IMPROVED N2N TRUST BASED MECHANISM TO MITIGATE THE EFFECT OF WORMHOLE IN DYNAMIC SOURCE ROUTING PROTOCOL

[1]NISHA SHARMA, [2]MUKESH KUMAR GUPTA, [3]DURGA PRASAD SHARMA, [4]M. K. BANERJEE

[1] Department of Computer Science & Engineering, Suresh Gyan Vihar University Jaipur, India.
[2] Department of Electrical Engineering, Suresh Gyan Vihar University Jaipur, India.
[3]Dean Research, RTU Research Centre at MAISM & International Consultant (IT) ILO U.N., Geneva
[4]Research and Development, Suresh Gyan Vihar University Jaipur, India.

E-mail: [1]sharma_nisha2005@rediffmail.com, [2]mkgupta72@gmail.com, [3]dp.shiv08@gmail.com, [4]mkbanerjee@hotmail.com

ABSTRACT

The Wireless Ad-hoc network or Mobile Ad-Hoc network is multi-hop network and rely on dynamic infrastructure where nodes are generally mobile and require signal as a communication component. Mobile Ad-Hoc Network (MANET) is growing more popular due to its advantages of being adaptable, quick to set up, cost-effective, and durable. On the other hand, it has limitations like limited wireless range, frequently changing routes, packet drop, heterogeneous devices, and limited battery power. Hence, MANET is vulnerable to various types of security attacks unlike the infrastructure-based wired network. One of the most dangerous attack is wormhole attack which causes major impact on routing. In view of the necessity to provide secure routing, identification of malicious node is not enough, isolation of malicious node is necessary without considerable overheads in MANETs. This research work presents Node to Node (N2N) Trust based mechanism for secure routing in MANETs based on Node-to-Node packet delay. It uses aggregated N2N trust to detect source malicious node of wormhole and isolate the malicious node to ensure that the malicious node does not intercept the routing. Thus, the mechanism offers routing of data traffic securely with improved throughput. In this work, we have employed NS3 (Network Simulator-3) simulator for experimental analysis and (Dynamic Source Routing) DSR protocol as reference for implementation of N2N Trust based algorithm.

Keywords: *Wormhole, Trust Based, DSR, MANET, Packet Delay, Accuracy, Innovation.*

1. INTRODUCTION

The MANET is multi-hop network with no infrastructure where nodes are generally mobile and require signal as a communication component. A pure ad-hoc network has neither a centralized administrator nor a pre-defined infrastructure to guide the communication among nodes. For communication, the nodes use multi-hop strategy to communicate with the nodes which are not in their transmission range and nodes have to act both as router and host. MANET is highly demanding, because it is flexible, cost effective, and robust and connection establishment in less time [1]. On the other hand, these characteristics of MANET make it vulnerable to launch a different kind of attack and the Wormhole attack is assumed to be the most dangerous attack. A wormhole attack can be launched in 2 phases: first is tunnel establishment and second is tunnel exploitation. In first phase two or more malevolent nodes conspire to establish a tunnel. This tunnel is not harmful by itself; instead, it improves the throughput of the network by providing a dedicated path for transferring traffic. In phase two the tunnel is exploited for various kinds of attacks like replaying, packet dropping, packet modification, routing attack, etc. In DSR the wormhole attack is generally taken place during route discovery phase since it is a source routing protocol. Once the malicious node is part of discovered route or route in cache, It can launce different kind of attacks such as dropping packets, sending route error messages etc. In literature, there is not much work done specifically on rectifying wormhole attack in DSR protocol. This leads to the need to secure routing protocols [2]. The routing protocol is considered to be secured if it can identify the malicious nodes and isolate the malicious node for a reliable route from source to destination. A trustworthy and efficient route can be discovered by using aggregated trust values of nodes and hop count. However, the challenge is to guarantee improved throughput with reduced overhead of routing procedure [3]. Wormhole attack also increases the packets drop rate and delivers confidential data to the attacker nodes compromising the security [4]. Early detection of wormhole attack is important to prevent the data loss and packet drop both and existing approaches are not capable of providing complete assurance of attack detection as well as are time consuming solutions [5]. Because an ad-hoc network has no infrastructure and is decentralized, it is difficult to detect a wormhole attack [7]. In the present scenario, many researchers have presented the wormhole attack detection solutions which are reputation-based system where nodes behavior is taken into consideration to check node's trustworthiness for future data transfer. Current solutions, rely on some unrealistic or impractical assumptions, such as that packet processing delays at each node are roughly the same, because round trip time (RTT) measurements are used. Detecting the wormhole attack malicious node is not enough, it should be detected and isolated from MANET to protect the network and devices from being attacked by the malicious node in further transactions. In this research work, we are presenting a method for removal of malicious node from the network. In the invented methodology, the malicious node is detected and isolated from the route established for MANET, also it is ensured that, the malicious node will not be entering into the new established route of the MANET thereafter.

