source of data packets. In Patil et al. [8] presented a better ALERT protocol utilizing pseudonym of node location methodology to withstand DoS attacks. Node trust is also used by academics to detect fraudulent nodes and defend against various attacks. In Kumar et al. [9] created a DoS-resistant AODV protocol. According to the proposed protocol, dummy and false packets are transmitted between the source and destination nodes. This bogus transmission is carried out in order to determine the node's trustworthiness and detect any fraudulent nodes. Researchers have also offered secure routing methods for certain DoS threats. In Marimuthu et al. [10] proposed an Extended Optimized Link State Routing protocol that works on the authentication mechanism to resist certain categories of DOS attacks.

2.4 Prevention of Black Hole Attacks with Secure Routing Protocols

Researchers also have investigated different types of methods to safeguard from black hole attacks which are presumed to be one of the most frequent attacks. The route discovery process in the dynamic source routing protocol along with the RREP packets are optimal which makes it resistant to black hole attacks. To prevent black hole attacks, Deshmukh et al. [11] included an authenticity value in the Route Reply (RREP) packet in DSR protocol. In Bhardwaj [12] suggested methods to check the packets in order to confirm the route authentication. The old reactive routing system AODV can assist to protect from malicious attacks by discovering malicious routes and malicious nodes. In the AODV protocol Singh et al. [13] suggested to prevent black hole attacks, a blacklist flag and routing identities are used to identify hostile nodes. The Chengetanai [14] protocol mitigates the black hole attack in the AODV routing protocol by verifying that the packet's timestamp satisfies the destination timestamp. To avoid black hole attacks, in Yadav et al. [15] demonstrated an approach in which, the destination node decides the legitimacy of the RREQ response path based on the criteria in a reliable AODV routing protocol. They have provided a methodology where in the route is made secure by using encryption which helps to prevent black hole attacks.

2.5 Prevention of Gray Hole and Worm Hole Attacks with Secure Routing Protocols

Only a limited number of routing protocols have been developed expressly for grey hole and wormhole attacks. To determine the applicable secure routes, online packet data calculation devices and parameters are

used, In Kumar et al. [9] discovered Data packet transmission rates that are abnormally high on some nodes. This technique can withstand a variety of attacks since nodes with abnormal packet data available bandwidth may be plotting a black hole, grey hole, or wormhole attack. The major objective of the proposed research work is to mitigate the gray hole attack in the 5G oriented Internet of Medical Technology applications.

3 Proposed Methodology

The proposed framework for the minimization of Gray-Hole Attack in 5G based IoMT applications is discussed in this section. The Network Model, identification of Neighbor and Multi Point Relay (MPR) and Secure Routing Strategy are the essential components in the proposed attack mitigation system.

3.1 Proposed Architecture

In Optimized Link State Routing Protocol based networks, node authentication is a technique used to particularly handle a DoS attack known as node isolation attack. We assign a unique key to each unique node to improve node and network security. When sending data packets from source to destination, the node will validate the key value. If the key value is found to be correct, the packet will be successfully transmitted. It detects malicious nodes attempting to manipulate Topology Control (TC) messages using just the victim's internal data. Hence based on the authentication the Multi-point Relay Nodes (MPRs) will be permitted and they will be avoided in case of MPR node path with invalid authentication. To establish a new MPR node that can be accessed via alternate routes, a novel approach, known as Node Authentication (NA), is proposed. The proposed approach is based on each node's own information gained during ordinary routing, as well as the use of virtual (fictitious) nodes. The overall system flow diagram is defined in Fig. 2 below. By avoiding the fictitious node, the victim node is able to arrive at their destination in a secure environment.

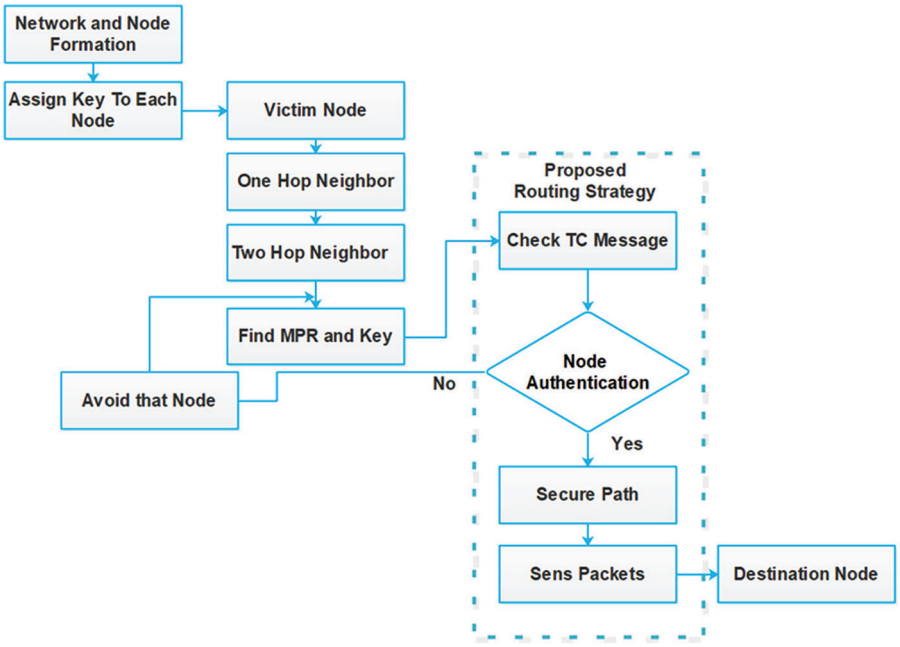


Figure 2: Flow diagram of the proposed node authentication scheme

3.2 Modules of the Proposed Node Authentication Scheme

The modules present in the proposed Node Authentication Scheme are as follows:

1. Model of a network
2. Neighbor and Multi Point Relay (MPR)
3. Secure routing approach

3.2.1 Model of a Network

A 5G wireless network instance with 'N' number of nodes is considered in the Network Animator (NAM) animator's 2D plane. The deployed nodes are aware of their location and can communicate directly with their neighbors. Through multi-hop communications, the entire network is fully connected. Every node has a set maximum and minimum transmission range R. The communication between nodes is organised like a tree, with the destination at the edge. In this communication tree, data is exchanged via the nodes as shown in the Fig. 3 given below.

