detection and Prevention of malicious node in wireless sensor network

A THESIS

Submitted by

VISHNU K
(RCAS2021MCS202)

in partial fulfillment for the award of the degree of

MASTER OF SCIENCE
SPECIALIZATION IN
INFORMATION SECURITY AND CYBER FORENSICS

DEPARTMENT OF COMPUTER SCIENCE

RATHINAM COLLEGE OF ARTS AND SCIENCE

(AUTONOMOUS)

COIMBATORE - 641021 (INDIA)

MAY - 2023

RATHINAM COLLEGE OF ARTS AND SCIENCE
(AUTONOMOUS)
COIMBATORE - 641021

BONAFIDE CERTIFICATE

This is to certify that the thesis entitled **DETECTION AND PREVENTION OF MALICIOUS NODE IN WIRELESS SENSOR NETWORK** submitted by **VISHNU K (RCAS2021MCS202)**, for the award of the Degree of Master of Computer Science specialization in **"INFORMATION SECURITY AND CYBER FORENSICS"** is a bonafide record of the work carried out by him under my guidance and supervision at Rathinam College of Arts and Science, Coimbatore.

Dr.P.SIVAPRAKASH M.Tech.,Ph.d **Dr.P.SIVAPRAKASH M.Tech.,Ph.d**

Supervisor Mentor

Submitted for the university examination held on 09.05.2023

INTERNAL EXAMINER **EXTERNAL EXAMINER**

RATHINAM COLLEGE OF ARTS AND SCIENCE
(AUTONOMOUS)
COIMBATORE - 641021

DECLARATION

I, **VISHNU K (RCAS2021MCS202)**, hereby declare that this thesis entitled **"DETECTION AND PREVENTION OF MALICIOUS NODE IN WIRELESS SENSOR NETWORK",** is the record of the original work done by me under the guidance of **Dr.P.Sivaprakash M.Tech.,Ph.d**, Faculty Rathinam College of Arts and Science, Coimbatore. To the best of my knowledge, this work has not formed the basis for the award of any degree a similar award to any candidate in any University.

Place: Coimbatore **VISHNU K**

Date: 09.05.2023 **Signature of the Student**

COUNTERSIGNED

Dr.P.Sivaprakash M.Tech.,Ph.d
Supervisor

Contents

Acknowledgement

On successful completion for project look back to thank who made in possible. First and foremost, thank **"THE ALMIGHTY"** for this blessing on us without which we could have not successfully our project.I am extremely grateful to **Dr.Madan.A. Sendhil, M.S., Ph.D.,** Chairman, Rathinam Group of Institutions, Coimbatore and **Dr. R.Manickam MCA., M.Phil., Ph.D.,** Secretary, Rathinam Group of Institutions, Coimbatore for giving me opportunity to study in this college.

I am extremely grateful to **Dr.S.Balasubramanian, M.Sc., Ph.D(Swiss)., PDF(SwissUSA).,** Principal, Rathinam College of Arts and Science(Autonomous), Coimbatore.

Extend deep sense of valuation to **Mr.A.Uthiramoorthy, M.C.A., M.Phil., (Ph.D),** Rathinam College of Arts and Science (Autonomous) who has permitted to undergo the project.

Unequally I thank **Dr.P.Sivaprakash, M.Tech., Ph.D.,** Mentor and **Dr.Mohamed Mallick, M.E.,Ph.D.,** Project Coordinator, and all the Faculty members of the Department - iNurture Education Solution pvt ltd for their constructive suggestions, advice during the course of study.

I convey special thanks, to the supervisor **Dr.P.Sivaprakash M.Tech.,Ph.d** who offered their inestimable support, guidance, valuable suggestion, motivations, helps given for the completion of the project. I dedicated sincere respect to my parents for their moral motivation in completing the project.

List of Figures

List of Abbreviations

WSN	Wireless Sensor Network
HMND	Hybrid Malicious Node Detection
RTT	Round Trip Time
PDR	Packet Delivery Ratio
NS-2	Network Simulator-2
AODV	Ad-hoc On-Demand Distance Vector
AOMDV	Ad-hoc On-Demand Multipath Distance Vector
CH	Cluster Head
PSO	Particle Swarm Optimization
NRT	Neighbour Ratio Threshold
LNCA	Local Negotiated Clustering Algorithm

Abstract

In Wireless Senor Networks(WSNs) security is the most significant issue when sending an essential message via wireless connection. WSN are vulnerable to the most popular types of attacks and threats, such as malicious node. A malicious node is very challenging issues that records the packets from one location of the network and tunnels them to another location to undermines the performance of the wireless network and disrupt the most routing protocol. However, the existing solutions have been developed to overcome the malicious node, but still suffering from additional hardware, incur high delay delivery, or fail to provide high throughput, Energy efficiency as well as high delay. In our proposed Hybrid Malicious Node Detection (HMND) algorithm is proposed, which is able to detect both in-band malicious node through performs Round Trip Time (RTT) based on its hop count, and Packet Delivery Ratio (PDR), also out-of-band Malicious nodes through performs transmission range between successive nodes in a more optimistic manner than existing solutions. HMND reduce the delay and energy through avoids performing malicious node detections for all available nodes in the network. HMND does not rely on any special hardware and middleware. The proposed algorithm HMND was executed using NS-2 network simulator. The performance metrics was taking into consideration to evaluate the performance of the proposed algorithm the throughput, end to end delay, packet delivery ratio, and consuming energy. The proposed algorithm utilized Ad-hoc On-Demand Distance Vector (AODV) routing protocol to improve the detection method. The experimental results have shown the performance metrics of the proposed approach HMND outperformed in Malicious node detection compared with existing method.

Chapter 1

Introduction

1.1 Wireless sensor network

Several nodes for the sensor are found in the WSN. To model and forecast eco-friendly technologies to these nodes track broad geographical areas and have features like as minimal bandwidth, less storage, and minimum power usage. Sensor nodes in WSN are distributed in different regions where they gather data from their sensor nodes. In WSN, sensor nodes are configured to conduct numerous jobs, like as signal processing, transmission to the base station of the collected information, and verification of routes with minimal resources. In numerous environments like as an environmental control, military applications, defence, robotics deployment, and lots of more, it is considered that wireless sensor networks are helpful. This leaves WSN prone to several forms of assaults. In all these threats, since it utilises both in-band and out-of-band networks, it is claimed that the harmful assault is a malicious node. Malicious node assault is classified as denial-of-service attack, where through fast channel connection speed named Malicious node link/tunnel, attacker nodes/malicious nodes are intertwined. In Malicious node assaults, there could be at least two attackers in the network, often known as hostile nodes. To access the data for themselves, the attackers control the network and maintain track of wireless operations. Protection problems for the mobile ad hoc networks still relevant as they are fixed in WSN nodes, but all mobile nodes are movable in Mobile Ad hoc Networks (MANETs) [1–4]. It's quite difficult to secure the network in the case when the sensor nodes are in moving state, means nodes are changing their location. A node in MANET is wireless that specifically interacts without any bases often serve as a node-to-node communicator. These Medium nodes are like the usage of multi hop radio networks via routers that are connected without the assistance of pre-existing networking infrastructures through wireless connections. In a malicious node, two conniving sensor nodes tunnel control and data packets between each other, with the intention of creating a shortcut in the WSN. Such a low-latency tunnel between the two conniving nodes will likely increase the probability of its being selected as an active path. With rapid development and increases in the volume of wireless mobile computing technology that has driven a revolution within the computing world, ad-hoc networks have emerged in many forms. Mobile Ad-Hoc networks is a collection of wireless mobile node which communicate directly with each other within its radio coverage to form a temporary networks without pre-existing infrastructure or central base stations [1], [2]. MANET is an unreliable, open medium, self-configured wireless networks and the process of dynamicdevice communication where the participating node can enter or leave is simplied. This leads to changing network topology rapidly and unpredictably [3]. Routing protocols play an important role in wireless network to route the packet over multiple hops and from one node to another, it is the backbone of wireless networks and have ability to show the shortest path from source and destination to achieve specic tasks [4]. In addition, some routing protocols specialized for using in wireless networks with low power consumption [5]. In MANET, the participating node has a limited transmission range. Therefore, two nodes will not be able to communicate with each other if they are not in the range of radio coverage of each other. Thus, the transmission through multi-hops scenario will be employed and the intermediate node has to forward the packet to the next node until it reaches the destination [6]. Due to the wireless transmission spontaneous nature and characteristics of MANET, this makes MANET prone to several type of attack and security threats such as malicious node [7], [8]. Thus, it's important to ensure the condentiality of data transmission in the wireless network from node to node without compromising data transmission integrity. The malicious node is very challenging issues and one of the serious security threats in detection to MANET. The malicious node initiated when an adversary create a communication link between two distant nodes by captures the packet from one location of the network and sends it to unauthorized location of the network. To generate fake connections, mislead the legitimate path, changing or dropping the sent packets which will lead in giving a false network topology [7], [9] and [10] .The attackers are directly connected with each other. Thus, it has the ability to connect faster than legitimate nodes to carry out the attack. encapsulation (in-band) that is forwarding the packet through available legitimate nodes in the network. The out-of-band channel which is also forwarding packets over long distances and use separate external communication link between malicious nodes [11]. In out-of-band attack, the source node and destination node are away from each other. But, due to the fake created tunnel they appear that they are near and direct neighbours of each other which will reduce the hop count. On the other hand, in-band attack use legitimate routes and actual hop count does not increases during traversal. A malicious node does not require the knowledge of a security system, which includes cryptography mechanisms, public/private keys, etc. Thus cannot be detected using cryptographic mechanisms, therefore, even if the transferred packet was encrypted with any type of encryption, the malicious node will be able to tunnel the packet to another distant malicious node [12] and [13].

1.2 Objective of the Project

A malicious node creates holes in network and without any information to the source it keeps on receiving the data packets and consumes the nodes energy and disturbs the delivery of packet. The Malicious node in the network also processes the received packets to the third-party node which is never been the part of the network which affects the overall performance of the WSN. After going with literature for malicious node detection and avoidance in the clustered WSN the at most requirement is to consider the system in a way that can predict the Malicious node in the path and can predict the hole free path for the data transmission. In the current work the major focus is to create secondary paths for the data transmission between defined sources and destination and to predict the hole free path for the data transmission. For the prediction or detection process various parameters are used like time taken to receive acknowledgement, time taken to deliver, pre-defined thresholds, etc. Using the criteria on the basis of computed parameters the secondary path is selected with the assurance that the energy consumption will be efficient, reduction in the packet delivery ratio, packet drop ratio.

1. To study the state of art for malicious node prevention and detection in clustered WSN
2. To study and evaluate the current work in the field
3. To design a hybrid smart technique for the spotting and prevention of Malicious nodes in the clustered WSN,
4. To confirmation the efficacy of the proposed treatment using the defined set of performance evaluation parameters and comparison of the same with some current defined techniques in the literature.

1.3 Existing System

1.3.1 Local Negotiated Clustering Algorithm (LNCA) Outline

Phase I: Create a cluster in that, during a certain time frame, each step is completed.

Step 1: Data interchange readings.

- Each node collects information from the location.
- Transmits the information to its nearest neighbours. The node collects, in return, the data sent by same node party.

- Once a node has access to data from its adjacent neighbours, the node matches the reading of the receiving node to its own.
- The transmitting node raises the ”degree of node” by one.
- A receiving node in its ”neighbour node list” stores the transmitting node id.

Step 2: Exchange Degree Node.

- Each node transmits to its immediate neighbours its ”residual energy” and ”node degree”. The node collects, in return, the information sent to the similar group of nodes.
- In neighbouring node list, each node’s ”node degree” corresponds to the divisions’ ”node degree”.
- The node chooses itself as a representative of the cluster and if it has highest degree of node.
- The node shares as like as the “total node degree along the adjacent node population (say group G) and the node’s residual energy is greater in G, when the node chooses a CL as a cluster head (CH) itself.
- If a node ID group is used to break the tie, and neighboring nodes share the same overall node degree or same residual power. For e.g., when the node has the lowest node ID, the head of the cluster selects itself.

Step 3: Cluster head declaration.

- A CH chosen for their own immediate neighbors in Stage 2 transmitted cluster head (CH) announcements. The TTL3 is set to "many" in CH announcements.

- A cluster head node receives CH post if its ' neighboring node list' contains the final-hop node from in that the packet was made. Node checks Receiving node: if in its neighbouring node.

- Decreases TTL by one in this CH note obtained. If TTL $>$ 0, and node transmits to its own immediate neighbours the CH announcement.

- The parameter "chReceived"4 is verified. Whether it is incorrect to "chReceived".

- Declares as its cluster head the source node which a root node that created the notification from CH and sets "chReceived" to real.

- Sends a message to the cluster header for "registration"5(unicasts).

- "If "chReceived" is still "wrong" at the endings of a node for Step 3 pick themselves as a 'directed cluster head,' a node which is not a CH.

Step 4: Final cluster formation

- If a group is formed, the CH places the submit node ID in the "member node list" receive a "registration" request.