A Node to Node (N2N) Trust based scheme was introduced, where node to node packet delay between adjacent nodes, along the route is mapped during packet transmission; based on this information trust value of each node is evaluated. Further identification of wormhole attack malicious node is done on the basis of derived trust values. The invention proposes a method which identifies the malicious node by extending the N2N trust-based algorithm [8]. After identification of the malicious node, it is isolated from the network and security from wormhole attack is ensured. Isolating the malicious node is necessary to avoid their selection in route for further transmission. For the effective and efficient wormhole attack detection solution the DSR protocol is used as a part of the invention. The paper is organized as follows; following the introduction, the survey is explaining the existing solutions implemented for securing MANET from wormhole attacks. Section 3 tells the objectives of the research work and Section 4 includes the description of proposed research methodology in detail. Section 5 is explaining the simulation and analysis of the result. Section 6 is conclusion of the implemented research.

2. RELATED WORK

This section highlights the brief review of previous works implemented to defend and eliminate the wormhole attacks in wireless ad-hoc networks.

In [14], the authors have presented the proposed protocol for detecting the wormhole attacks and protecting the dynamic route establishment from malicious nodes. The approach is secure DSR protocol with multi-rate transmission. The important consideration of the work is the variation in transmission rate based on nodes with different capabilities, energy and wireless conditions and considering fixed transmission rate is the inappropriate assumption and specifically designed for DSR protocol. The limitation of this research is, assumptions are defined for data rates in wireless link.

In [15], the authors have presented the work of wormhole attack detection and eliminates the possibility of wormhole attack using the modified AODV approach. The base for this work is the performance degradation of network due to wormhole attack. The approach is identification of two neighbor hopes, if any of these found illegal, it is detection as malicious node in wormhole route and isolated immediately. The disadvantage of the model is high false positive rate and accuracy in detection.

In [19], a wormhole detection algorithm is proposed on the basis of Node-to-Node packet delay in packet transmission. In this work, the trust value for each node along the route is determined by observing the packet transactions between adjacent nodes; based on the trust value identification of source malicious node of wormhole is done. Later the trust value is further used for making routing decisions and choosing a secured route.

A technique of using sequence number to detect the wormhole attack was proposed earlier in [9]. In the proposed technique, the source node temporarily stores all route reply (RREP) packets from different nodes with their sequence numbers. Then source node (S) calculates the average of all sequence numbers and stores it. After calculating the average, it discards all reply packets if the sequence number of any node goes beyond the average value S. In this way, wormhole nodes can be excluded from the route, and only trusted nodes can communicate in the network. Moreover, author in [10] suggested a technique to detect wormhole wherein some nodes are selected as monitor nodes based on their trust values. These Monitor nodes further monitor their neighbor nodes based on their behavior of packet. Comparison and analysis of effect of the wormhole attack on DSR and AODV routing protocols is reported for the case where the wormhole tunnel count are increased in MANET. Such study and analysis due to [11], show that there is great impact of wormhole attack on DSR protocol. It has also suggested a trust-based routing algorithm for DSR in which the geometric mean of the trust values is calculated for the considerable node density in both forward and backward directions for every route from source to destination. By doing so, any node having lower trust value will be diminished from the opportunity of being involved in the route for data transmission. In [12], the author proposed a similar trust-based approach to detect the malicious and compromised node is recorded in literature. For the concerned trust-based approach, the proposed algorithm has used the physical and logical trust metrics to calculate the trust measure for the mobile node present in the MANET. Work, energy, and bandwidth are taken as the physical trust parameters whereas, the affinity, and trustworthy are considered as logical trust parameters for measuring the trustworthiness of the node present in the network. Further, it is reported that Diffie - Hellman algorithm for secrete key exchange is used for secure communication. A trust calculation-based mechanism is proposed in [13], which is seen to have used the multiple path selection method for finding the best path for routing. Few fake packets are sent to evaluate the trust of neighbor node. For increasing the security of data Elliptic curve cryptography technique is used for the encryption.

The above-mentioned solutions are based on trust and threshold values for detecting the wormhole nodes. Several forms of route or node attributes, like received signal strength indication, number of neighbors, network visualization, frequency of node appearances in routes, geographical location information, and packet latency, have been used in the literature to detect wormholes or wormhole nodes. The majority of these qualities, on the other hand, are unsuitable for examining the existence of all wormhole variants, and some are based on implausible assumptions. However, these solutions create high routing overhead and delay in the network. Additionally, some techniques have computational complexity and required extra hardware, which affects the standard routing protocol and increases the cost and delay. Although many researchers have worked for security of MANET, but the area of research in this direction seems to remain open.

3. OBJECTIVES

Following are the objectives of this research work:

3.1 To detect the wormhole attack in Mobile Adhoc Network using N2N trust mechanism.
3.2 To isolate the malicious node in wormhole attack to prevent the unauthorized data access.
3.3 To implement the time efficient wormhole attack detection system.