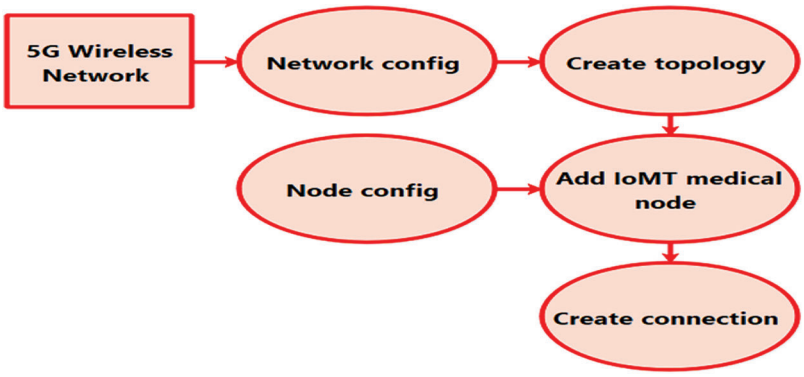


Figure 3: Setting up the network model in the NAM simulator

3.2.2 Neighbour and Multi-Point Relay (MPR)

The equation for the computation of distance between the each node's one hop neighbours is as follows:

$$Distance = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \tag{1}$$

The energy of the neighboring node is determined using the Eq. (2).

$$RE_{AVG} = \frac{RE_i}{N} \tag{2}$$

The shortest path among any two nodes are determined using Eq. (3).

$$x_{ij} = x_{ij} / \sum_{n=1}^{N} x_n^2 \tag{3}$$

If the estimated distance between nodes is much less than or equivalent to 250 m range, they are considered neighbours and are listed together. The two hop neighbours of a node are also calculated and added to a list in the same way. This list is sorted by unique nodes and, if present, removes itself from the list. The MPRs (Multi Point Relays) are then found using the sorted list. An MPR is defined as a node in a sorted list that has more than two neighbours as shown in the Fig. 4 given below.

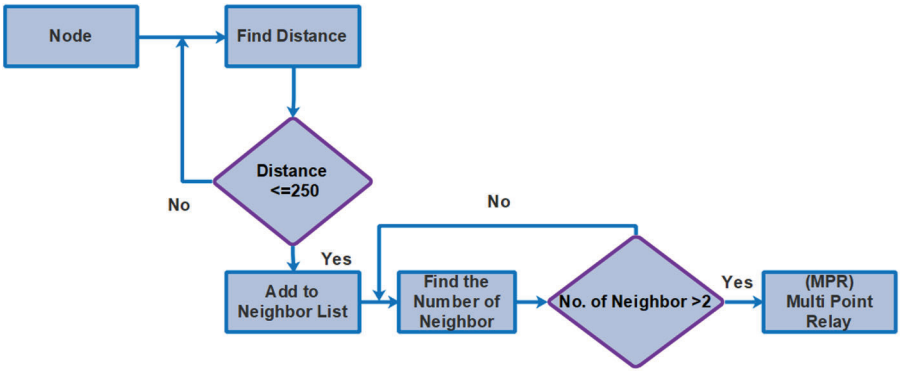


Figure 4: Flow diagram of the neighbour and multi-point relay (MPR)

3.2.3 Secure Routing Approach

By utilising a fictional node and authenticating Topology Control (TC) messages, secure routing in a Medial D2D network can be achieved, bypassing a DoS attacker [16]. As the TC message delivered by the attacker may have inconsistencies due to the fact that it may not be sent by the attacker's original neighbours, we have to check the TC messages to locate the attacker nodes. As the MPR nodes are used to find the shortest routing path, the attackers can be filtered out. We utilized the NA-OLSR routing to arrive at the secure routing path as shown in the Fig. 5 given below.

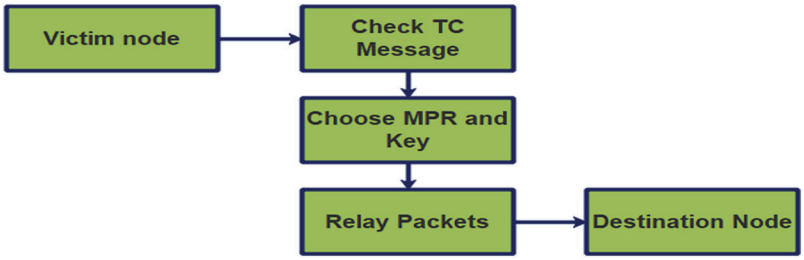


Figure 5: Secure routing approach

We have taken the MPR list to check if it contains any fictious attackers, or any fictious nodes. In case of fictious attackers or nodes found it will be removed from the list. Once after the removal of anomalies the shortest route to the destination has been found. The path is provided for routing UDP packets using the NA-OLSR protocol.

4 Simulation Setup

The built-in NA-OLSR module in the Network Simulator (NS2) was used. It was enhanced to support node authentication using the protocol described above. Most simulation value sets were run a total of _1,000 times, with the average results presented. The movement was 1.5–2 m/s (5.4–7.2 km/h) where applicable and broadcast range was roughly 250 m. A series of simulations were used to verify the efficiency of node authentication against Gray-hole attacks [17]. In a 750 m × 1000 m space, a randomised network topology with a fluctuating number of nodes was employed, with network density ranging from 30 to 100 nodes.

The Simulated sessions which have no communication between its components were rejected, and the estimated outcome was ignored. Three predetermined nodes were used in each simulation. There is a victim,

source node, and an attacker that sends messages to the victim. The target nodes which are assumed to be as victims and source nodes are positioned randomly. The simulation settings are such that the victim nodes and the nodes from where the attack [18] originates are separated by a minimum of two hops distance. This limitation is demonstrated by the fact that one-hop neighbours are virtually secured from attackers, rendering all additional protection redundant.