1.3.2 Phase II: Data Reporting

A selected cluster head, such as the forced head of the cluster, submit their "member node list" and data readings to the base station. After a random back-off, a node sends a packet cycle to prevent conflicts triggered by at the same time, nodes sent out packets (e.g., the back-off time is arbitrarily raised from 0 to 20 s during our experiments). Phase II (data reporting) will be recurrent. On the other side, every few data reporting intervals, Step I (Cluster configuration) can be used to re-select cluster heads. The exact occurrence of Step I be contingent on the reliability of the environment the more often the value(s) of the mechanism being tracked change, the most probable a re-clustering of the WSN is needed.

1.4 Challenges in Existing system

A malicious node creates holes in network and without any information to the source it keeps on receiving the data packets and consumes the nodes energy and disturbs the delivery of packet. The malicious node in the network also processes the received packets to the third-party node which is never been the part of the network which affects the overall performance of the WSN. After going with literature for malicious node detection and avoidance in the clustered WSN the at most requirement is to consider the system in a way that can predict the malicious node in the path and can predict the hole free path for the data transmission. In the current work the major focus is to create secondary paths for the data transmission between defined sources and destination and to predict the hole free path for the data transmission. For the prediction or detection process various parameters are used like time taken to receive acknowledgement, time taken to deliver, pre-defined thresholds, etc. Using the criteria on the basis of computed parameters the secondary path is selected with the assurance that the energy consumption will be efficient, reduction in the packet delivery ratio, packet drop ratio.

Chapter 2

Literature Survey

Several algorithms and scientic studies that have been devoted for MANET. Some of these algorithm require specialized hardware or incur high communication overhead. However, we will concentrate on literature on some of the prevailing solutions on MANET and give brief description of all the relevant literature reviewed. Chiu and Lui [15] propose malicious node detection method called Delay Per Hop Indication (DELPHI). DELPHI perform multipath approach and calculates mean delay per hop of every path. The sender calculate mean delay per hop of each route. Thus, malicious node nodes can be detected if the path that has longer delays and will not be selected to transmit the data packet. Due to the information and detection that DELPHI perform at the sender, it does not require synchronized clock to determine the positioning of the node. Amish and Vaghela [16] propose an extension to AODV to detect malicious node called Ad-hoc On-demand Multipath Distance Vector routing protocol (AOMDV). The proposed method based on RTT calculation from the source to destination for every route, then, it divide the value of RTT by corresponding hop count and the average value is a threshold value and compare the RTT value with the threshold to determine the existence of malicious node. Tun and Maw [17] proposed a malicious node detection mechanism based on RTT and neighbour number. The consideration in here is that the adversary can increases the number of neighbours of the nodes within the radius, to provide inaccurate RTT value between successive nodes. Therefore, when the RTT value between two successive nodes is high and the neighbour number is considerable greater than the average neighbour number, there is a suspect that a malicious node path is in between. Capkun et al. [18] propose a method called Secure Tracking of Node Encounter (SECTOR) against malicious node. The distance between two nodes can be calculated based on the speed of data transmitted. The detection method measure the time between sending out a challenges bit and receiving the response, the rest node will compute an upper bound of the distance which is between these two nodes, after than, check whether this distance violates and physical constraints. Lai [19] propose a method against malicious node, by applying the standard routing protocol IPv6 for Low Power and Lossy Networks (RPL). However, this approach delimits the maximum distance that a packet can take in the transmission. The rank of a node denied RPL is adopted to measure the distance. The proposed detection method discovers malicious Malicious node nodes if unreasonable rank values are identified. Hu et al. [20] propose malicious node detection mechanism based on packet leashes. The proposed methodology consider both geographical and temporal leashes. The geographical rely on current location and transmission time associate with the packet. The receiving node will compute the distance to the sender and the time it took the packet to traverse the path to determine whether the packets recipient within a certain distance from the sender. In temporal leashes, based on clock that is tightly synchronized but do not rely on GPS information. The sending node will associate the transmission time and the expiration time to every sent packet to restrict the packet to travel over long distances, and at the receiving node will use its own packet reception time for verification. By using compute lightweight operations which will determine whether the packet pass through the Malicious node path. Hu and Evans [21] proposed mechanism based on directional antennas to prevent malicious node. Neighbour lists will be built in a secure way by using the direction in which a signal is heard from a neighbour with the assumption that the antennas on all the nodes are aligned. However, it only prevents the kind of malicious node in which malicious nodes try to deceive two nodes into believing that they are neighbours. Chen et al. [22], propose a distance-consistency-based secure localization scheme that is employed against malicious node. It consist of three different phases of detection of malicious node. Firstly, detect and identifies whether it is under a duplex malicious node or a simplex malicious node. And second, the valid locator's identification, different identification schemes are proposed to identity the V-locators. Third, self-localization, after identifying the V-locators, the sensor conducts the self-localization using the Maximum Likelihood Estimation (ML) method with correct distance measurements. Jamali and Fotohi [23] proposed a method against malicious node through Artificial Immune System (AIS) which is able to protect against a set of extraneous attacks without affecting the overall performance of the network. The proposed approach consist of two phases, in the rest phase a test packet will be employed and sent from each route and the destination is obliged, a confirmation packet will be send upon receiving test packet. Thus, if the route contain malicious node, the packet will not reach its destination and validation packet will not be received. While in the second phase, usually malicious node having lower hop count compare with actual nodes. Thus, when having a low number of hop counts in a route, the possibility of pollution of this route would increase. Which is the situation with a low round trip time and an increase of total energy of the existing nodes in the route. Tamilarasi and Santhi [24] proposed a method against malicious node in WSN through identifying the malicious node and select the best path. Initially, several path will be generated between source and destination called 'K' using Ad-hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. Then, the malicious node path will be identifies through source node by verifying the Detection Packet (DP) and Feedback Packet (FP) from the destination. After determine the malicious node paths, the source node will selects the best path among the attacker free paths using Particle Swarm Optimization (PSO) algorithm and forwards the data to the destination through the best path. Sankara and Murugaboopathi [25] proposed mechanism based on Quality of Service (QoS) for entire network to detect the malicious node. The Modified Secure AODV protocol (MSADOV) has been proposed which uses the packet forward ratio and round trip time to prevent the malicious node in MANET. In addition, the proposed approach able to detect both active and passive attacks. Jamali and Fotohi [26] proposed a method against wormhole attack node called Defending Against Malicious Node (DAMN) that employ employs fuzzy logic system and artificial immune system. First phase will select high performance route between the source and the destination using fuzzy logic approach. While the second phase will use Artificial Immune System (AIS) based denies scheme against malicious node, where antibodies are trained to detect and eliminate malicious antigens. Aswale and Joshi [27] proposed malicious node prevention using hybrid cryptography algorithm. The proposed technique uses Modied Rivest, Shamir, Adleman (MRSA) and AES for secure and energy-efficient data transmission from source to destination over public channels. Because AES encryption more efficient for large amount of data and does not require high energy, so, it will be used for plaintext encryption and RSA use to encrypt AES key. Thus, AES will encrypt the data of source node. Fotohi et al. [28] proposed malicious node detection system using Agent-based Self-protective Method for Unmanned Aerial Vehicle Networks (ASP-UAVN). The source node will initiate Route Request (RREQ) to the destination to detect the existing routes. Then, once the Route Reply (RREP) is received, a self-protective method using agents and the knowledge base is employed to choose the safest route among other routes and detect the attacking UAVs. This mechanism will protect the network against malicious node, selective forwarding and sink hole attacks.

Chapter 3

Methods and proposed system

3.1 Methods

The proposed algorithm combines RTT based on its hop count, PDR and transmission range features to obtain high accuracy of malicious node detection. The proposed algorithm was implemented for both out-of-band and in-band malicious node and the K-Means clustering algorithm has been employed in this study to determine threshold value in packet delivery ratio, it is a widely used algorithm in the field of data mining. Additionally, K-means is an iterative and powerful algorithm which loops until it converges to a locally optimized solution [14]. In this section, i characterize the preliminaries that required to achieve this study.

3.2 Adversary Model

The network is established in an antagonistic environment where the adversaries are present. Which assume that the adversaries are able to eavesdrop, record and replay messages, including routing protocol messages. Furthermore, the adversary can compromise the legitimate nodes, allowing them to extract their cryptographic secrets messages. This give the opportunity for the adversary to deploy and control a malicious node. The adversary capable of colluding with other malicious nodes. One of these collusion attack is the malicious node.

3.3 Malicious node Description

A malicious node is one of the gravest attacks that are considered a challenging problem and can be launched at the network layer of the OSI model [29]. It consists of two malicious nodes involved in the routing path and communication link between them as illustrated between N and M malicious node. The attacker receives packets at one location in the network and send them to a remote location in the network and then replays them locally. The tunnel can be created in many ways such as in-band and out-of-band. The routing path between source and destination will be selected through the created tunnel [9], [30], [31] and [32], which will be used later for packets exchange between malicious nodes. Because of unauthorized access by malicious nodes, the packet can be dropped and cause delay in time for important packet to reduce the network performance or send to another network and at end the network will be disrupted. malicious node can be classified into four modes of attack operations, which are, packet encapsulation, high power transmission, packet relay and out-of-band. The tunnel can be launched through wired and wireless transmission or an optical link as mentioned in [33], [35]. The packet will be forwarded through distant malicious node by creating an illusion that they are close to each other whereas in reality, they are far. Malicious nodes are equipped with higher transmission power and higher bandwidth in comparison to other legitimate nodes. Therefore, they can transmit packets over long distances to create fake shortcuts, preventing the legitimate nodes to be discovered by its neighbours, creating incorrect routing paths, and then causing network disruptions [34], [35] and [36]. This fake shortcut path which is created by malicious node node will be employed for packet exchange among themselves.

3.4 In-Band malicious node

Based on the medium used, the packets can be tunneled through an in-band and out-of-band attack between two distant malicious nodes [37]. In in-band attacks, the assailants will use the legitimate nodes that have been compromised and the valid existing wireless medium for building a link between malicious nodes. Which will perform the attack on any unprotected packets while packet transmission as illustrated. Assume that the source node is denoted S and destination node denoted D, in that case the routing path is S, M1, A, B, M2, D forms an in-band attack. Therefore, In-band attack is very dangerous and does not need extra hardware to launch it [38], [39] and [40]. In addition, unlike out-of-band attack, in-band attack will consume the normal nodes energy due to the usage of these nodes to perform the attack and route the packet over long path.

3.5 Out-Of-Band malicious node

Whereas an out-of-band attack that initiated through different wireless medium via a side channel. Such a channel has high-gain directional antennas, between two distant nodes to prevent legitimate node from appearing. Creating an illusion to the source

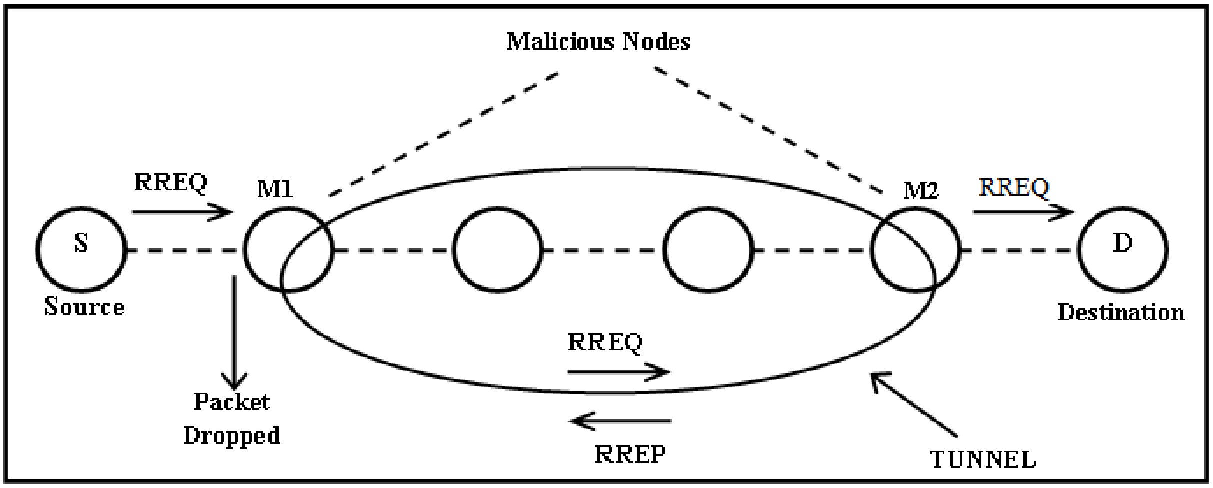


Figure 3.1: Malicious node construction between M1 and M2.

a link that has fewest number of hops and the destination is near but in reality they are far. As illustrated in Figure 3.1, the routing path is S, M1, M2, and D to form an out-of-band attack. Therefore, it requires high transmission mode and long range wireless transmission compared to legitimate node [38], [39] and [40] that will enable the malicious node node to construct a direct tunnel between pairs of malicious nodes located away from one another. Thus, the network performance will be disrupted and packets dropped, once the adversary take control over a large amount of packets that passing through the malicious node tunnel.

3.6 Hybrid malicious node Detection Algorithm

The proposed algorithm is based on Hybrid Malicious Node Detection (HMND) in mobile ad-hoc network. It has been introduced a Neighbour Ratio Threshold (NRT) to avert performing malicious node checking in all available nodes. Then, the detection algorithm will be employed to combine various detection methods. The proposed algorithm procedures are.

