International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 4, July-Aug-2021, ISSN (Online): 2395-566X

Detection and Prevention of Wormhole Attack using the Trust-Based Routing System

M. Tech. Scholar Rachna Pandey, Prof. Pradeep Tripathi
Department of Computer Science & Engineering,
Vindhya Institute of Technology and Science,
Satna,MP,India
pandeyrachna38@gmail.com , pradeepit32@gmail.com

***Abstract*- Mobile Ad Hoc Network (MANET) is a rising spot of concentrate in the correspondence framework world. As the MANET is with without foundation, it is having dynamic nature of self-assertive system topology. The extent of this proposition is to do the investigation of wormhole attack and flooding attack set up its counteractive action system by applying it on responsive directing convention AODV, NS-2 organize test system is utilized for execution examination and reproduction. The extent of this postulation is to roll out improvements in the AODV steering convention by including a noxious node in the current AODV directing convention and in every one of the records identified with it. At that point to check the execution of system in view of a few parameters like PDR, throughput and End to end delay, TCP and UDP parcel examination and so on the outcome is being shown in NAM. A gathering of worm hole node effortlessly utilized against directing in mobile promotion sells systems. These sorts of attack are called communitarian attack. Two malevolent nodes are making a passage is called nodeholeattack. An assailant causes the clog in organize by producing an extreme measure of activity. The aggressor node always sends the gigantic amount of pointless information bundles into the system. This causes a tremendous clog of undesirable parcel into the system. Because of the hindering the information parcels, RREQ, RREP or RERR bundle send by the genuine node. To keep the wormhole, node opening, community-oriented wormhole and flooding attack, the counter measure which Trust esteem is figured on the premise of course ask for, course answer and information parcels. After count get put stock in values between 0 to 1. In the event that trust esteem is more prominent than 0.5 at that point marks node is solid and permit on a system generally piece. System execution of proposed convention trusted AODV steering convention is assessed. The outcome demonstrates execution change when contrasted with standard AODV convention.**

***Keywords*- : MANET, AODV, TAODV, NS2, UDP.**

I. INTRODUCTION

A MANET is a self-sorted out system of portable nodes and independent framework with no prior system foundation. MANET is typically alluded to as an appropriated arranges since the system association and message conveyance is circulated among the nodes.

The nodes in the system from a discretionary topology are associated over remote connections. The flexibility of node development inside the system, together with the joining or leaving the system, brings about unique and unusual topology changes. These versatile nodes discuss straightforwardly with their prompt neighbour and in a roundabout way with the far-off nodes by means of middle nodes utilizing multi-jump correspondence as appeared in figure1.1.

Commonplace remote versatile nodes incorporate portable workstations, mobile phones, stash paces or individual advanced help [1].

The halfway nodes go about as switches and forward the movement to different nodes in the system. Least setup necessity and fast arrangement of system permits a fitting and-convey technique for systems administration.

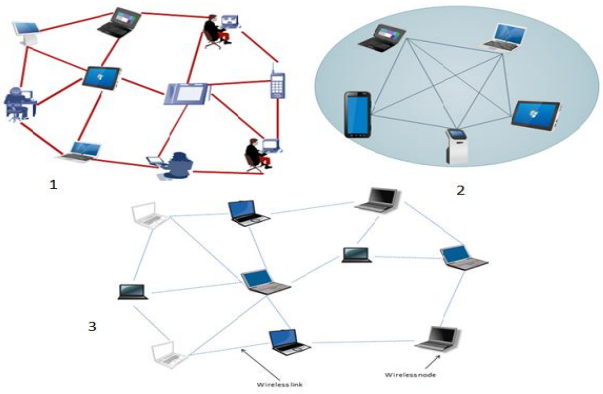

Fig 1. Mobile Ad hoc Network.

Subsequently, such systems discover applications in circumstances where there is inaccessibility of assets or absence of time to introduce and arrange a system like military systems and inquiry and safeguard operations [2].