4.1 Results and Discussion

This section explains the experiment used to efficiently evaluate the proposed system's accuracy and performance in comparison to the approaches specified.

4.1.1 Node Initialization

A total of 40 medical nodes have been added to the 5G wireless network. The NA-OLSR routing protocol were configured. With Constant Bit Rate (CBR) traffic, the Nam animation is specified for a size of 1500 × 1500 pixels. The snapshot of the scenario of 40 nodes is shown in Fig. 6 given below.

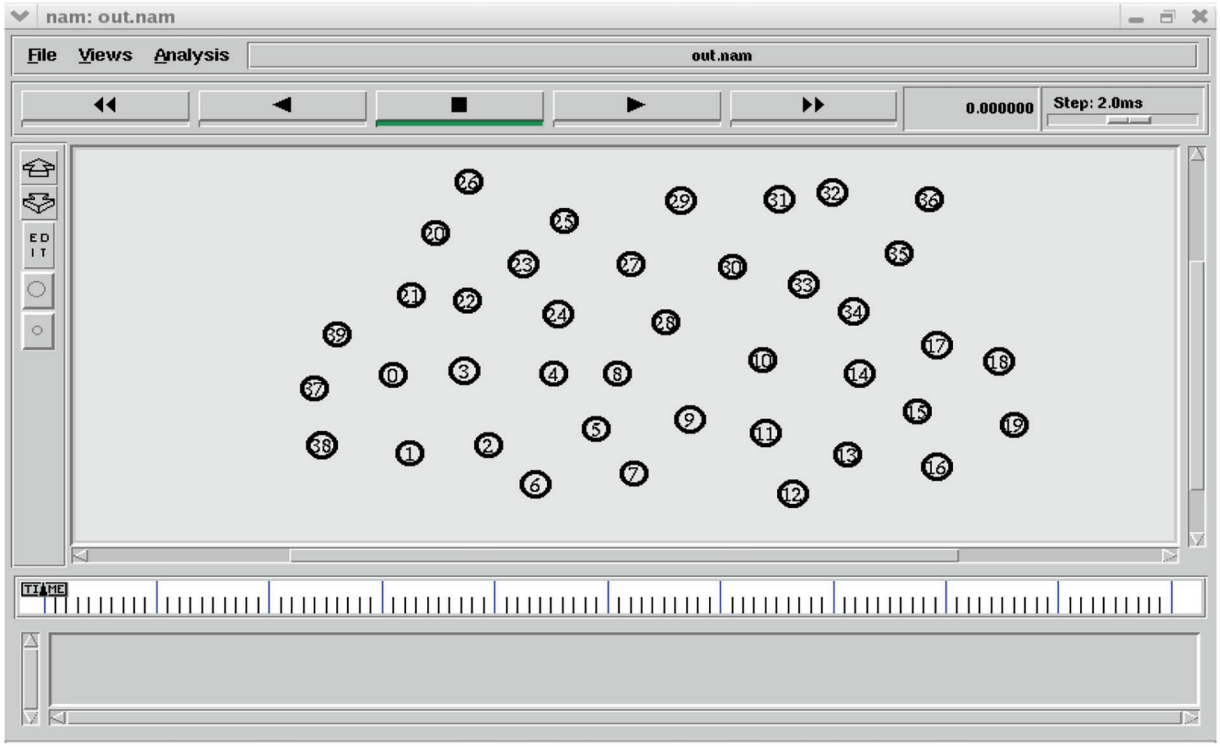


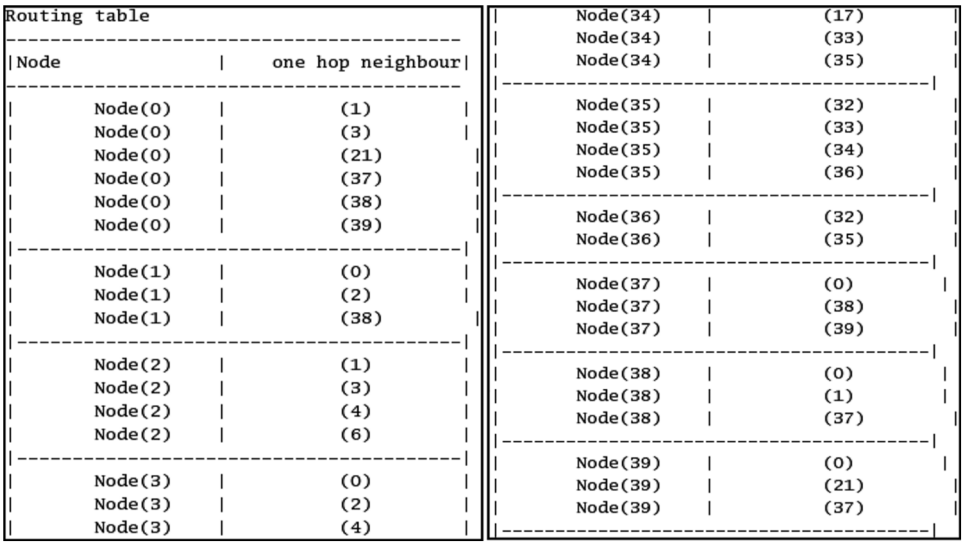
Figure 6: Node initialization

4.1.2 Single Hop Neighbour Detection

Distance calculation algorithms are used to identify the one hop neighbour for each node.

$$d = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \tag{4}$$

The nodes are deemed neighbours and are put in a list if the distance estimated is below or equivalent to 250 m range. Neighbour detection from node 0 to node 39 is shown in the Fig. 7 given below.