Step 1: Employ a technique called Neighbour Ratio Threshold (NRT) to minimize the number of nodes needed to be detected.

Step 2: After that, determine whether the neighbouring nodes lay in the transmission range of the source or not. If it is outside range of the source, then classify it as out-of-band malicious node. Otherwise move to step 3.

Step 3: Finally, employ round trip time based on its hop count and packet delivery ratio to determine the in-band attack in case of the neighbouring nodes are in the transmission range of the source.

A. Assumptions

In this section, some assumptions are presented regarding network and opponent capabilities in the proposed design in WSN.

Assumption 1: It was assumed that, two nodes are considered neighbours if the distance between them is within the transmission range.

Assumption 2: In the proposed model, the nodes start with the same energy level and have a random speed and mobility direction.

Assumption 3: The malicious nodes can launch many kinds of malicious node.

Assumption 4: All mobile nodes are randomly distributed in 2-dementional square network.

B. Neighbour Ratio Threshold (NRT)

One of the most energy consuming methods as well as increasing delay for nodes in the network is the process of checking whether every single node was affected by a malicious node or not. Generally, the malicious node does not attack all the nodes in a wireless network. Malicious node increases the number of neighbour nodes which causes inaccurate RTT and increases the connectivity of the network. Therefore, a simple effective technique has been used that is called Neighbour Ratio Threshold (NRT). It will compare the neighbour number of a node with all its neighbours to avoid launching the malicious node detection on all nodes in WSN. After neighbour discovery processes, the nodes will know their neighbours. Then, the node calculates the ratio of its neighbour number and the average neighbour number (sN_i) of all its neighbours, named the neighbour ratio. Then, the Neighbour Ratio (NRT_i) will be compared with the Neighbour Ratio Threshold (NRT) to determine whether malicious node detection is needed or not as illustrated below in algorithm 1, where the entire network E contain nodes N and their neighbours set S.

Algorithm 1 Neighbor Ratio Threshold(NRT).

```
Start
for each node $n_i$ in N and its neighbor set $S_i$ in S do
        Let $s_i = |S_i|$(which is the neighbor number of $n_j$);
        for each node $n_j$€$S_i$ do
          $s_j = |S_j|$(which is the neighbor number of $n_j$);
          Set a=0;
            $a = a + s_j$;
         To find the average neighbor number of $n_j$'s neighbors, Then $si = \frac{a}{si}$
         To Find the $n_i$'s neighbor ratio $NRT_i = \frac{si}{si}$
         if $NRT_i > NRT$ then
            put ni to suspected nodes set A area;
          end
End of Pseudocode.
```

3.6.1 Out-of-band malicious node detection

1) Transmission Range Phase

To illustrate this phase of the proposed algorithm, it's important to identify the nodes within its communication range for each network nodes. This phase relies on the transmission time between every two successive nodes to conclude the transmission range of every node. The nodes that are not in range of the source node will be considered as malicious nodes, due to limited radio coverage and the distribution of the legitimate nodes which are closer to one another. Thus, if the link between the nodes has a high transmission time, it would be classified as an out-of-band malicious node. Transmission time between nodes are proposed and calculated to the out-of-band attack.

Algorithm 2 Out-of-Band Detection Algorithm

Input: Transmission Time(TT) value, threshold value.

Output: out-of-band detected.

```
Start
Nodes are deployed using AOMDV protocol
Calculate the transmission time for each node in the routing table.
 TT=Hello Packet 2 - Hello Packet
If ($TT < threshold$) then
  Neighboring node in the range of source node
  No Out-of-band malicious node detected, go to algorithm 4
else
    Out of band detected
  End of Pseudocode.
```

3.6.2 In-band malicious node detection

1) RTT phase

This phase relied on the RTT value based on its hop count. RTT is the amount of time in milliseconds (ms) between the source nodes sending the request and receiving a response message from the destination node. This phase based on the fact that the RTT value between two fake neighbours is considered as a higher value compared to two real neighbours. Time Threshold is proposed to compare it with the expected time (RTT) of a particular node taking into consideration number of hops. Therefore, when the RTT of that node is lower than time threshold, then the node will be assessed and placed in the trusted list and no malicious node exists in that link. However, when the RTT value for that node is higher than time threshold, then a malicious node link is exist.

2) PDR Phase

Third Phase, where all nodes that reach this phase will be examined by their Packet Delivery Ratio (PDR). The nodes that are in the suspicious list will be checked by PDR detection and compare their PDR with the threshold value that is calculated using K-means clustering algorithm as illustrated in (3). The algorithm processes the input one at a time and tries all possible values of the PDR from 0-1, maintaining these results in their hidden units that implicitly contains information about the history of all the past PDR results. The centroid value (output) of the hidden units is the threshold of the PDR which will be compare with the PDR of the each node. If it's less than the threshold value, a malicious node is detected in this route. Otherwise that node is considered a trusted node and no malicious node exists However, three phases manage to increase the efficiency and performance of malicious node detection. Each phase achieve a particular form of detection resulting in having the potential to detect malicious nodes. The in-band detection algorithm illustrated parameters. The performance metrics considered to evaluate the proposed algorithms analysing performance are throughput, end to end delay, packet delivery ratio, and consumed energy. Moreover, the simulation was carried out under various number of mobile nodes to ensure and prove the efficiency of the proposed approach Hybrid Malicious Node Detection (HMND) in wireless sensor network.

Algorithm 3 PDR threshold value using K-Means algorithm

```
Run NS2 simulation.
Gather the mobility, trace file and result file that resulted from the previous simulation.
Run K-Means Clustering Algorithm
    Cluster the input file for each node to be run as one element
        Else
    The algorithm try all possible values for PDR for Node A
    For all results for Node A:
      Select PDR with the best result
The previous step done for all nodes
Now the optimal PRD for each node is ready
PDR for all nodes process to find the average optimal PDR for the network
End of Pseudocode.
```

Algorithm 4 In-Band Malicious Node Detection Algorithm

Input: RTT threshold, PDR threshold (Centroid), number of hops.

Output: in-band detected.

```
Start
Nodes are deployed using AOMDV protocol
Start
If ($RTT > threshold$) then
  Add node to the suspicious list
  Start
    If ($PDR >= threshold$) then
      No malicious node detected
    else
       In-Band malicious attack
 else
 No malicious node detected, add to the trusted list
 End of Pseudocode.
```

Chapter 4

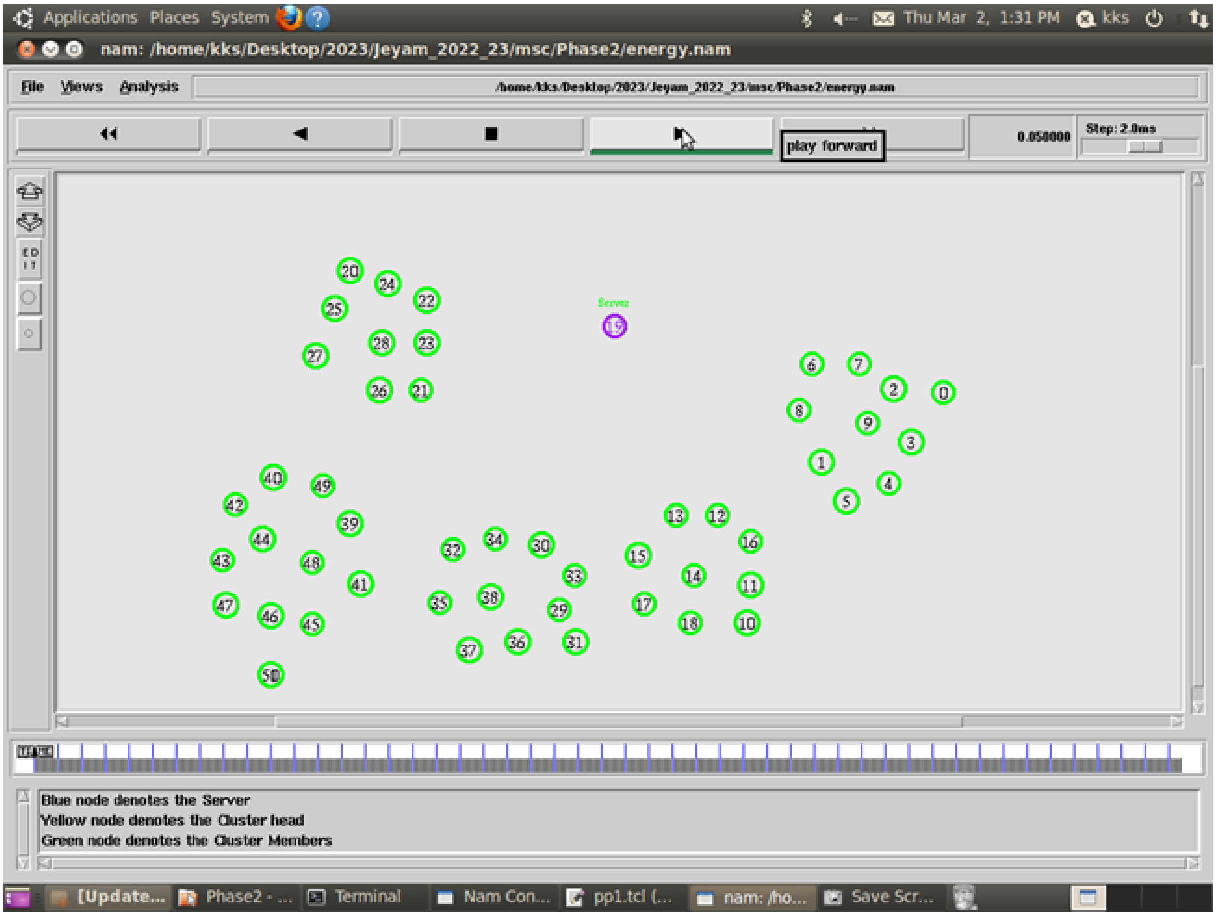
Result and Discussion

4.1 Results and Discussion

Using NS2 software, the nodes are to be created. NS2 consists mainly of two languages, C++ and Otcl. Each of these two languages has its own strengths and weaknesses. NS2 beautifully integrates these two languages to draw out their strengths. For most of the time, you would not need to know the integration mechanism. However, in order to properly apply these two languages, first need to understand their strengths and weaknesses.

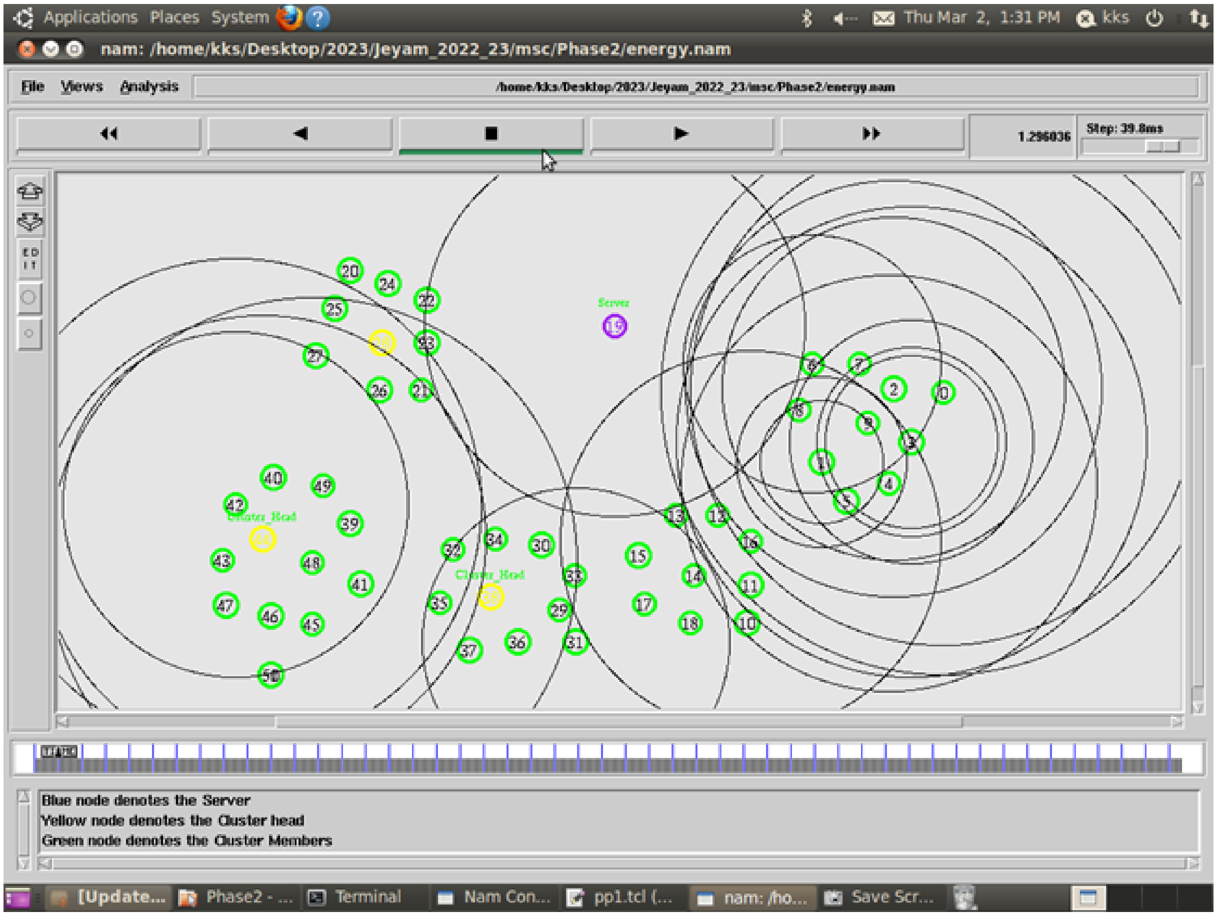
C++: C++ is a compiled programming language. A C++ program needs to be compiled (i.e., translated) into the executable machine code. Since the executable is in the form of machine code, C++ program is very fast to run. However, the compilation process can be quite annoying.