1. Attacks in MANET:

This section gives the nitty gritty comprehension of the portable impromptu systems and their security issues [3]. The portable impromptu system might be helpless against unapproved get to and control of information since it doesn't check a client's personality before permitting the get to. MANET is more defenceless than wired system [4].

The main level of attack happens at directing in specially appointed system [5]. Though the second level of attacks tries to harm the security of the system. The attacks in MANETs are isolated into two noteworthy sorts [6].

It is appeared in figure 1.2 beneath:

- Passive Attacks
- Actives Attacks

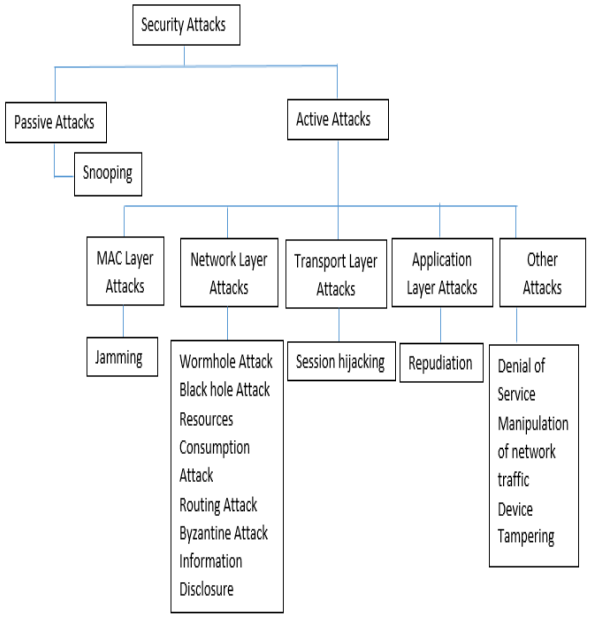

Fig 2. Classifications of Attacks. [7]

II. LITERATURE REVIEW

Silvia Krug et al. One normal methodology is to give better network by including extra nodes and endeavor the subsequent contacts as proficiently as would be prudent. Surely understood DTN conventions are anyway not ready to ensure that, since they are ignorant of associations that keep going for a moderately prolonged stretch of time and in this manner give stable network. These outcomes from general plan suppositions of the DTN conventions and are significant for the execution of crossover MANET-DTN arrangements.

In this paper, we give an audit to this circumstance and propose a half and half arrangement idea dependent on layer 3 benefit disclosures and a contact-mindful utility scoring component for DTN conventions and execute our idea for instance in one DTN convention.

Utilizing reproductions, we can demonstrate that this blend of components can give better generally speaking execution within the sight of enduring stable contacts [8].

K. Thamizhmaran et all. In this way, the creators have presented another strategy of Intrusion Detection System (IDS) named EA3ACK utilizing EAACK with Secure Hybrid Shortest Path Routing (SHSP), which is structured just for MANETs for decreasing postponement. Recognize strategy is actualized to redress any sort of assaults on the system with SHSP steering calculation other than amending shortcoming aftereffects of past work through the Network Simulator-2.

At last, in this proposed plan, a protected correspondence is furnished with diminishing overhead, deferral, and parcel misfortune utilizing EA3ACK with SHSP calculation expanding the effectiveness of system topology [9].

Amit Kumar Roy et all. proposed work prevents the AODV routing protocol against the wormhole attack in WMNs. The simulation of our proposed work had done using NS-3 simulator, and the results show that the performance of our detection algorithm improves over the existing detection techniques against wormhole attack [10].

Snehal Deshmukh-Bhosale et all. proposed work in this paper is an implementation of an intrusion detection system (IDS) for Wormhole attack and attacker. Wormhole attack is one of the most severe attacks taking place at 6LoWPAN adaption layer of RPL network. In this type of attack, a pair of attacker nodes forms a tunnel between two nodes as if they are directly connected to each other to misguide network traffic. The proposed IDS is implemented in Contiki OS, using Cooja Simulator. We have used received signal strength indicator (RSSI) to identify the attack and attacker node [11].