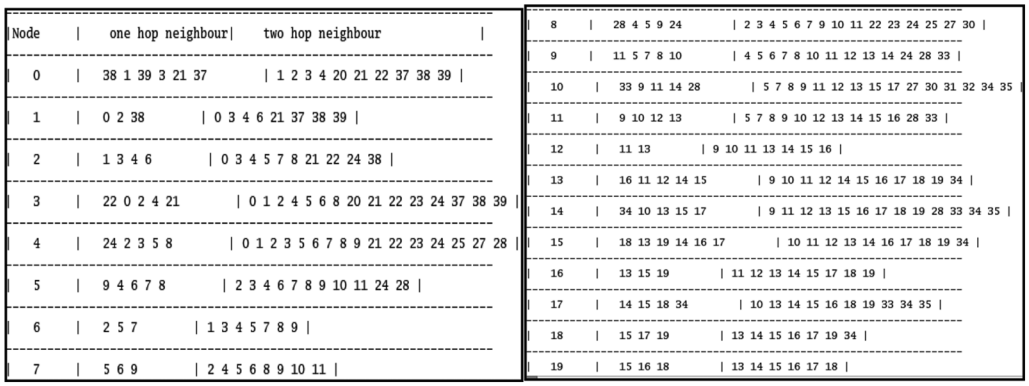
Routing table

Node	one hop neighbour
Node(0)	(1)
Node(0)	(3)
Node(0)	(21)
Node(0)	(37)
Node(0)	(38)
Node(0)	(39)
Node(1)	(0)
Node(1)	(2)
Node(1)	(38)
Node(2)	(1)
Node(2)	(3)
Node(2)	(4)
Node(2)	(6)
Node(3)	(0)
Node(3)	(2)
Node(3)	(4)
Node(34)	(17)
Node(34)	(33)
Node(34)	(35)
Node(35)	(32)
Node(35)	(33)
Node(35)	(34)
Node(35)	(36)
Node(36)	(32)
Node(36)	(35)
Node(37)	(0)
Node(37)	(38)
Node(37)	(39)
Node(38)	(0)
Node(38)	(1)
Node(38)	(37)
Node(39)	(0)
Node(39)	(21)
Node(39)	(37)

Figure 7: Neighbour detection

4.1.3 Two Hop Neighbour Detection

The Nodes' two hop neighbours were calculated, for example, if node 0's neighbours are 4, 5, 6, then the neighbour nodes of 4, 5, 6 are assumed to be node 0's two hop neighbours and are added to a list as shown in the Fig. 8 given below.



Node	one hop neighbour	two hop neighbour
0	38 1 39 3 21 37	1 2 3 4 20 21 22 37 38 39
1	0 2 38	0 3 4 6 21 37 38 39
2	1 3 4 6	0 3 4 5 7 8 21 22 24 38
3	22 0 2 4 21	0 1 2 4 5 6 8 20 21 22 23 24 37 38 39
4	24 2 3 5 8	0 1 2 3 5 6 7 8 9 21 22 23 24 25 27 28
5	9 4 6 7 8	2 3 4 6 7 8 9 10 11 24 28
6	2 5 7	1 3 4 5 7 8 9
7	5 6 9	2 4 5 6 8 9 10 11
8	28 4 5 9 24	2 3 4 5 6 7 9 10 11 22 23 24 25 27 30
9	11 5 7 8 10	4 5 6 7 8 10 11 12 13 14 24 28 33
10	33 9 11 14 28	5 7 8 9 11 12 13 15 17 27 30 31 32 34 35
11	9 10 12 13	5 7 8 9 10 12 13 14 15 16 28 33
12	11 13	9 10 11 13 14 15 16
13	16 11 12 14 15	9 10 11 12 14 15 16 17 18 19 34
14	34 10 13 15 17	9 11 12 13 15 16 17 18 19 28 33 34 35
15	18 13 19 14 16 17	10 11 12 13 14 16 17 18 19 34
16	13 15 19	11 12 13 14 15 17 18 19
17	14 15 18 34	10 13 14 15 16 18 19 33 34 35
18	15 17 19	13 14 15 16 17 19 34
19	15 16 18	13 14 15 16 17 18

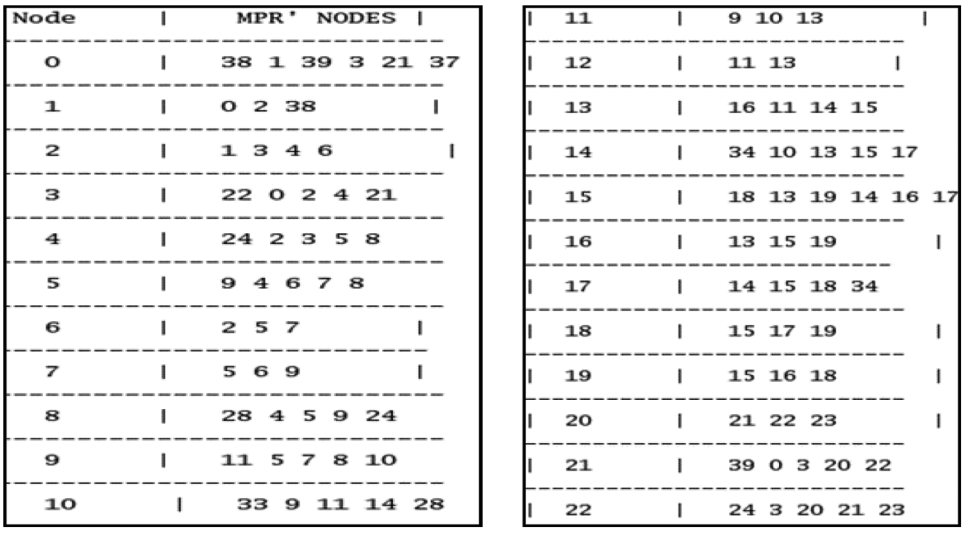
Figure 8: Two hop neighbour detection

4.1.4 MPR (Multi Point Relay) Selection

The two-hop neighbour list is sorted by unique nodes, and if node 0 is available in the list, it is removed. The loop is run, and the two hop neighbours of each node with unique neighbours are obtained. This sorted list is then used to look for Multi Point Relays. An MPR is defined as a node in a sorted list which has more than two neighbours as shown in the Fig. 9 given below.