Otcl: Object-oriented Tool Command Language (Otcl) is an interpreted programming language. An Otcl program can run on the fly without the need for compilation. Upon execution, the interpreter translates Otcl instructions to machine code understandable to the operating system line by line. Therefore, Otcl codes run more slowly than C++ codes do. The upside of Otcl codes is that every change takes effect immediately.



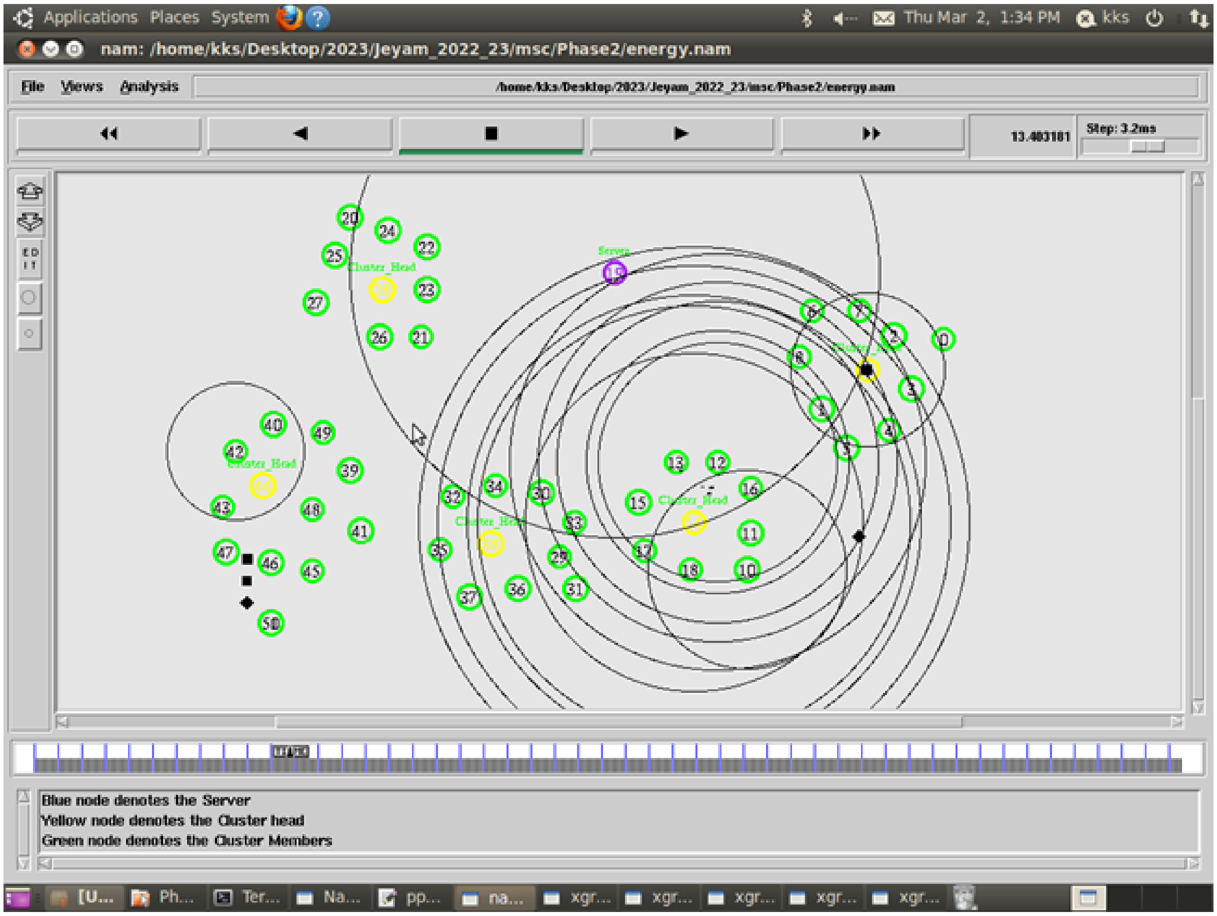
Blue node denotes the Server
Yellow node denotes the Cluster head
Green node denotes the Cluster Members

Figure 4.1: Node creation


Applications Places System
Thu Mar 2, 1:31 PM kks
nam: /home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
File Views Analysis
/home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
1.296036
Step: 39.8ms
Server
Cluster_Head
Cluster_Head
[Update... Phase2 - ... Terminal Nam Con... pp1.tcl (... nam: /ho... Save Scr...

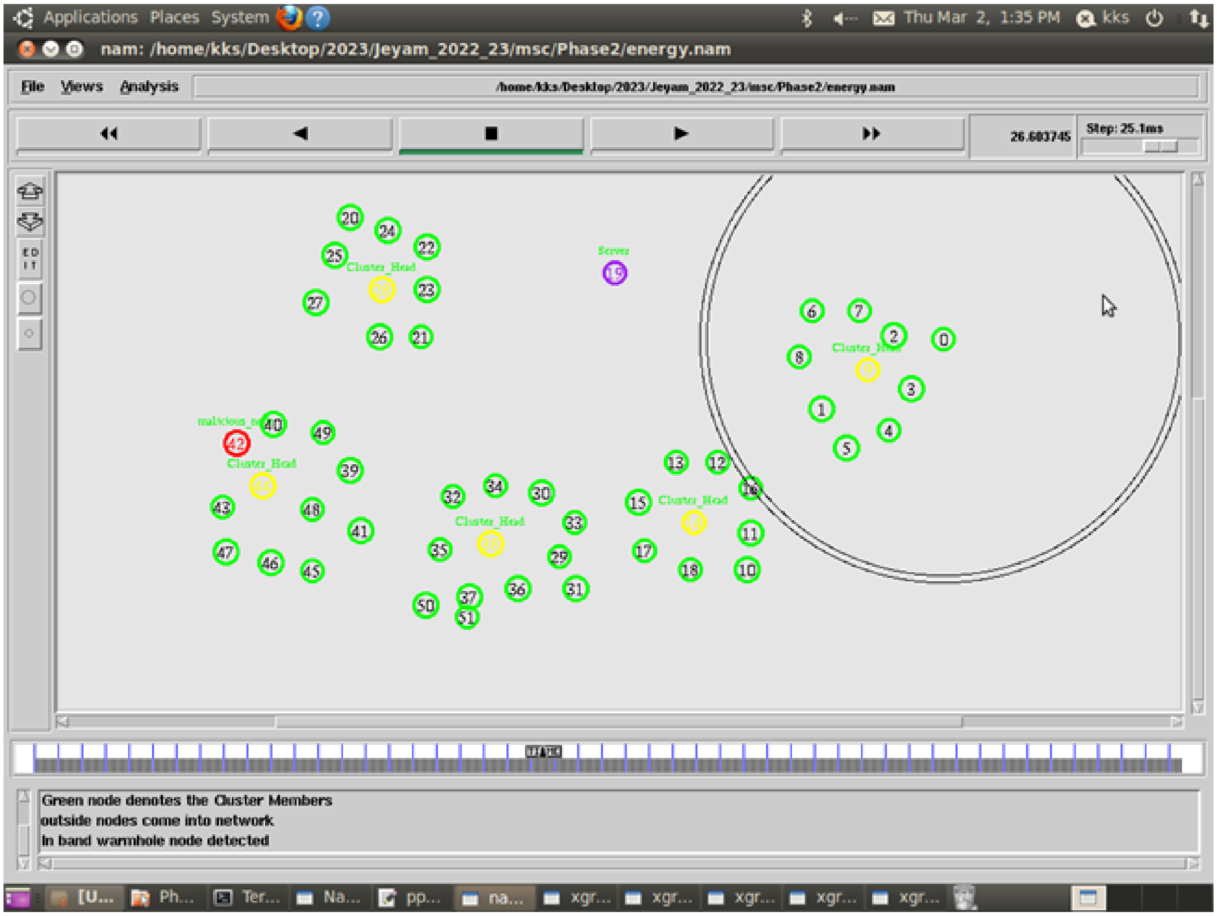
Blue node denotes the Server
Yellow node denotes the Cluster head
Green node denotes the Cluster Members

Figure 4.2: Packet Transmission


Applications Places System
Thu Mar 2, 1:34 PM kks
nam: /home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
File Views Analysis
/home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
13.403181
Step: 3.2ms
Server
Cluster_Head
Cluster_Head
Cluster_Head
Cluster_Head
Cluster_Head
[U... Ph... Ter... Na... pp... na... xgr... xgr... xgr... xgr... xgr...

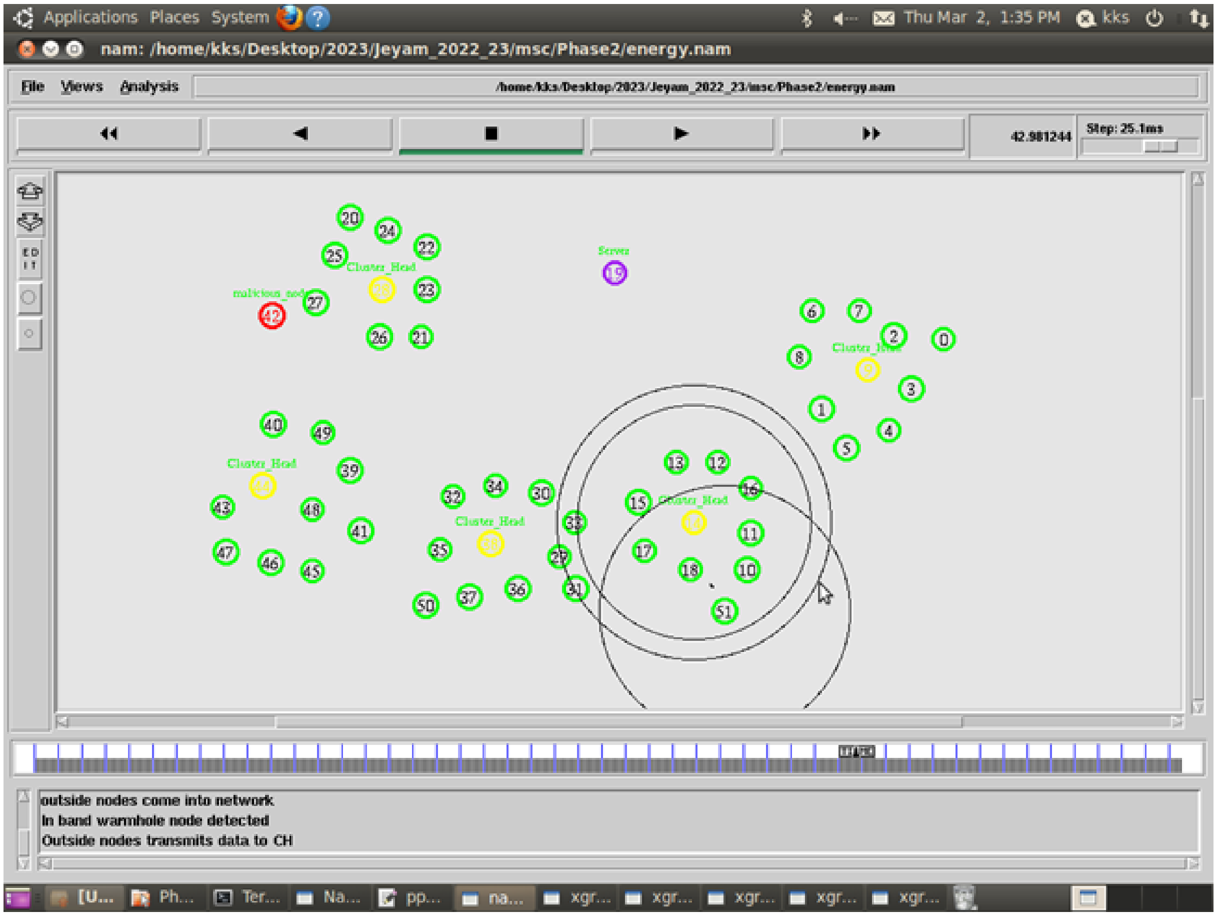
Blue node denotes the Server
Yellow node denotes the Cluster head
Green node denotes the Cluster Members

Figure 4.3: Packet loss


Applications Places System
Thu Mar 2, 1:35 PM kks
nam: /home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
File Views Analysis
/home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
26.603745
Step: 25.1ms
Server
Cluster_Head
malicious_n
20
24
22
25
23
27
26
21
6
7
2
0
8
3
1
4
5
40
42
49
39
43
48
41
47
46
45
32
34
30
33
35
29
36
31
37
50
51
13
12
16
15
11
17
18
10
[U... Ph... Ter... Na... pp... na... xgr... xgr... xgr... xgr... xgr...