III. PROBLEM STATEMENT

- A malicious attack injects routing overhead that is increasing significantly.
- This routing overhead directly impacts on the network performance in terms throughput, end to end delay and packet delivery ratio.
- The attackers consume the node energy, and data packets information.
- Due to the malicious attacks packets are continuously modified therefore packet lost rate is increased mean while network throughput reduced.

IV. PROPOSED WORK

The trust level esteem figuring depends on the parameters appeared in the table 3.1. The check field portrays around two criteria achievement and disappointment which depicts whether the communicate was an effective transmission or a disappointment. RREQ and RREP are the course request and course answer separately which is traded between nodes in the system. Information alludes to the payload transmitted by the node in the directing way.

Table 1. Trust Value Calculation Parameters.

Communication Type	Rreq	Rrep	Data In Max Queue Size (1000)
Success	Rreqs	Rreps	Datas
Failure	Rreqf	Rrepf	Dataf

The parameter RREQS is characterized as the course ask for achievement rate which is computed in view of number of neighbouring nodes who have effectively gotten from the source node which has communicate it, REEQF characterized as the course ask for not a win rate which is ascertain base on number of neighbouring nodes which have not gotten the inquiry ask for, RREPS is characterizes as the course answer achievement rate which is figured as fruitful answers gotten by the source node which has sent the RREQ and RREPF is characterized as the course answer disappointment rate which is figured in view of the quantity of neighbouring nodes which have not sent the answers for the question ask forgot.

Facts is characterized as the information achievement rate computed in view of effectively transmitted information and DATAF is characterized as information disappointment rate ascertained in light of information which have neglected to achieve goal. Nonetheless, it is perceived that for each system there will be least information misfortune because of different limitations.

$$RRR = (RREQS - RREQF) / (RREQS+RREQF) \quad \text{…….. (1)}$$

$$RPR = (RREPS - RREPF) / (RREPS + RREPF) \quad \text{……. . (2)}$$

$$RDR = (DATAS - DATAF) / (DATAS +DATAF) \quad \text{…..…… (3)}$$

Where RRR, RPR and RDR are middle of the route esteems that are utilized to ascertain the nodes Request rate, Reply rate and Data transmission rate. The estimations of RRR, RPR and RDR are standardized to fall in scope of -1 to +1. On the off chance that the qualities fall past the standardized range then it obviously demonstrates that the disappointment rate of the node is expanded and means that the comparing node may not be able for directing.

$$TV = (RRR + RPR + RDR) /3 \quad \text{..... (4)}$$

Where, TV is the trust esteem and T (RREQ), T (RREP) and T (DATA) are time factorial at which course request, course reaction and information are sent by the node in a specific order. Aside from the previously mentioned standardized range, utilizing the above equation the trust esteem (TV) is figured for every node amid steering and is checked against the edge esteem (extend - 1 to +1).

Table 2 Threshold Comparison.

Trust Value	Action	Node Behavior
0 - 0.4	Block	Unreliable node
0.4 - 0.7	Allow	Reliable nodes
0.7 – 1	Allow	Most Reliable

- **Unreliable:** The depended node of the system is delegated Unreliable node. These nodes have least trust esteem.
- **Reliable:** These are the nodes which have the trust level among the Most Reliable and Unreliable. Implies a node is Reliable to its neighbour implies it has sent a few bundles through that node.
- **Most Reliable:** The nodes with higher trust esteems are considered as most solid node.

This node might be the best node for some other transmission between some other source and goal in a similar system. TAODV checks each node with its trust an incentive to make itself extreme and in charge of valuable and capable directing and furthermore to ensure security in MANET.