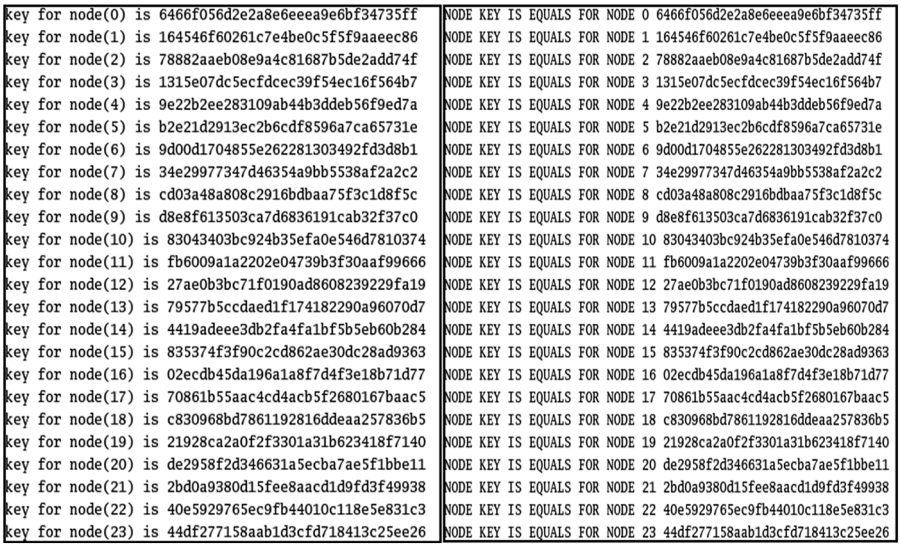
4.1.5 Evaluating the Keys and TC Message

Every node gets its own key. The key value is checked by the node during the transport of data packets from the origin to destination device. If the value of the key is correct, then the packet will be successfully transmitted as shown in the Fig. 10 in the given below.



Node	MPR' NODES
0	38 1 39 3 21 37
1	0 2 38
2	1 3 4 6
3	22 0 2 4 21
4	24 2 3 5 8
5	9 4 6 7 8
6	2 5 7
7	5 6 9
8	28 4 5 9 24
9	11 5 7 8 10
10	33 9 11 14 28
11	9 10 13
12	11 13
13	16 11 14 15
14	34 10 13 15 17
15	18 13 19 14 16 17
16	13 15 19
17	14 15 18 34
18	15 17 19
19	15 16 18
20	21 22 23
21	39 0 3 20 22
22	24 3 20 21 23

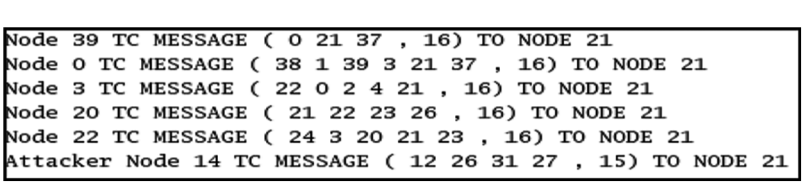
Figure 9: MPR (Multi Point Relay) selection



key for node(0) is 6466f056d2e2a8e6eeea9e6bf34735ff	NODE KEY IS EQUALS FOR NODE 0 6466f056d2e2a8e6eeea9e6bf34735ff
key for node(1) is 164546f60261c7e4be0c5f5f9aaeec86	NODE KEY IS EQUALS FOR NODE 1 164546f60261c7e4be0c5f5f9aaeec86
key for node(2) is 78882aaeb08e9a4c81687b5de2add74f	NODE KEY IS EQUALS FOR NODE 2 78882aaeb08e9a4c81687b5de2add74f
key for node(3) is 1315e07dc5ecfdcec39f54ec16f564b7	NODE KEY IS EQUALS FOR NODE 3 1315e07dc5ecfdcec39f54ec16f564b7
key for node(4) is 9e22b2ee283109ab44b3ddeb56f9ed7a	NODE KEY IS EQUALS FOR NODE 4 9e22b2ee283109ab44b3ddeb56f9ed7a
key for node(5) is b2e21d2913ec2b6cdf8596a7ca65731e	NODE KEY IS EQUALS FOR NODE 5 b2e21d2913ec2b6cdf8596a7ca65731e
key for node(6) is 9d00d1704855e262281303492fd3d8b1	NODE KEY IS EQUALS FOR NODE 6 9d00d1704855e262281303492fd3d8b1
key for node(7) is 34e29977347d46354a9bb5538af2a2c2	NODE KEY IS EQUALS FOR NODE 7 34e29977347d46354a9bb5538af2a2c2
key for node(8) is cd03a48a808c2916bdbaa75f3c1d8f5c	NODE KEY IS EQUALS FOR NODE 8 cd03a48a808c2916bdbaa75f3c1d8f5c
key for node(9) is d8e8f613503ca7d6836191cab32f37c0	NODE KEY IS EQUALS FOR NODE 9 d8e8f613503ca7d6836191cab32f37c0
key for node(10) is 83043403bc924b35efa0e546d7810374	NODE KEY IS EQUALS FOR NODE 10 83043403bc924b35efa0e546d7810374
key for node(11) is fb6009a1a2202e04739b3f30aaf99666	NODE KEY IS EQUALS FOR NODE 11 fb6009a1a2202e04739b3f30aaf99666
key for node(12) is 27ae0b3bc71f0190ad8608239229fa19	NODE KEY IS EQUALS FOR NODE 12 27ae0b3bc71f0190ad8608239229fa19
key for node(13) is 79577b5ccdaed1f174182290a96070d7	NODE KEY IS EQUALS FOR NODE 13 79577b5ccdaed1f174182290a96070d7
key for node(14) is 4419adeee3db2fa4fa1bf5b5eb60b284	NODE KEY IS EQUALS FOR NODE 14 4419adeee3db2fa4fa1bf5b5eb60b284
key for node(15) is 835374f3f90c2cd862ae30dc28ad9363	NODE KEY IS EQUALS FOR NODE 15 835374f3f90c2cd862ae30dc28ad9363
key for node(16) is 02ecdb45da196a1a8f7d4f3e18b71d77	NODE KEY IS EQUALS FOR NODE 16 02ecdb45da196a1a8f7d4f3e18b71d77
key for node(17) is 70861b55aac4cd4acb5f2680167baac5	NODE KEY IS EQUALS FOR NODE 17 70861b55aac4cd4acb5f2680167baac5
key for node(18) is c830968bd7861192816ddeaa257836b5	NODE KEY IS EQUALS FOR NODE 18 c830968bd7861192816ddeaa257836b5
key for node(19) is 21928ca2a0f2f3301a31b623418f7140	NODE KEY IS EQUALS FOR NODE 19 21928ca2a0f2f3301a31b623418f7140
key for node(20) is de2958f2d346631a5ecba7ae5f1bbe11	NODE KEY IS EQUALS FOR NODE 20 de2958f2d346631a5ecba7ae5f1bbe11
key for node(21) is 2bd0a9380d15fee8aacd1d9fd3f49938	NODE KEY IS EQUALS FOR NODE 21 2bd0a9380d15fee8aacd1d9fd3f49938
key for node(22) is 40e5929765ec9fb44010c118e5e831c3	NODE KEY IS EQUALS FOR NODE 22 40e5929765ec9fb44010c118e5e831c3
key for node(23) is 44df277158aab1d3cfd718413c25ee26	NODE KEY IS EQUALS FOR NODE 23 44df277158aab1d3cfd718413c25ee26