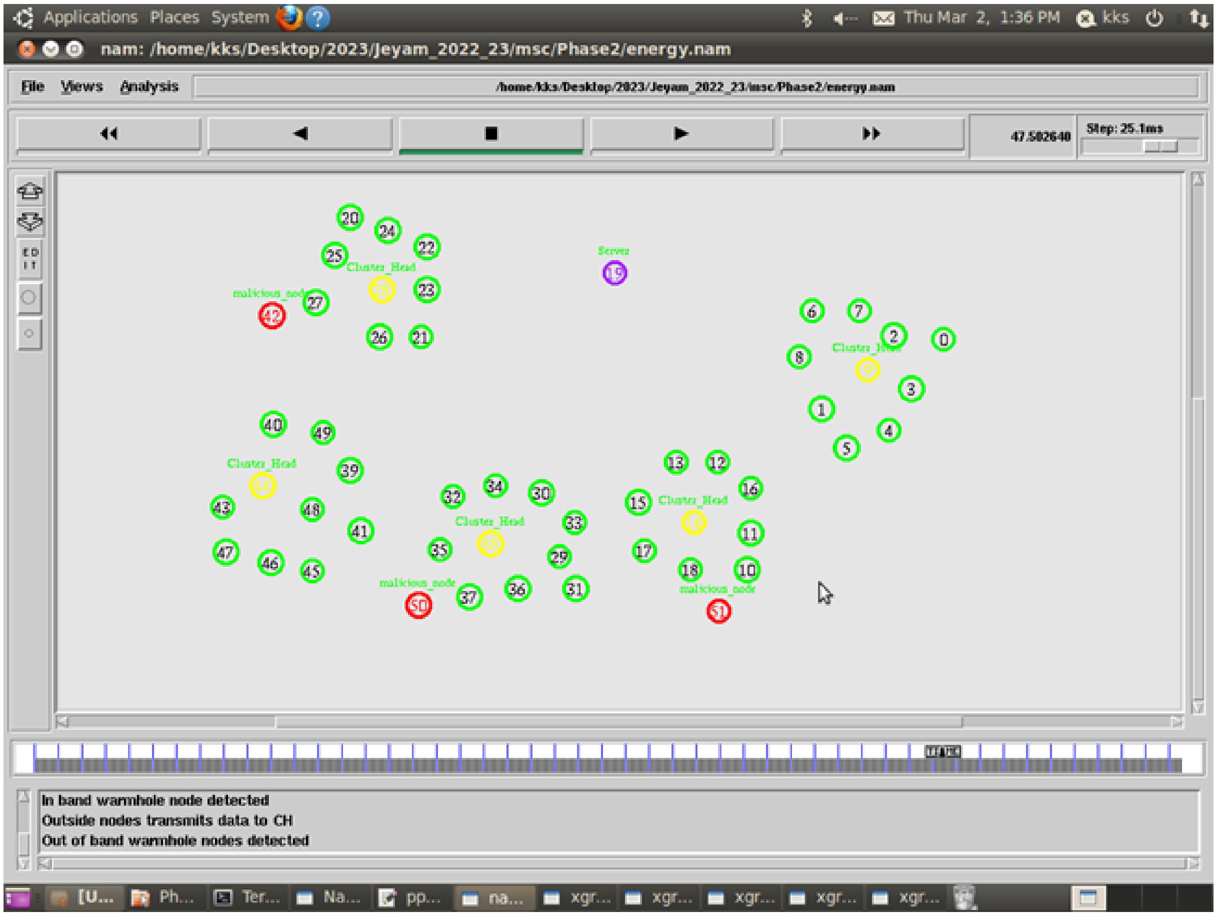
```
Green node denotes the Cluster Members
outside nodes come into network
In band warmhole node detected
```

Figure 4.4: In-band Malicious Node Detection


Applications Places System
Thu Mar 2, 1:35 PM
kks
nam: /home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
File
Views
Analysis
/home/kks/Desktop/2023/Jeyam_2022_23/msc/Phase2/energy.nam
42.981244
Step: 25.1ms
Server
Cluster_Head
malicious_node
Cluster_Head
Cluster_Head
Cluster_Head
Cluster_Head

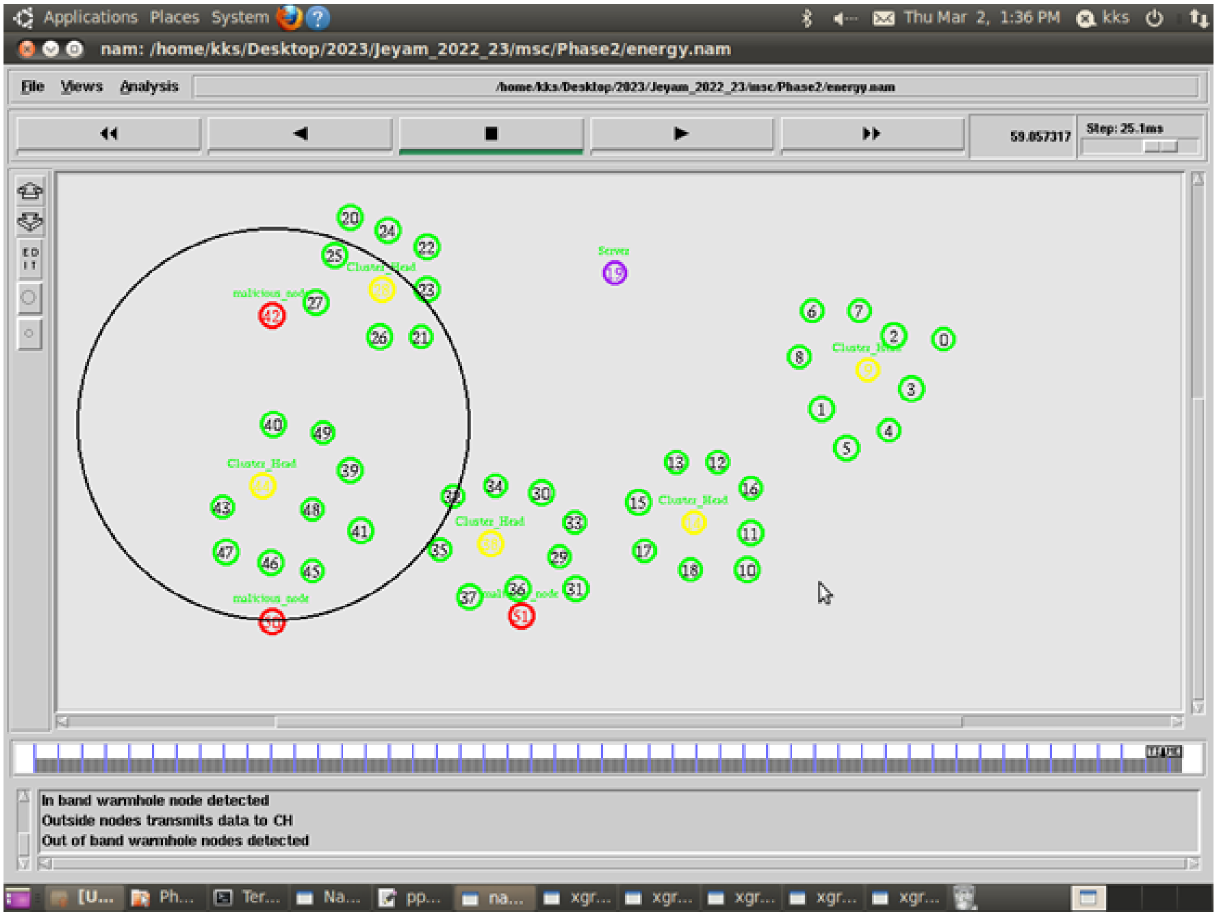
outside nodes come into network
In band warmhole node detected
Outside nodes transmits data to CH

Figure 4.5: Remove the Malicious node from network



```
In band warmhole node detected
Outside nodes transmits data to CH
Out of band warmhole nodes detected
```

Figure 4.6: Out of band Malicious detection



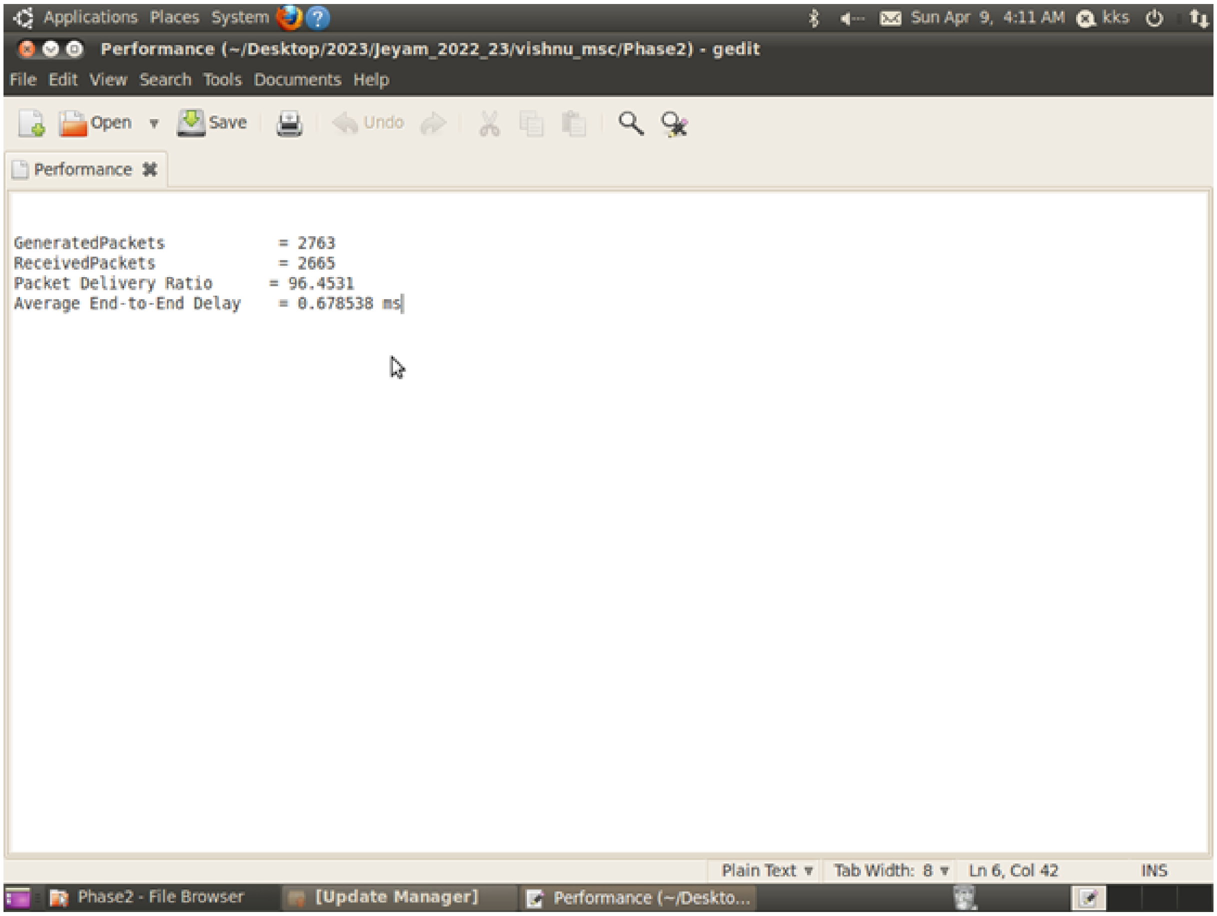
```
In band warmhole node detected
Outside nodes transmits data to CH
Out of band warmhole nodes detected
```

Figure 4.7: Malicious node Removal

4.2 Performance Analysis

A. PDR

In order to evaluate the efficiency of the proposed approach HMND, we compared its performance with some other well-known malicious node detection approach such as LNCA using number of nodes metrics. In the all figures below, the x-axis represents the number of nodes and the y-axis represents the metrics with different network scenarios. PDR in HMND compared with our existing algorithm with various number of nodes. This plot shows the rate of successfully packet received by destination. The PDR values in HMND are in below figure. The reason behind that the LNCA algorithm based on neighboring information where malicious nodes can fabricate their neighborhood list to manipulate the detection method. Also, the detection will be hard if the tunnel is less than four hops. While the throughput in HMND remain highest even with different network size. Therefore, HMND can provide higher performance, quality and successful PDR to the destination compared to the LNCA.



```
GeneratedPackets           = 2763
ReceivedPackets            = 2665
Packet Delivery Ratio     = 96.4531
Average End-to-End Delay   = 0.678538 ms
```