1. Flow Chart of Proposed Work.

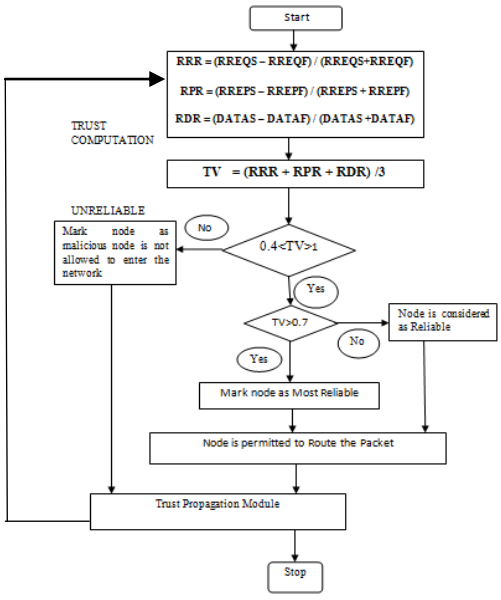

Figure: 3 Flow Chart of Proposed Method.

V. SIMULATION PARAMETERS

Table 3 Summarizes the Parameters of our Simulations.

Parameter	Value
Network Area	1000×1000
Simulation time	150s
Number of nodes	20, 50
Traffic type	TCP/CBR
Traffic model	Random Waypoint
Pause time	1s
Maximum speed	5 m/s
Wormhole node	0, 2,4,6,8 | 0,5,10,15,20

VI. RESULT SCREEN SCENARIO

Figure 4.1 20 numbers of nodes are made and remote node convey one another. These scenarios display nodes.

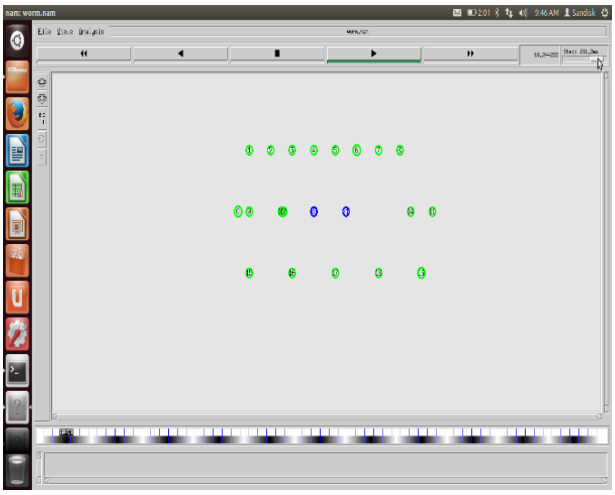

Fig 4. Creating Nodes on NS2 Tool.

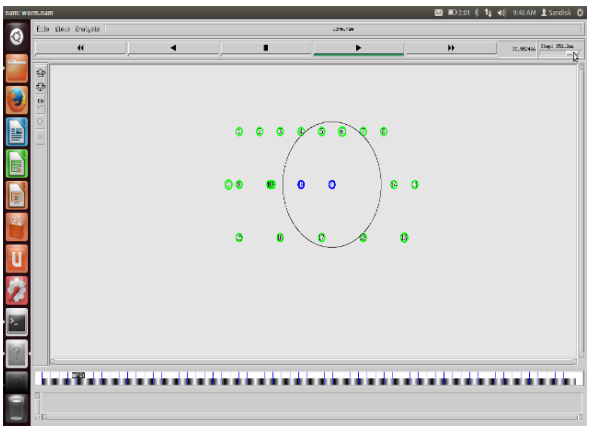

Fig 5. Display Malicious Nodes during Commutation.

Figure 4.2 remote center confer each other and data transmission using AODV count with 2 aggressors. In the midst of correspondence each aggressor get all packages its neighboring association center points and Drop all bundles so data can't reach to objective.

Figure 4.3 remote centre point gives each other and data transmission using TAODV computation with 2 aggressors. In the midst of correspondence each assailant gets all packages its neighbouring association centres and drop all groups.