Figure 10: Evaluating the keys

The TC messages exchanged by relay nodes and attacker nodes [19]; From the above Fig. 10 the details of the attacker node can be found (For ex: For the Node 14 its neighbour is 34, 10, 13, 15, 17). The attacker may send fictitious TC message to isolate the victim node from the network as shown in Fig. 11 given below.



```
Node 39 TC MESSAGE ( 0 21 37 , 16) TO NODE 21
Node 0 TC MESSAGE ( 38 1 39 3 21 37 , 16) TO NODE 21
Node 3 TC MESSAGE ( 22 0 2 4 21 , 16) TO NODE 21
Node 20 TC MESSAGE ( 21 22 23 26 , 16) TO NODE 21
Node 22 TC MESSAGE ( 24 3 20 21 23 , 16) TO NODE 21
Attacker Node 14 TC MESSAGE ( 12 26 31 27 , 15) TO NODE 21
```

Figure 11: Fictitious TC message

4.1.6 Finding Shortest Route to Destination

Considering a destination node and a source/victim node, the shortest route from source to Destination device was calculated. For example, if the source node is node 21 and the destination node is node 18, the MPRs of 21 are 39, 0, 3, 20, 22. We have taken the MPR list and checked to see if it contains any attacker, attacker fictious, and fictious nodes, and if found, they were removed from the list.

First, we computed the distance between 21 and 39 and stored it in variable 'g'. Next, we calculated the distance between 21 and 0 and saved it in variable 'g1'. Finally, we compared the distance between 'g' and 'g1' and chose the node with the lowest distance value as the relay node. Similarly, we calculated MPR for all 21 nodes and select the best one (for example, node 3) to act as a relay. Shown in the Fig. 12 in the given below.

```
Source Node is 21
Destination Node is 18
39 0 3 20 22
|----------------------------------------|
SELECTED NEXT HOP NODE 3
|----------------------------------------|
3
22 0 2 4 21
|----------------------------------------|
SELECTED NEXT HOP NODE 4
|----------------------------------------|
4
24 2 3 5 8
|----------------------------------------|
SELECTED NEXT HOP NODE 8
|----------------------------------------|
8
28 4 5 9 24
|----------------------------------------|
SELECTED NEXT HOP NODE 9
|----------------------------------------|
9
11 5 7 8 10
|----------------------------------------|
SELECTED NEXT HOP NODE 33
|----------------------------------------|
33
34 10 35 30 31 32
|----------------------------------------|
SELECTED NEXT HOP NODE 34
|----------------------------------------|
34
14 17 33 35
|----------------------------------------|
SELECTED NEXT HOP NODE 17
|----------------------------------------|
17
14 15 18 34
|----------------------------------------|
SELECTED NEXT HOP NODE 18
|----------------------------------------|
18
21 3 4 8 9 10 33 34 17 18
```

Figure 12: Finding shortest route to destination

4.1.7 Attack Detection

Consider a destination node and a source/victim node. For example, Let's pretend node 21 is the source and node 18 is the destination. We have taken the MPR list and check to see if it contains attacker, attacker fictious, and fictious node, if found it will be removed from the list. The relay's neighbours are then taken and the best one is found, and this cycle continues until we arrive at our target and find a way. The path shown in the Fig. 13 is for sending UDP packets using the NA-OLSR protocol as the routing protocol.

4.2 Experimental Analysis

We have used a 40-node setup in this scenario. For all scenarios, the sink packets were monitored for Packet Lost, Packet Delivery Ratio and End-to-end latency in order to calculate the performance of the communication network.