Figure 4.8: PDR And Delay Calculationl

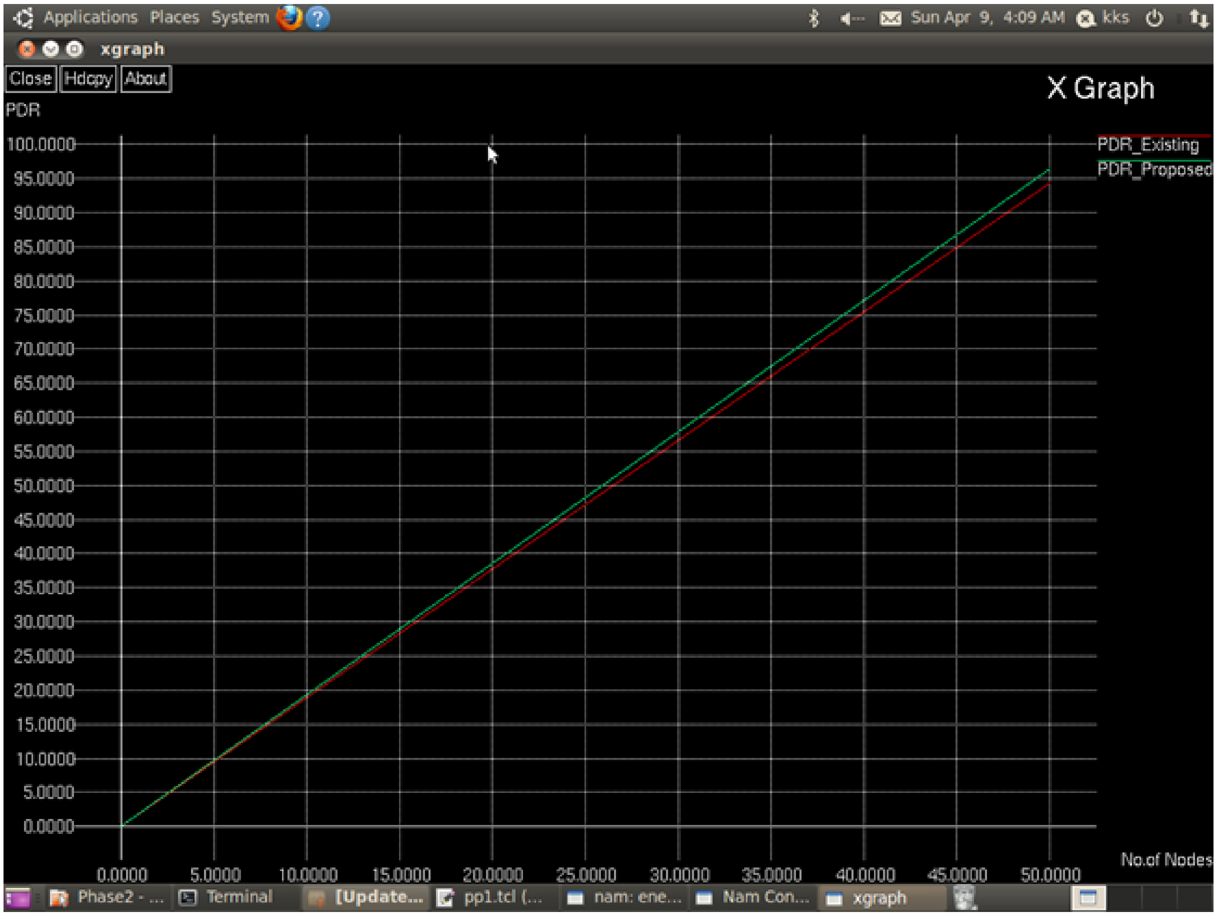


Figure 4.9: Malicious node Removal

B. End to End Delay

Figure 4.13 presents the packet delay that plays an important role for measuring the network performance. Since minimum delay ensure the quality and performance of transmission. The delay values for HMND in below above Figure 4.11 respectively. In Figure 4.13, the plots show the highest delay in LNCA at various network density. This is because LNCA perform two stages of checking between neighbours in the elected path to check whether there is a three hops path to nodes. However, when the network density increase, the HMND remain with smallest delay compared LNCA that has negatively impacted performance. It is very clear that the HMND will ensure the packet can be transmitted in a safe path and short time across the network.

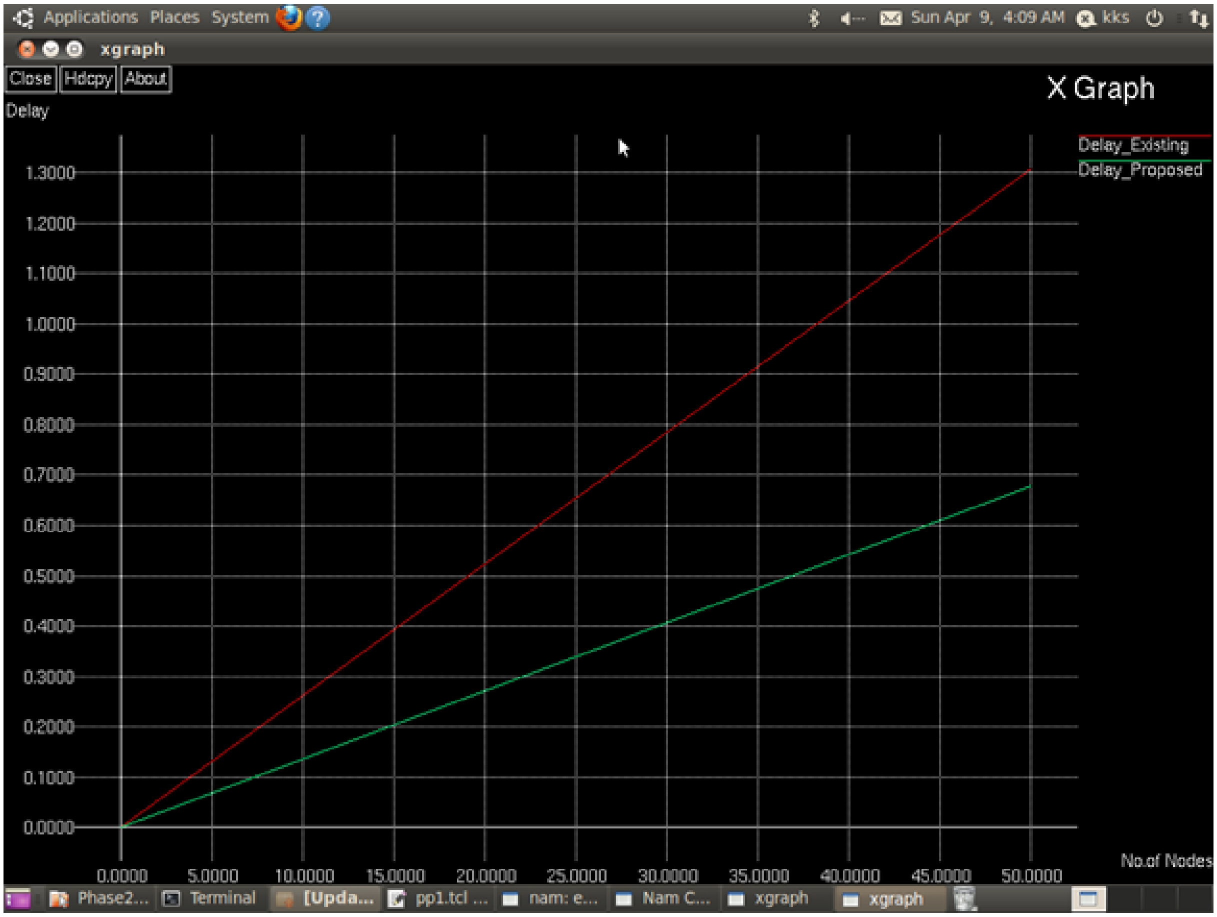
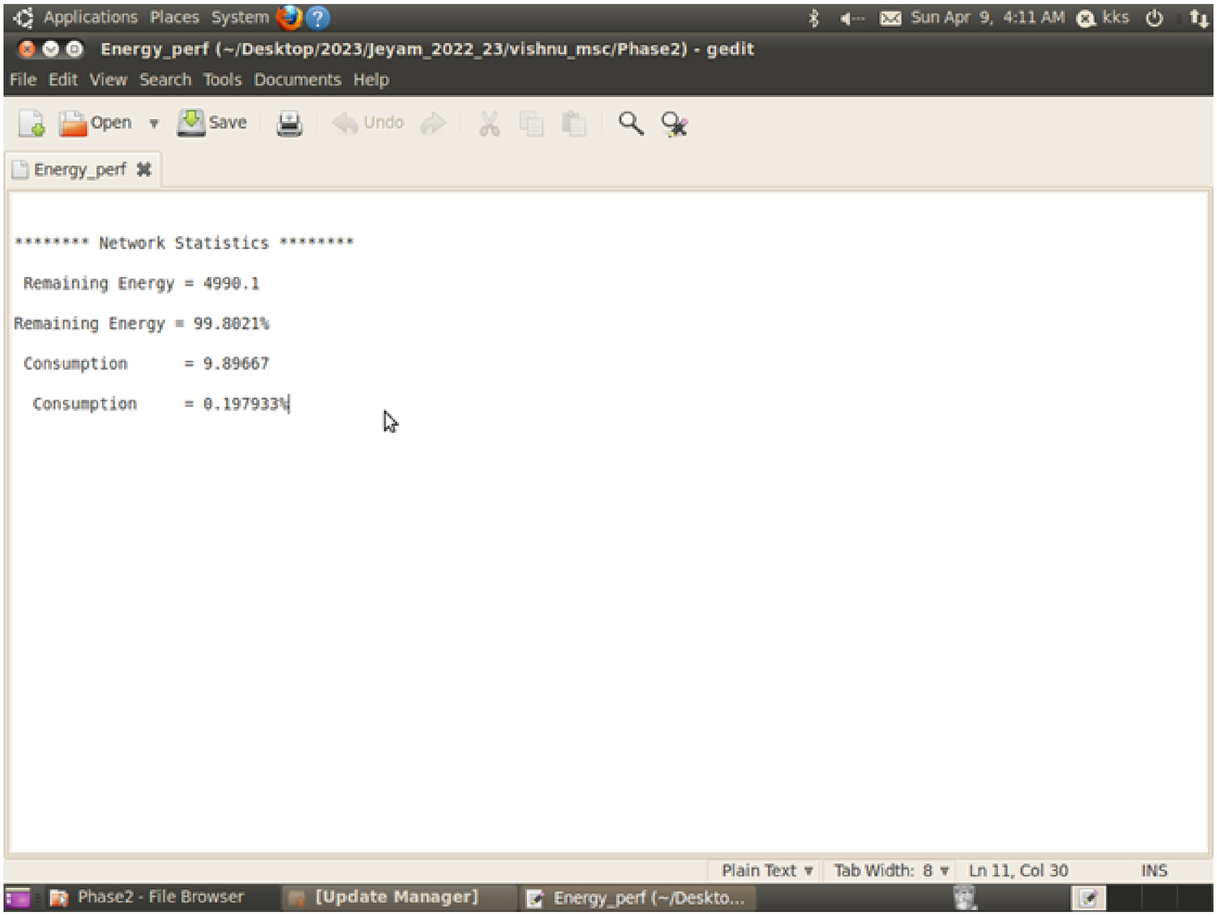


Figure 4.10: Delay Comparison

C.Energy Consumption

Figure 4.15 shows the comparison in amount of energy consumption required from the HMND and LNCA between number of nodes. The below figure describe that HMND consumes energy respectively and for LNCA. Where energy consumption in HMND within the normal range and is considered less than LNCA when the network under attack. LNCA consume additional energy. The reason behind that is the second stage of checking that is require discovering additional neighbours two hops away from the following neighbor to the intersection with source within 3 hops. HMND employ (NRT) which will decrease the amount of energy consumed in the network.



```
******** Network Statistics ********
 Remaining Energy = 4990.1
Remaining Energy = 99.8021%
 Consumption      = 9.89667
  Consumption     = 0.197933%
```