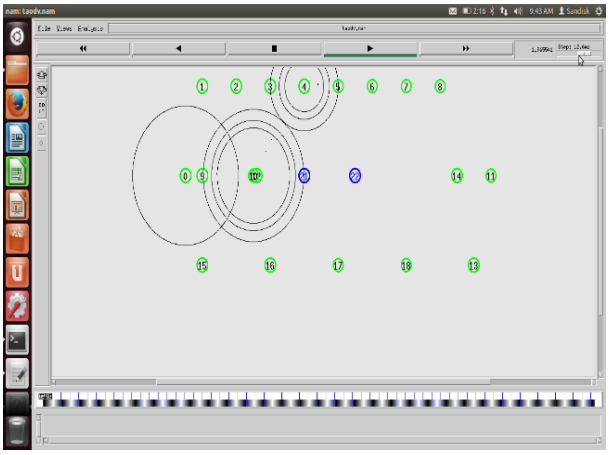

Fig 6. Detection of Worm Holes Attacker Using TAODV.

Figure 4.4 remote centre point pass on each other and data transmission using TAODV count with 2 attackers. Using TAODV recognize noxious centre points and change the course in the midst of bundle transmission.

So finally, data transmitted among source and objective canter point's way Secure Route. Our model depends after suppositions: All canter points are relative in their physical properties.

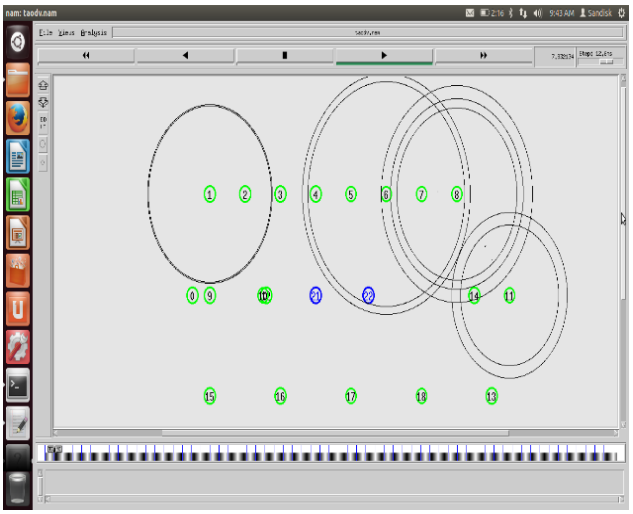

Fig 7.Prevention of Worm Holes Attacker Using TAODV.

1. Simulation:

1.1 Simulation Result for 20 Nodes:

Table 4. Simulation Result For 20 Nodes.

	Simulation Result for 20 Nodes				
	Number of Malicious Node				
Parameters	0	2	4	6	8
Throughput (kbps)	45.21	33.85	18.46	11.96	7.24
End-to-End Delay (ms)	0.29	0.55	1.49	6.37	13.11
Packet Delivery Ratio (%)	43.98	36.78	19.42	9.65	12.36

1.2 Simulation Result For 50 Nodes:

Table 5. Simulation Result For 50 Nodes.

	Simulation Result for 50 Nodes				
	Number of Malicious Node				
Parameters	0	5	10	15	20
Throughput (Kbps)	59.65	47.55	34.87	19.58	8.95
End-To-End Delay (Ms)	1.38	2.48	3.21	5.39	6.58
Packet Delivery Ratio (%)	31.85	24.45	18.36	15.89	8.66