4.2.1 Ratio of Packets Delivered

The performance of any routing protocol is measured by many parameters of which the packet delivery ratio is a significant indicator of the performance. The simulation settings used determine the protocol's reliability. The significant metrics to be taken into consideration are packet size, number of hops,

available bandwidth, and network topology. The packet delivery ratio is the ratio of packets received at the destination to packets transmitted from the source. A sample of 1000 packets is transmitted over the network to determine the packet delivery ratio. The performance improvement is directly proportional to the packet delivery ratio as stated in Tab. 1 and computed from the formula given below.

$$Packet\ Delivery\ Ratio = \Sigma(The\ total\ number\ of\ packets\ received\ by\ all\ destination\ nodes)/ \Sigma(The\ total\ amount\ of\ packets\ that\ all\ source\ nodes\ have\ sent) \quad (5)$$

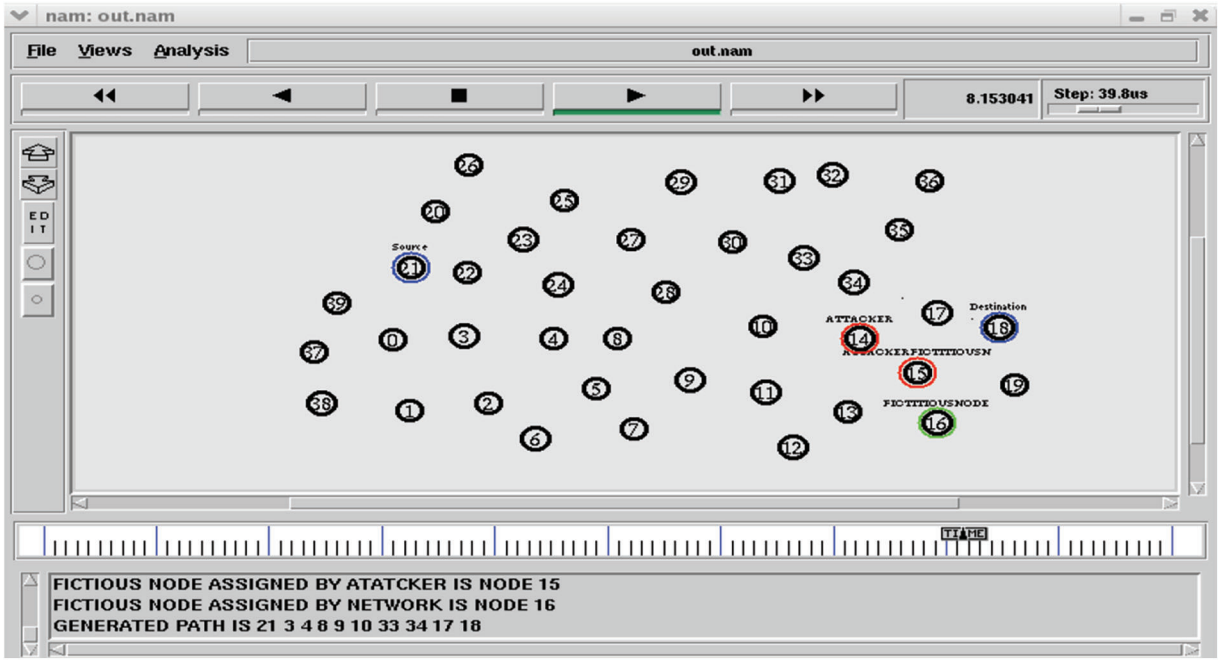


Figure 13: Attack detection

Table 1: Comparison of PDR of AODV and NA-OLSR

NODES	Existing system (AODV) units (%)	Proposed system (NA-OLSR) units (%)
5	0.01128	0.02128
10	0.30223	0.70223
15	0.40223	0.70223
20	0.34096	0.68096
25	0.50863	0.80864
30	0.53750	0.72352
35	0.47466	0.76600

For 40 nodes the experiment was set to run for 10 s. It is calculated in bits per second (bit/s) and has a decent net connection channel capacity. While bypassing the attacker, the proposed framework has a high packet delivery ratio when compare to existing system.

4.2.2 End to End Delay

End-to-end delay is the average time it takes a packet to transit from its source to its destination across a network. The average end-to-end latency can be calculated by taking the mean of all successfully delivered messages' end-to-end delays. As a result, the terms of throughput influences end-to-end latency. The probability of packet drops increases as the number of hops between a source and destination increases. The experiment was set to run for 10 s on node 40. In the existing system, the delay is high when the attacker is present in the routing path shown in Tab. 2. It can be expressed mathematically as given below:

$$Average\ End\text{-}to\text{-}End\ Delay = Total\ time\ taken\ from\ start\ to\ finish / Total\ no.\ of\ packet\ sent \quad (6)$$

Table 2: End to end delay

NODES	Existing system (AODV) UNITS (M/S)	Proposed system (NA-OLSR) UNITS (M/S)
5	1.58929	0.98929
10	1.00589	0.50598
15	0.50509	0.10589
20	0.60628	0.06198
25	0.80459	0.10467
30	0.50509	0.20583
35	0.60529	0.10532

4.2.3 Packet Loss

Packet loss is defined as the ratio of packets that has never made it to their destination to the number of packets originated by the source. It can be expressed mathematically as a formula shown in below

$$Packet\ Loss = \frac{Number\ of\ Packets\ sent - Number\ of\ Packets\ Received}{No.\ of\ Packets\ Sent} \quad (7)$$

The packet drop in the initialization phase is depicted in the Tab. 3. For node 40, the experiment lasted 10 s. When data transmission fails to reach its destination in a timely manner, it is referred to as packet drop. Packets are frequently dropped before reaching their destination. When there is a delay in bypassing the attacker, packet loss is observed to be moderately significant in Existing system.

Table 3: Packet loss

NODES	Existing system (AODV) UNITS (BYTES)	Proposed system (NA-OLSR) UNITS (BYTES)
5	1000	960
10	6060	3460
15	4430	1430
20	6840	4940
25	10250	5250
30	6300	4970
35	7980	3990

5 Conclusion

Trust management is critical for providing a seamless and dependable communication process between the IoMT integrated eHealth network devices. In a big decentralized system, maintaining reliable communications among various devices is a difficult challenge. A novel method called Node Authentication (NA) with OLSR was presented for this purpose, and the proposed approach was able to mitigate the gray hole attack. The potency of the attack was increased when the attacker was permitted to follow the victim around. The information used to defend the 5G Device to Device (D2D) network was entirely based on the victim's knowledge. The use of a trustworthy third party is no longer necessary. Furthermore, the identical technology that was employed in the attack enhanced the level of protection. With the identification of the topology used and by promoting fictitious nodes, a node can able to detect the suspicious nodes and prevent them designating as a lone MPR, thus avoiding the attack's most key exploit.