Figure 4.11: Energy Analysis

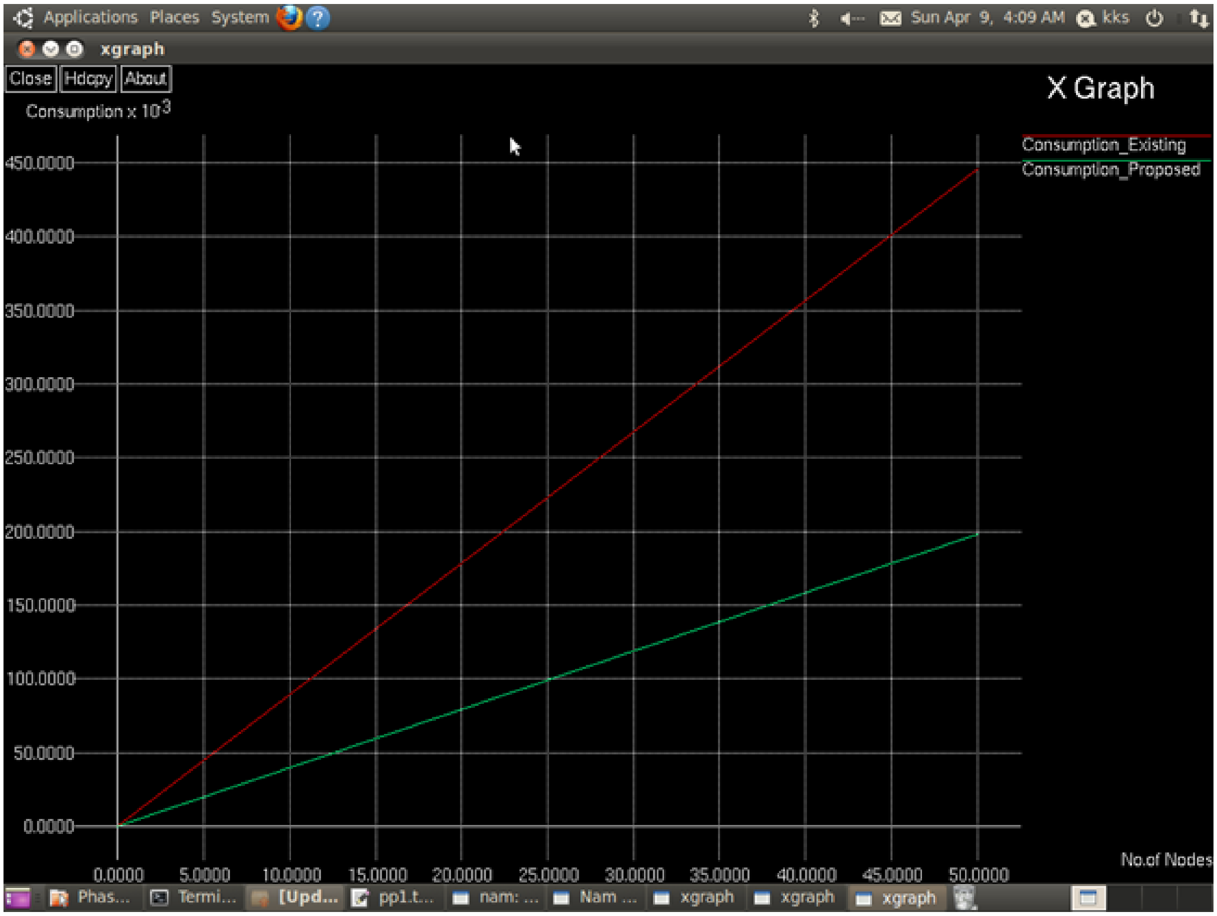


Figure 4.12: Consumption Comparison

D. Energy Efficiency

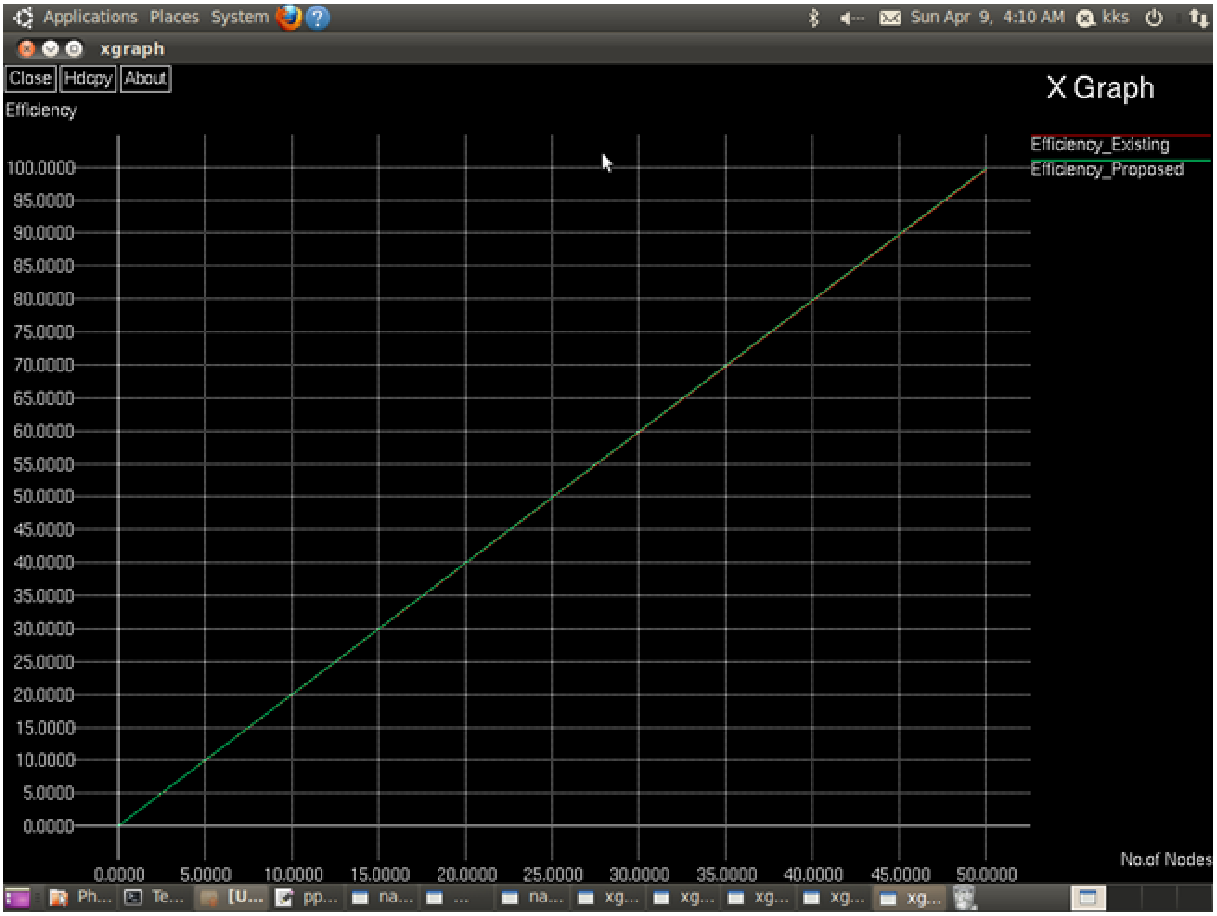
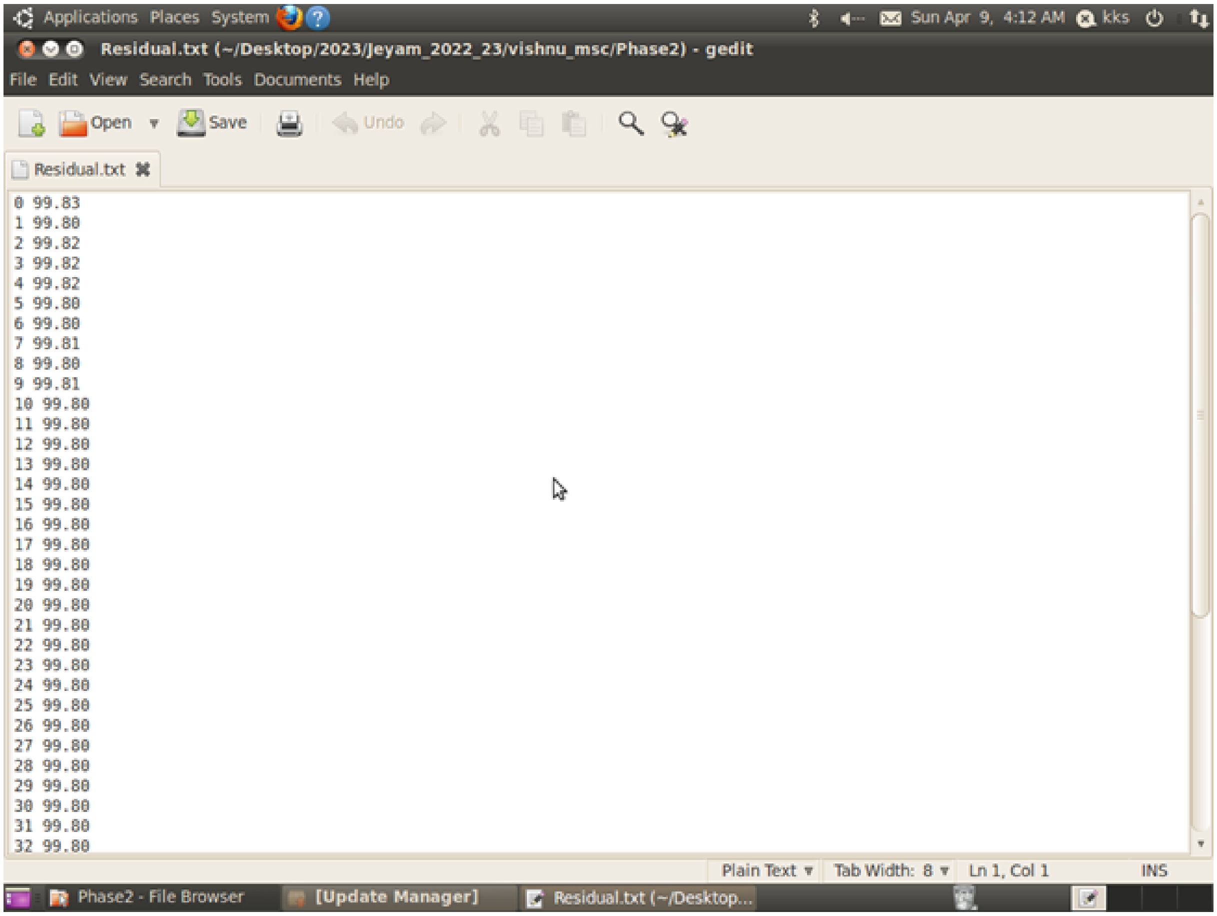


Figure 4.13: Energy Efficiency Comparison


Applications Places System
Sun Apr 9, 4:12 AM kks
Residual.txt (~/Desktop/2023/Jeyam_2022_23/vishnu_msc/Phase2) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Residual.txt
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
Phase2 - File Browser
[Update Manager]
Residual.txt (~/Desktop...

```
0 99.83
1 99.80
2 99.82
3 99.82
4 99.82
5 99.80
6 99.80
7 99.81
8 99.80
9 99.81
10 99.80
11 99.80
12 99.80
13 99.80
14 99.80
15 99.80
16 99.80
17 99.80
18 99.80
19 99.80
20 99.80
21 99.80
22 99.80
23 99.80
24 99.80
25 99.80
26 99.80
27 99.80
28 99.80
29 99.80
30 99.80
31 99.80
32 99.80
```

Figure 4.14: Residual Energy of all nodes

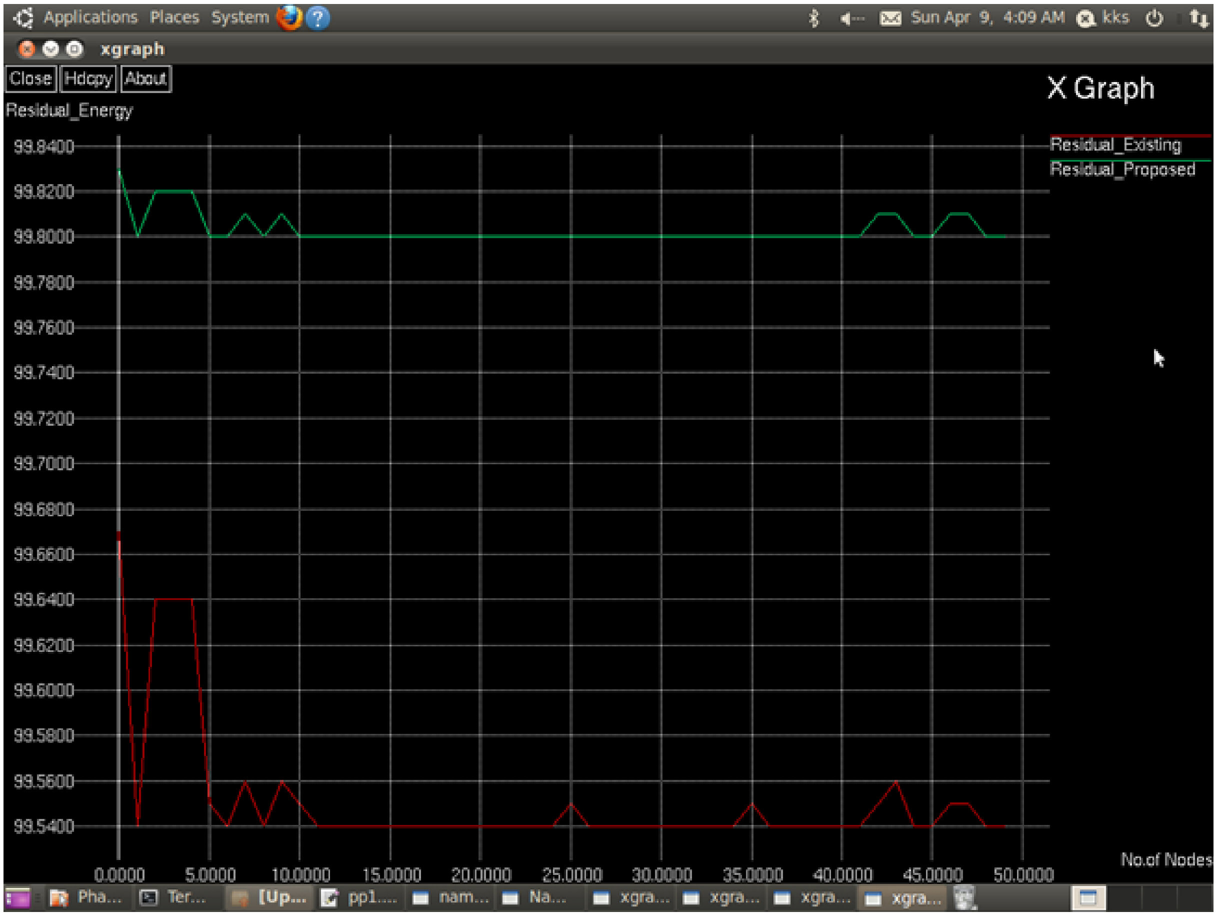


Figure 4.15: Comparison of Residual Energy

Chapter 5

Conclusion and Future Work

5.1 Conclusion

A Hybrid Malicious Node Detection (HMND) algorithm in MANET able to detect two types of malicious node, in-band malicious node using round trip time and packet delivery ratio that used K-means clustering algorithm. While out-of-band malicious node uses transmission range between successive nodes. HMND was proposed to enhance the malicious node detection for both types, in-band and out-of-band. Neighbour ratio threshold helped to lower the energy consumption and delay through reducing the number of detection nodes. This algorithm is applied on the AOMDV protocol and implemented using NS-2 simulator to measure different parameters for various number of nodes with different metrics. The simulation of the proposed algorithm outcomes have clearly proved that the proposed approach has higher performance, more effective and detection accuracy over compared algorithms in several metrics such as throughput, packet delivery ratio, end to end delay and consuming energy. HMND detection approach ensures that the malicious node is treated for both types in-band and out-of-band attack. However, the proposed algorithm in general outperformed other algorithms in a set of measured parameters.