4. RESEARCH METHODOLOGY

This section describes the basic contextual framework for the detection and isolation of malicious node in DSR. This mechanism is featured to identify and isolate the malicious node of

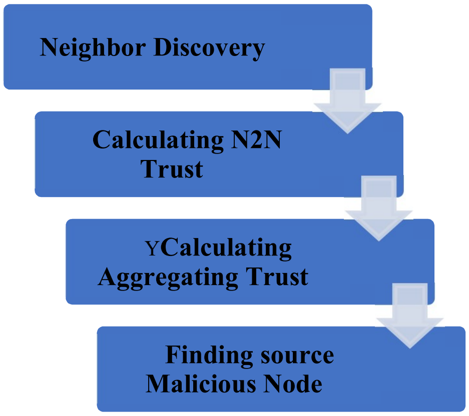

Figure 1: Block Diagram for Detection of source malicious node of wormhole attack

wormhole in MANET. The mechanism contains two phases. First phase is implemented for detection of source malicious node of wormhole attack and second phase is implemented for isolation of the source malicious node of wormhole attack.

4.1 Detection of source malicious node of wormhole attack:

The mechanism proposed in [19] identify the malicious node in the network. Identification of malicious node is not enough to provide adequate security, so, isolating the malicious node is also necessary. We are proposing the mechanism to isolate the malicious node in the network and to avoid the malicious nodes from getting chosen for further data transmission. In this paper we propose a mechanism which is extension of the N2N trust-based mechanism proposed in [8] where identification of malicious source wormhole node is performed on the basis of node-to-node packet delay during packet transmission.

In this mechanism, the packet transmission between nodes is observed, a predefined amount of time, the trust manager periodically calculates the trust values for each node. PML list against every neighboring node is also maintained and updated until the identification process is completed and resets it after completion of the identification process [8].

The mechanism for detection of source malicious node of wormhole attack in DSR is represented in form of a flow chart in Figure 2. When the source node desires to send data to some target node, first Route Discovery procedure starts, and at the same time, each node also stores its neighboring node in its Trust Table. This action is performed in the first step: Finding the neighbor node. The data transmission begins after successful establishment of route. Each node along the discovered route fills its PML column in Trust Table whenever a packet is transmitted from source to destination. It stores packet ID and Timestamp in the PML field. In the second step, the N2N Trust value is calculated based on the gathered information in the PML field of Trust Table.

Initially when no packet has been transmitted the N2N trust value will be 1 against the neighboring node. The N2N Trust value varies from 0 to 1. Trust value 1 represents the most trusted node and 0 represents the least trusted node. This process keeps going for 1 sec after that N2N trust value is calculated for each node. In step 4 aggregated trust value is calculated for the nodes that have more than one recommending node. The routing decisions are made based on the obtained trust value. The node that has a trust value near 0 is considered an untrusted node and must be avoided for further communication. As a result of step 4, we get a list of IP Addresses of untrusted nodes. To identify malicious nodes, the sequence of the list of IP Addresses of untrusted nodes is matched with listed IP Addresses of intermediate nodes of the discovered route. If the sequence matches, then it represents the existence of a wormhole and the first node in the list of nodes of discovered route sequence, will be the source of the wormhole tunnel [19].

Table 1 : Trust Table

<IP Address> Neighbor ID	**<Node to Node Trust Value> N2N Trust Value**	**{<Packet Meta List>} PML**
ID1	N2N_TV1	{{P1,T1};{{P2,T2};….{Pm,Tm}}
ID2	N2N_TV2	{{P1,T1};{{P2,T2};….{Pm,Tm}}
….	….	….
….	….	….
IDn	N2N_TVn	{{P1,T1};{{P2,T2};….{Pm,Tm}}

4.2 Isolating the malicious Node:

Detection of a malicious node is not enough; it is required to isolate the malicious node from the network to provide maximum security from the malicious node and the malicious nodes do not get involved further in any subsequent transaction. Isolating the malicious node will stop the damage from being spread as well as the malicious activities in the network. In this paper, we are presenting a method for removal of malicious node from the network. In this method we need to remove the malicious node from the existing route present in cache as well as need to stop the malicious node from being a part of new discovered route. The mechanism for isolation of source malicious node of wormhole attack in DSR is represented in form of a flow chart in Figure 3. For this a Malicious Node List (MNL) is maintained by each node in the network and follows the steps mentioned below:

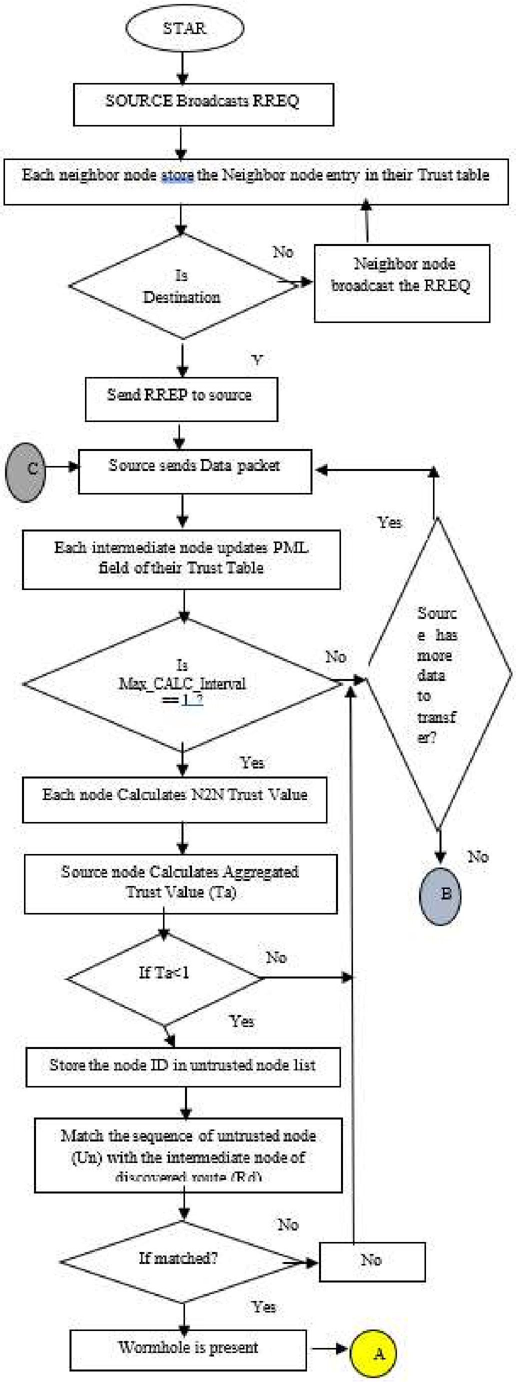
STAR
SOURCE Broadcasts RREQ
Each neighbor node store the Neighbor node entry in their Trust table
Is Destination
No
Neighbor node broadcast the RREQ
Y
Send RREP to source
C
Source sends Data packet
Yes
Each intermediate node updates PML field of their Trust Table
Is Max_CALC_Interval ==1 ?
No
Sourc e has more data to transf er?
Yes
Each node Calculates N2N Trust Value
No
B
Source node Calculates Aggregated Trust Value (Ta)
If Ta<1
No
Yes
Store the node ID in untrusted node list
Match the sequence of untrusted node (Un) with the intermediate node of discovered route (Rd)
No
If matched?
No
Yes
Wormhole is present
A

Figure 2 : Detection Of Source Malicious Node Of Wormhole Attack

- Source node removes the malicious node from its route cache.
- New discovered route should not contain the malicious node.
- All the intermediate nodes are informed about the malicious node to update their MNL list.
- Rejection of Route Request or Route Reply initiated by malicious node.

Each node creates an MNL list. After the source node identifies the malicious node, it removes the route entries from the route cache having the malicious node involved in it and stores the malicious node in MNL.

In case the source node needs a new route for the transaction, route discovery procedure is started. Only the route containing non-malicious nodes is detected. Source node sends Malicious Node Packet (MNP) to nodes along the discovered route. The intermediate nodes update their MNL by making entry of the malicious n If any malicious node initiates a route request, a route replies the receiver node and verifies it by checking its MNL list and ignores the route request or route reply without processing it further.

Isolation Algorithm: To isolate malicious nodes and discover the non-malicious route.

1. Create a list of the malicious node (MNL – Malicious Node List).

2. Add the detected ID of the malicious node in MNL.

3. Remove the malicious route containing the malicious node from Route Cache.

4. Start Route Discovery

5. Accept Discovered route containing non-malicious nodes.

6. Send MNP (Malicious Node Packet - {Malicious node Ids}) to the intermediate nodes of discovered routes i.e. non-malicious nodes.

7. Each intermediate node updates its MNL if the node is an untrusted neighbor.

8. IF ROUTE_REQUEST arriving from malicious node THEN

REJECT ROUTE_REQUEST

ELSE

ACCEPT ROUTE_REQUEST

ENDIF

```
9. IF ROUTE_REPLY arriving from malicious node THEN
    REJECT ROUTE_REPLY
    ELSE
    ACCEPT ROUTE_REPLY
    10. ENDIF
    11. Perform steps 10 to 19 on all nodes including the source node.
    12. END
```