This proposed OLSR-based attack mitigation approach could prevent Gray-hole as well as black-hole attacks. We have collected the packet details with a couple of points and also used the internal knowledge gathered by participating nodes, to analyse the node authentication mechanisms. One of the vital concerns is that a non-stop attacker may be attempting to modify network architecture in order to find the security breaches. Although undetected latent attackers could able to drop packets the chances of violating security with the exploits will be significantly reduced since there is no assurance that the routes may be passing through the attacker nodes. We assign a unique key to each independent node to improve node and network security. The node validates the key value when the data transmission from source to destination takes place. If key value found to be correct, the packet will be successfully transmitted. This modified key-based approach, would improve the network security and prevent most similar type of attacks, such as DDOS attempts. The key will be created using a hash function such as MD5 or SHA-1. The suggested approach takes into account the node security by assigning each node a unique key. While the node initialization, the unique key will be shared between nodes. The key will be validated before transmitting the packet to the next hop, boosting the overall network security. The performance analysis of the proposed system exhibits 98.23% of Packet Delivery Ratio and 10% of end to end transmission delay which is proven to be an outperforming performance when compared to the existing methodologies. In future, the proposed work can be extended by identifying the malicious devices at the initial stages and shall be isolated from the network.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy *et al.,* "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, no. 1, pp. 3028–3043, 2017.

[2] T. Li, C. Lee, Y. Weng and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, pp. 1–10, 2016.

[3] D. Raffo, C. Adjih, T. Clausen and P. Muhlethaler, "Securing OLSR using node locations," in *Proc. European Wireless Conf. 2005-Next Generation Wireless and Mobile Communications and Services*, Nicosia, Cyprus, vol. 5, pp. 1–7, 2005.

[4] H. Liu, J. Xia and Q. T. Wang, "Research on a secure and energy-efficient routing protocol for Ad Hoc networks," *Journal of Physics*, vol. 48, no. 2, pp. 83–88, 2021.

[5] T. P. Venkatesan, P. Rajakumar and A. Pitchaikkannu, "A overview of proactive routing protocols in MANET," in *Proc. Int. Conf. on Communication Systems and Network Technologies*, Bhopal, India, pp. 173–177, 2014.

[6] A. Kurniawan, "Selective route based on SNR with cross-layer scheme in wireless ad hoc network," *Journal of Computer Networks and Communications*, vol. 25, pp. 1–13, 2017.

[7] C. Tata and M. Kadoch, "Secure multipath routing algorithm for device-to-device communications for public safety over LTE heterogeneous networks," in *Proc. Int. Conf. on Future Internet of Things and Cloud*, Washington, vol. 7, pp. 212–217, 2015.

[8] P. Patil, N. Marathe and V. Jethani, "Improved ALERT protocol in MANET with strategies to prevent DoS & MITM attacks," in *Proc. Int. Conf. on Automatic Control and Dynamic Optimization Techniques*, Pune, India, vol. 21, pp. 372–377, 2017.

[9] J. A. Kumar and A. Choorasiya, "A security enhancement of AODV routing protocol in mobile ad hoc network," in *Proc. Int. Conf. on Communication and Electronics Systems (ICCES)*, Coimbatore, India, pp. 958–964, 2017.

[10] M. Marimuthu and L. Krishnamurthi, "Enhanced OLSR for defense against DoS attack in ad hoc networks," *Journal of Communications and Networks*, vol. 15, no. 1, pp. 31–37, 2013.

[11] S. R. Deshmukh and N. Chatur, "Secure routing to avoid black hole affected routes in MANET," in *Proc. Symp. on Colossal Data Analysis and Networking (CDAN)*, Indore, India, vol. 16, pp. 1–4, 2016.

[12] A. Bhardwaj, "Secure routing in DSR to mitigate black hole attack," in *Proc. Int. Conf. on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kaniyakumari, India, vol. 13, pp. 985–989, 2014.

[13] K. Singh and S. Sharma, "A new technique for AODV based secure routing with detection blackhole," in *Proc. IEEE Int. Conf. on Power, Control, Signals and Instrumentation Engineering*, Washington, United Sates of America, vol. 41, pp. 1528–1534, 2017.

[14] G. Chengetanai, "Minimising black hole attacks to enhance security in wireless mobile ad hoc networks," in *IST-Africa Week Conf.*, Washington, United States of America, vol. 12, pp. 1–7, 2018.

[15] S. Yadav, M. C. Trivedi, V. K. Singh and M. L. Kolhe, "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme," in *Proc. 4th IEEE Uttar Pradesh Section Int. Conf. on Electrical, Computer and Electronics (UPCON)*, United States of America, vol. 26, pp. 1–4, 2017.

[16] D. Prabakaran and S. Ramachandran, "Multi-factor authentication for secured financial transactions in cloud environment," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 1781–1798, 2022.

[17] J. V. Vadavi and A. G. Sugavi, "Detection of black hole attack in enhanced AODV protocol," in *Proc. Int. Conf. on Computing and Communication Technologies for Smart Nation (IC3TSN)*, Gurgaon, India, pp. 118–123, 2017.

[18] D. Nitnaware and A. Thakur, "Black hole attack detection and prevention strategy in DYMO for MANET," in *Proc. 3rd Int. Conf. on Signal Processing and Integrated Networks (SPIN)*, Delhi, India, pp. 279–284, 2016.

[19] M. Ahmed and M. A. Hussain, "Performance of an IDS in an ad hoc network under black hole and gray hole attacks," in *Proc. Int. Conf. on Electronics, Communication and Instrumentation (ICECI)*, Newyork, USA, pp. 1–4, 2014.