5.2 Future Work

In the future, I will focus on using Ad-hoc network in a large size topological area which provided greater flexibility and more accurate detection performance in wireless networks. In addition, I will overcome the consuming energy due to the limited energy supply of mobile node. It is of the utmost importance to focus of study on malicious node detection, as it enables us through seeking out more possible techniques to counteract the attack in my future research, in order to apply HMND to more complex condition.

References

1. GY, P. K., & Pushpalatha, S. Detection And Prevention Of Malicious Node In Manet's Through Reliable Multipath Routing.Sep 9, 2022.

2. Singh, S., & Saini, H. S. (2022). Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN. Wireless Personal Communications, 122(2), 1305-1327.

3. Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile ad-hoc network (MANET). IEEE Access, 9, 11872-11883.

4. S. Majumder and D. Bhattacharyya, "Mitigating malicious node in MANET using absolute deviation statistical approach," in Proc. IEEE 8th Annu. Comput. Commun. Workshop Conf. (CCWC), Las Vegas, NV, USA, Jan. 2018, pp. 317320.

5. J. Seo and G. Lee, "An effective malicious node defence method for a smart meter mesh network in an intelligent power grid," Int. J. Adv. Robot. Syst., vol. 9, p. 49, Dec. 2012.

6. S. Amutha and K. Balasubramanian, "Secured energy optimized ad hoc on-

demand distance vector routing protocol," Comput. Electr. Eng., vol. 72, pp. 766773, Nov. 2018.

7. S. Rezaei, M. Gharib, and A. Movaghar, "Throughput analysis of IEEE 802.11 multi-hop wireless networks with routing consideration: A general framework," IEEE Trans. Commun., vol. 66, no. 11, pp. 54305443, Nov. 2018, doi: 10.1109/TCOMM.2018.2848905.

8. M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things against sinkhole attack using RPL protocol-based node rating and ranking mechanism," Wireless Pers. Commun., vol. 114, no. 2, pp. 12871312, Sep. 2020.

9. A. Amara korba, M. Nafaa, and S. Ghanemi, "Analysis of security attacks in AODV," in Proc. Int. Conf. Multimedia Comput. Syst. (ICMCS), Marrakech, Morocco, 2014, pp. 752756, doi: 10.1109/ICMCS. 2014.6911193.

10. R. Singh, J. Singh, and R. Singh, "WRHT: A hybrid technique for detection of malicious node in wireless sensor networks," Mobile Inf. Syst., vol. 2016, Jan. 2016, Art. no. 8354930.

11. S. R. M. Jamali; Fotohi; Analoui, "An articial immune system based method for defense against malicious node in mobile ad hoc networks," Tabriz J. Electr. Eng., vol. 47, 4, 2018, pp. 14071419

12. J. Li, D. Wang, and Y. Wang, "Security DV-hop localisation algorithm against malicious node in wireless sensor network," IET Wireless Sensor Syst., vol. 8, no.

2, pp. 6875, Apr. 2018, doi: 10.1049/iet-wss.2017.0075.

13. Z. Shi, R. Sun, R. Lu, J. Qiao, J. Chen, and X. Shen, "A malicious node resistant neighbor discovery scheme with RDMA protocol for 60 GHz directional network," IEEE Trans. Emerg. Topics Comput., vol. 1, no. 2, pp. 341352, Dec. 2013, doi: 10.1109/TETC.2013.2273220.

14. S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Multirate DelPHI to secure multirate ad hoc networks against malicious node," J. Inf. Secur. Appl., vol. 39, pp. 3140, Apr. 2018.

15. P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating malicious node on networked control systems," IEEE Trans. Autom. Control, vol. 59, no. 12, pp. 32243237, Dec. 2014, doi: 10.1109/TAC.2014.2351871.

16. R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Enhanced trust aware routing against malicious node in wireless sensor networks," in Proc. Int. Conf. Smart Sensors Appl. (ICSSA), Kuala Lumpur, Malaysia, May 2015, pp. 5659, doi: 10.1109/ICSSA.2015.7322510.

17. S. Shukla and S. Naganna, "A review on K-means data clustering approach," Int. J. Inf. Comput. Technol., vol. 4, no. 17, pp. 18471860, 2014.

18. H. Sun Chiu and K.-S. Lui, "DelPHI:Malicious node detection mechanism for ad hoc wireless networks," in Proc. 1st Int. Symp. Wireless Pervas. Com-put.,

Phuket, Thailand, 2006, p. 6, doi: 10.1109/ISWPC.2006.1613586.

19. P. Amish and V. Vaghela, “Detection And Prevention Of Malicious Node Node In Wireless Sensor Network using AOMDV protocol,” in Proc. 7th Int. Conf. Commun., Comput. Virtualization, 2016, pp. 700707.

20. Z. Tun and A. Maw, “Malicious Node Detection in Wireless Sensor Networks,” Int. J. Elect., Comput., Energetic, Electron. Commun. Eng., vol. 2, no. 10, p. 46, 2008.

21. S. Äapkun, L. Buttyán, and J.-P. Hubaux, “SECTOR: Secure tracking of node encounters in multi-hop wireless networks,” in Proc. 1st ACM workshop Secur. Ad Hoc Sensor Netw. (SASN), Washington, DC, USA, 2003, pp. 2132.

22. G.-H. Lai, “Detection of malicious node on IPv6 mobility-based wireless sensor network,” EURASIP J. Wireless Commun. Netw., vol. 2016, no. 1, p. 274, Dec. 2016.

23. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Malicious Node in Wireless Networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370380, Feb. 2006, doi: 10.1109/JSAC.2005.861394.

24. L. Hu and D. Evans, “Using directional antennas to prevent malicious node,” in Proc. Netw. Distrib. Syst. Secur. Symp., San Diego, CA, USA, Feb. 2004, pp. 241245.

25. H. Chen, W. Lou, X. Sun, and Z. Wang, “A secure localization approach against malicious node using distance consistency,” EURASIP J. Wireless Commun. Netw., vol. 2010, no. 1, Dec. 2009, Art. no. 627039, doi: 10.1155/2010/627039.

26. S. Jamali and R. Fotohi, “Defending against malicious node in MANET using an articial immune system,” New Rev. Inf. Netw., vol. 21, no. 2, pp. 79100, Jul. 2016.

27. N. Tamilarasi and S. G. Santhi, “Detection of malicious node and secure path selection in wireless sensor network,”Wireless Pers. Commun., vol. 114, pp. 329345, Sep. 2020.

28. S. Sankara Narayanan and G. Murugaboopathi, “Modied secure AODV protocol to prevent malicious node in MANET,” Concurrency Com- put., Pract. Exper., vol. 32, no. 4, Feb. 2020, Art. no. e5017, doi:10.1002/cpe.5017.

29. S. Jamali and R. Fotohi, “DAMN: Defending Against Malicious Node in MANETs by using fuzzy logic and artificial immune system,” J. Super- comput., vol. 73, no. 12, pp. 51735196, Dec. 2017.

30. A. Aswale and R. Joshi, “Security enhancement by preventing malicious node in MANET,” in Innovation in Electronics and Communication Engineerin, vol. 237. Singapore, Springer, 2020, p. 255.

31. R. Fotohi, E. Nazemi, and F. Aliee, “Anagent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks,” Veh.

Commun., vol. 26, May 2020, Art. no. 100267.

32. D. Kaur and P. Singh, “Various OSI layer attacks and countermeasure to enhance the performance of WSNs during malicious node,” ACEEE Int. J. Netw. Secur., vol. 5, no. 1, p. 62, Jan. 2014.

33. S. Ji, T. Chen, and S. Zhong, “Malicious node detection algorithms in wireless network coding systems,” IEEE Trans. Mobile Comput., vol. 14, no. 3, pp. 660674, Mar. 2015, doi: 10.1109/TMC.2014.2324572.

34. S. Gupta, S. Kar, and S. Dharmaraja, “WHOP:Malicious node detection protocol using hound packet,” in Proc. Int. Conf. Innov. Inf. Technol., Abu Dhabi, United Arab Emirates, 2011.

35. M. Okunlola, A. Siddiqui, and A. Karami, “A malicious node detection and prevention technique in wireless sensor networks,” Int. J. Comput. Appl., vol. 174, no. 4, pp. 18, Sep. 2017.

36. L. Lu, M. J. Hussain, G. Luo, and Z. Han, “Pworm: Passive and realtime Malicious node detection scheme for WSNs,” Int. J. Distrib. Sensor Netw., vol. 11, no. 11, Nov. 2015, Art. no. 356382.

37. M. Azer, S, El-Kassas, and M. El-Soudani, “Towards introducing complex malicious node in wireless ad hoc networks,” Int. J. Comput. Sci. Inf. Secur., vol. 1, no. 1, pp. 354373, May 2009.

38. S. Ali, P. Nand, and S. Tiwari, “Impact of malicious node on AODV routing protocol in vehicular ad-hoc network over real map with detection and prevention approach,” Int. J. Vehicle Inf. Commun. Syst., vol. 5, no. 3, p. 354, 2020.

39. D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, “Topological detection on Malicious nodes in wireless ad hoc and sensor networks,” IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 17871796, Dec. 2011, doi: 10.1109/ TNET.2011.2163730.

40. J. Anju and C. N. Sminesh, “An improved clustering-based approach for malicious node detection in MANET,” Int. Conf. Eco-Friendly Comput. Commun. Syst., Mangalore, Karnataka, 2014, pp. 149154, doi: 10.1109.2014.

41. S. Eidie, B. Akbari, and P. Poshtiban, “WANI:Malicious node avoidance using neighbor information,” in Proc. 7th Conf. Inf. Knowl. Technol. (IKT), Urmia, Iran, May 2015, pp. 16, doi: 10.1109/IKT.2015.7288750.

42. S. Khobragade and P. Padiya, “Detection and prevention of malicious node based on delay per hop technique for wireless mobile ad-hoc network,” in Proc. Int. Conf. Signal Process., Commun., Power Embedded Syst. (SCOPES), Paralakhemundi, Odisha, Oct. 2016, pp. 13321339, doi: 10.1109/SCOPES.2016.7955657.

43. P. Parvathi, “Comparative analysis of CBRP, AODV, DSDV routing protocols in mobile Ad-hoc networks,” in Proc. Int. Conf. Comput., Commun. Appl., Dindigul, India, vol. 2012, pp. 14, doi: 10.1109/ ICCCA.2012.6179145.

44. A. M. El-Semary and H. Diab, “BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map,” IEEE Access, vol. 7, pp. 9519795211, 2019, doi: 10.1109/ACCESS.2019.2928804.

45. J. Qi, Y. Yu, L. Wang, and J. Liu, “K-means: An effective and efficient K-means clustering algorithm,” in Proc. IEEE Int. Conferences Big Data Cloud Comput. (BDCloud), Atlanta, GA, USA, Oct. 2016, pp. 242249, doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.46.

46. N. Dhaachandra, K. Manglem, and Y. Chanu, “Image segmentation using K-means clustering algorithm and subtractive clustering algorithm,” in Proc. Int. Multi-Conf. Inf. Process., 2015, pp. 764771.

47. C. Yuan and H. Yang, “Research on K-value selection method of K-means clustering algorithm,” Sci. J., vol. 2, no. 2, pp. 226235, Jun. 2019, doi: 10.3390/j2020016.

48. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: A defense against malicious node in wireless networks,” in Proc. 23nd Annu. Joint Conf. Comput. Commun. Soc., San Francisco, CA, USA, 2003, pp. 19761986, doi: 10.1109/INFCOM.2003.1209219.

49. O. R. Ahutu and H. El-Ocla, “Centralized routing protocol for detecting malicious node in wireless sensor networks,” IEEE Access, vol. 8, pp. 6327063282, 2020, doi: 10.1109/ACCESS.2020.2983438.

50. W. A. Aliady and S. A. Al-Ahmadi, “Energy preserving secure measure against

malicious node in wireless sensor networks," IEEE Access, vol. 7, pp. 8413284141, 2019, doi: 10.1109/ACCESS.2019.2924283.