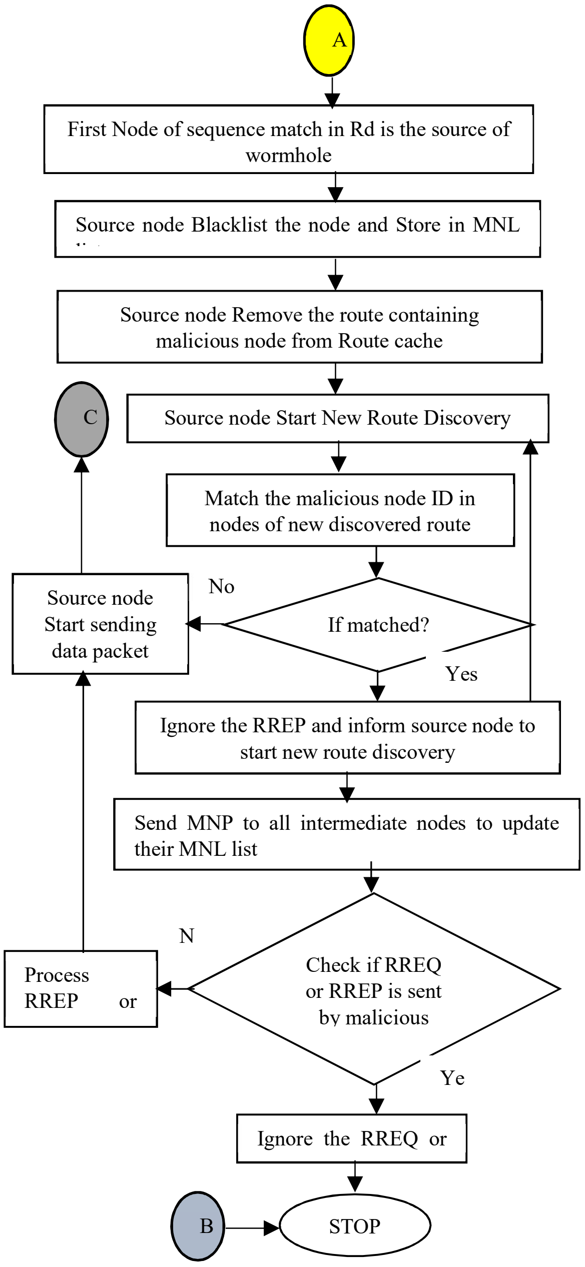
A
First Node of sequence match in Rd is the source of wormhole
Source node Blacklist the node and Store in MNL
Source node Remove the route containing malicious node from Route cache
C
Source node Start New Route Discovery
Match the malicious node ID in nodes of new discovered route
Source node Start sending data packet
No
If matched?
Yes
Ignore the RREP and inform source node to start new route discovery
Send MNP to all intermediate nodes to update their MNL list
N
Process RREP or
Check if RREQ or RREP is sent by malicious
Ye
Ignore the RREQ or
B
STOP

Figure 3 : Isolation of malicious node of wormhole in DSR

4.3. Augmentations of Proposed Mechanism with DSR

When any node desires to send a packet to a target node, the sender node broadcast RREQ (Route Request) packet to its neighboring nodes. Each neighbor node appends their IP address in the RREQ packet and again broadcasts it to its neighbors. This procedure is carried on until the intended target node receives the packet. When a node receives a RREQ it creates an entry of IP address of sender node in its Trust Table. The RREQ packet received by the target node carries the complete route to reach the target node from the source node. The destination node reverses the route and sends an RREP (Route Reply) packet back to source node via the reversed route. There may be multiple routes available from source node to target node having different set of nodes. The source node selects a route based on a hop counts or delays and starts sending packets to the target node through the selected route. The execution of proposed N2N Trust based algorithm also starts simultaneously and the trust value is calculated and updated periodically for each intermediate node through the selected route. Based on the obtained trust value, the malicious node is identified. If a wormhole exists, the proposed algorithm helps in detection and isolation of source malicious node of wormhole attack and finding the most trustworthy route to send data packets.

5. SIMULATION AND RESULTS

In this section, we discuss the tools and techniques used for evaluation of the effectiveness of the proposed method.

5.1 Simulation Environment:

The platform for simulation of proposed N2N trust-based algorithm was ubuntu Linux operating system version 16.04 LTS 64 bits. Ubuntu is an open-source operating system that can be downloaded for free from the internet. Its hardware requirements are at least core 2 duo processor, memory needed is at least 2 GHz and hard disk of at least 500 GB. Ubuntu operating system is also compatible with NS-3 simulator.

The major goal of the NS-3 software is to meet the system's requirements by first creating the software development environment's libraries, and then creating the user application program. The

Network Simulator tool is based on the notions of separate source and sink tracing and a standardized mechanism for linking sources and sinks. Use Case models are used to create NS-3 design simulations that allow the simulator to interact with the actual world **Error! Reference source not found.**. We simulate the proposed method in NS-3 simulator; DSR protocol is used as a reference. DSR is a Dynamic Source Routing protocol and perform better among all reactive routing protocols in constrained based environment **Error! Reference source not found.Error! Reference source not found.**.

A Compromised stranger node is introduced into the network which starts dropping the packet after a short while from the start of data packet transmission. The network should be able to identify these compromised nodes and should not upgrade them for communication. We are using the Random Walk 2D mobility model for node movement.

5.2 Simulation Parameters:

The proposed method is tested under different scenarios i.e., varying the CBR value and changing the value of a number of nodes in the network and vice versa. The simulation parameter chosen for each scenario are given in Table 2 and Table 3. The matrices taken into consideration, to analyze the performance of the network using proposed algorithm, are as follows:

Detection time: This is the Time taken to detect and isolate malicious node by proposed N2N trust-based mechanism. This time is measured after the route is discovered to begin data transfer also after the arrival of malicious node.

Throughput: It is the rate of successful data transfer in the ad hoc network and is measured as the ratio of the total packet received at the destination node by the total number of packets sent by the source node. Throughput is expressed in terms of bytes per second or bits per second.

$$\text{Throughput} = \frac{Totalpacketreceivedatdestination}{Totalnumberofpacketsentbysource}$$

Packet Drop (%) : It is the percent ratio of the number of packets drop or loss by the total number of packets transmitted.

$$\text{PDR} = \frac{(Totalnumberofpacketsent - Totalnumberofpacketreceived)}{Totalnumberofpacketsent} * 100\ \%$$

Execution time: This is the Time taken to execute by proposed N2N trust based mechanism. This time is measured after the route is discovered to begin data transfer [25].

In the first scenario, simulation is carried out by considering the varying value of CBR [26] from 64Kbps to 576Kbps and keeping the number of nodes in the network as 50 in the region 1200 X 1200 as shown in Table 2.

Table 2 : Simulation Parameters of Scenario 1

Parameters	Values
Protocol	DSR
Simulation Time	30 Seconds
Simulation Area	1200m x 1200m
Number of Nodes	50
Transmission Range	250
Movement Model	Random Walk 2D Model
Traffic Type	CBR (UDP)
No. of Wormholes	1
Malicious Nodes	2
CBR (Kbps)	64/128/192/256/320/384/448/512/576
Packet Size	512 bytes

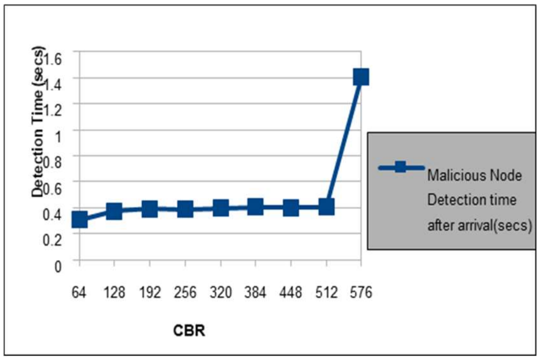

Figure 4 : Detection Time Performance: CBR Vs Detection Time

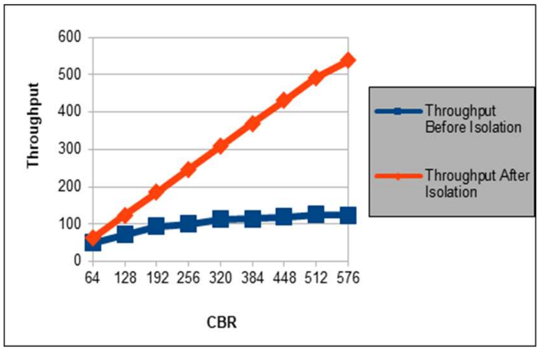

Figure 5: Throughput Performance: CBR Vs Throughput

From the result shown in Figure 4., it is clearly visible that the maximum time taken to detect the malicious node for 50 node networks is 1.4 seconds which is quite small. This time is measured after the new route is discovered.

As per the results shown in Figure 5 the average throughput before isolation is 101.74Kbps; after isolation, this is increased to 205.37Kbps and the new average throughput after isolation becomes 307.118Kbps. The average drop percent after isolation is found to be 1.746% and the overall packet dropping is reduced by 97.04% as shown in Figure 6

In the Second scenario, simulation is carried out by varying the number of nodes from 20 to 60 and keeping the value of CBR as 64Kbps in the region 1500 X 1500 as shown in the Table 3.

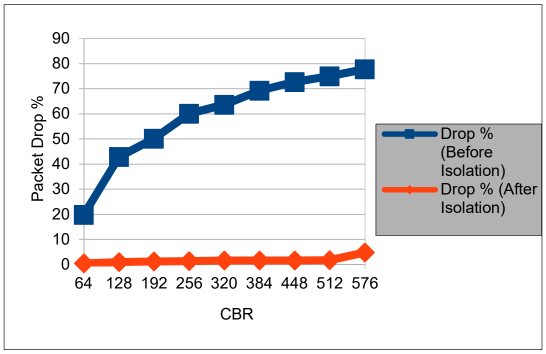

Figure 6 : Improvement in Packet Drop %: CBR Vs Packet Drop %

Table 3: Simulation Parameters of Scenario 2

Parameters	***Values***
Protocol	DSR
Simulation Time	30 Seconds
Simulation Area	1500m x 1500m
Number of Nodes	20/30/40/50/60
Transmission Range	250
Movement Model	Random Walk 2D Model
Traffic Type	CBR (UDP)
No. of Wormholes	1
Malicious Nodes	2
CBR (Kbps)	64
Packet Size	512 bytes

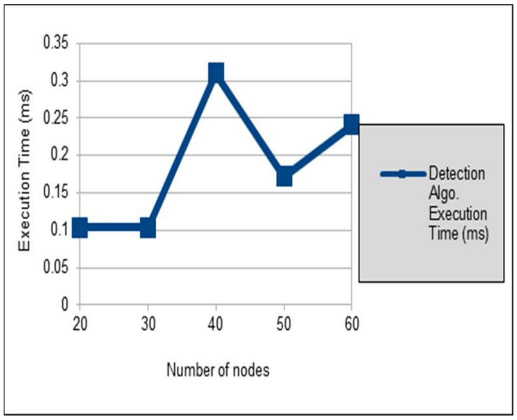

Figure 7: Execution Time Performance: Number of nodes Vs Execution Time (ms)

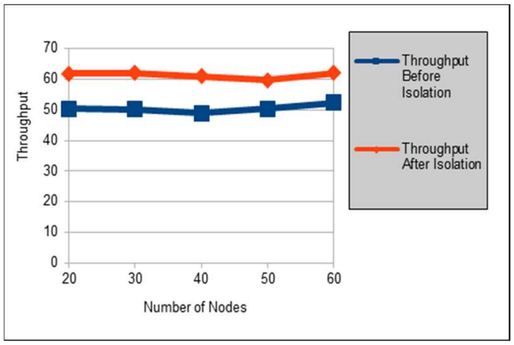

Figure 8 : Throughput Performance: Number of Nodes Vs Throughput

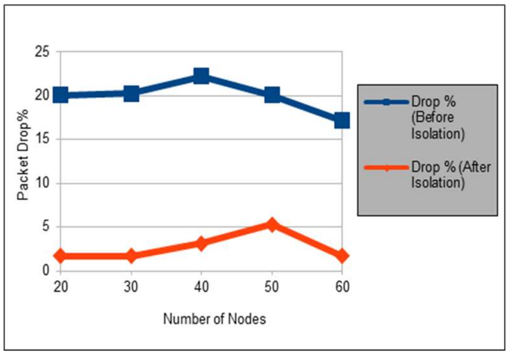

Figure 9 : Improvement in Packet Drop%: Number of Nodes Vs Packet Drop%

From the results shown in Figure 7, it can be noted that when number of nodes increases, the execution time gradually increases. But the maximum execution time taken by the proposed algorithm is 0.31 ms which is a negligible time value; this time value authenticates faster performance by the algorithm.

From the results shown in Figure 8 the average throughput before isolation is 50.467Kbps which is increased after isolation by 10.87Kbps and the new average throughput after isolation is 61.34Kbps.

Moreover, the average drop percentage after isolation is found is 2.706% and the overall packet dropping is reduced by 86.44% (Figure 9).

So, we can analyze from the results that in both the scenarios (varying CBR or varying number of node) when the value is increasing, Number of packet drop is increasing and throughput is decreasing. This is because of the fact that presence of wormhole is causing more packet drop and N2N trust-based algorithm is just detecting the presence of wormhole in the network and there is no protection from the malicious node. When the improved N2N trust-based mechanism is used that performs isolation i.e. removing the malicious node of wormhole attack will increase in throughput and decrease in number of packet drops as shown in result.

The proposed mechanism is appealing because they are effective, simple to deploy, and can be used on a wide range of network devices. From all the simulated results, it is realized that, the wormhole attack is efficiently detected and the wormhole can be isolated effectively using the N2N delivery mechanism with less packet drops and multi-rate functionality. In future work we would be comparing some of performance matrices with the other trust-based mechanism such as proposed in **Error! Reference source not found.** .

6. CONCLUSION

MANET has gained a huge popularity in deploying it at various applications at the same time it has some operational restrictions too like energy constrained, storage constrained, limited bandwidth, dynamic topology, Mobility etc. The proposed mechanism is designed considering limitation of resources in MANET in the sense that the implemented algorithm does not use any special hardware. The proposed extended N2N Trust-based algorithm is capable of successfully identifying the source malicious node of wormhole in the network in the DSR protocol. Moreover, it can isolate the malicious node from being involved in further communication.

The results show that the use of the proposed improved N2N Trust Based algorithm considerably reduces the overall Packet dropping and increases the Throughput of the network. In scenario 1 the packet drop is decreased by 97.04 % and in scenario 2 the packet drop is decreased by 86.44 %. Also, negligible time is taken for detection of malicious node by the use of proposed algorithm. The time is measured after the new route is discovered. If there is packet drop because of congestion it is also taken care by way of identifying and isolating the congested node and finding new route for further communication, that is, transferring the traffic to another discovered route. Thus, it is concluded that the proposed N2N Trust based mechanism increases the overall performance of the network when used with DSR protocol. In future, we may apply this mechanism with other MANET protocols like AODV and achieve efficient performance results.

ACKNOWLEDGMENT

We are grateful to our Department of Computer Science and Engineering's renowned Research and Development Department Head, members, and all respected academic members**,** [**Suresh Gyan Vihar University, Rajasthan**].

REFERENCES:

[1] Imran M, Khan F, Jamal T, Durad M. Analysis of Detection Features for Wormhole Attacks in MANETs. Procedia Computer Science. 2015;56:384-390.

[2] Singh R, Singh J, Singh R. WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks. Mobile Information Systems. 2016;2016:1-13.

[3] Gupta A., Gupta A. A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks. *Global Journal of Computer*

Science and Technology: E Network, Web & Security 2014: 22-31.

[4] Singh S, Singh Saini H. Security Techniques for Wormhole Attack in Wireless Sensor Networks. International Journal of Engineering & Technology. 2018;7(2.23):59.

[5] Baid D, Dugar K, Sarkar P. Survey on Wormhole Attack Detection Techniques in Mobile Ad-hoc Network. International Journal of Computer Applications. 2015;120(11):9-12.

[6] Sami S. Albouq, Erik M. Fredericks. Detection and Avoidance of Wormhole Attacks in Connected Vehicles. *In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '17)*. Miami. Florida: Association for Computing Machinery, 2017: 107-116.

[7] Poonam M, Garg K, Misra M. Trust Enhanced Secure Multi-Path DSR Routing. International Journal of Computer Applications. 2010;2(2):63-69.

[8] Sharma N, Sharma M, Sharma DP. A Trust based Scheme for Spotting Malicious Node of Wormhole in Dynamic Source Routing Protocol. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). 2020:140-145.

[9] Zardari Z, Memon K, Shah R, Dehraj S, Ahmed I. A lightweight technique for detection and prevention of wormhole attack in MANET. ICST Transactions on Scalable Information Systems. 2018:165515.

[10] Patel MM, Patel PM. Intrusion Detection System Based on Trust Value in Wireless Sensor Networks. *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*. Coimbatore, India: IEEE, 2019: 618-620.

[11] Tripathi S. Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR. *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*. Banglore, India: IEEE, 2019" 1-5.

[12] V. Kavitha, T.Sujithra, D.Lavanya. Trust Based Reliable Routing Protocol for Manet. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* (2019): 1595-1598.

[13] Bhawsar A, Pandey Y and Singh U. Detection and Prevention of Wormhole Attack using the Trust-based Routing System. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC* 2020: 809-814.

[14] Qazi S, Raad R, Mu Y, Susilo W. Securing DSR against wormhole attacks in multirate ad hoc networks. Journal of Network and Computer Applications. 2013;36(2):582–92.

[15] Okunlola M, Siddiqui A, Karami A. A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks. International Journal of Computer Applications. 2017;174(4):1–8.

[16] NS 3 [Internet]. Available from: http://www.nsnam.org/

[17] Johnson D, Hu Y, Maltz D. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. 2007.

[18] Cheng Y, Çetinkaya E, Sterbenz J. Dynamic Source Routing (DSR) Protocol Implementation in ns-3. Proceedings of the Fifth International Conference on Simulation Tools and Techniques. 2012: 367-364.

[19] Sharma N, Sharma DP, Sharma M. An Efficient Mechanism For Identification Of Malicious Node Of Wormhole In Dynamic Source Routing Protocol. *International Journal of Scientific & Technology Research.* 2020: 140-145.

[20] Bhosle AA, Thosar TP. Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications. 2012;2(1):45–54.

[21] Prasad M, Tripathi S, Dahal K. Wormhole attack detection in ad hoc network using machine learning technique. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2019: 8944634.

[22] Sharma N, Sharma DP, Sharma M. A REVIEW OF PROPOSED SOLUTIONS FOR WORMHOLE ATTACK IN MANET. Advances and Applications in Mathematical Sciences .2020: 331-344.

[23] Qian L, Song N, Li X. Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. Journal of Network and Computer Applications. 2007 Jan;30(1):308–30.

[24] Seo J, Lee G. An Effective Wormhole Attack Defence Method for a Smart Meter Mesh Network in an Intelligent Power Grid. International Journal of Advanced Robotic Systems. 2012 Jan 1;9(2):49.

[25] Mwangi EG, Muketha MG, Kamau GN. Optimized Trust-Based DSR Protocol to Curb

Cooperative Blackhole Attacks in MANETs Using NS-3." *International Journal of Networks and Communications* . 2020: 10-19.

[26] Al E. Mobile ad-hoc and sensor networks : Third international conference, MSN 2007 Beijing, China, December 12-14, 2007 : proceedings. Berlin ; New York: Springer, Cop; 2007.

[27] Jadhav AD, Pellakuri V. Accuracy Based Fault Tolerant Two Phase - Intrusion Detection System (TP-IDS) Using Machine Learning and HDFS. Revue d'Intelligence Artificielle. 2021 Oct 31;35(5):359–66.