2. Result Analysis:

2.1 Packet Delivery Ratio (PDR):

PDR =No of packet received / No of Send packets

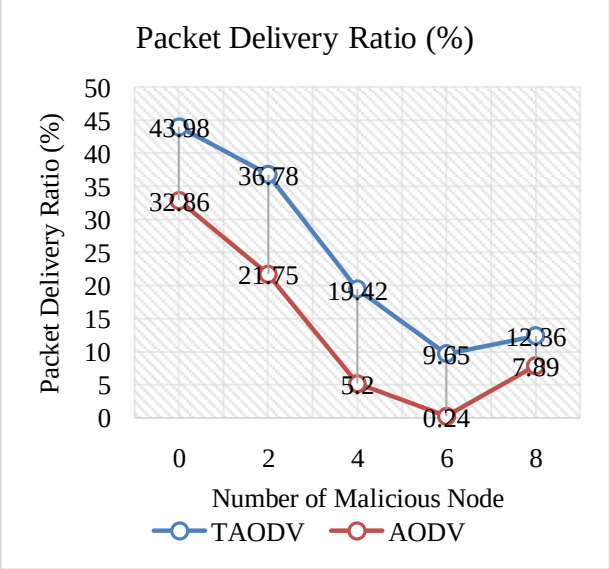

Fig 8. Packet Delivery Ratios for 20 Nodes.

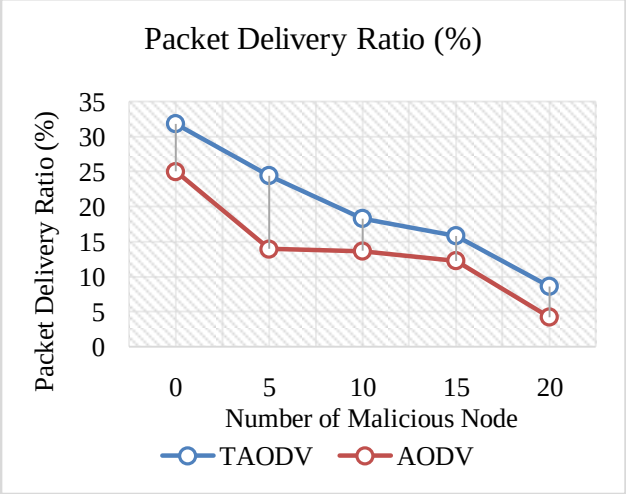

Fig 9. Packet Delivery Ratios for 50 Nodes.

2.2 End to End Delay:

E to E Delay = (Arrive time - Send time) / Number of send messages

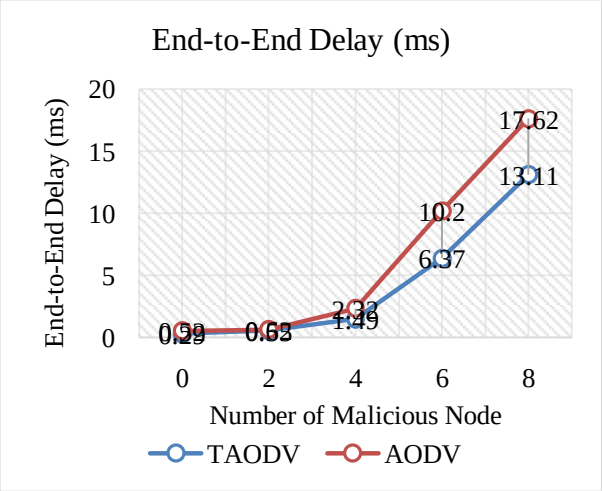

Fig 10. End to End Delay for 20 Nodes.

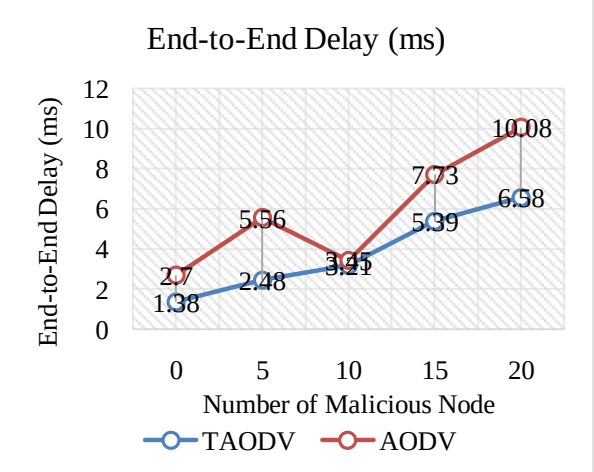

Fig 11. End to End Delay for 50 Nodes.

2.3 Throughput (kbps):

Throughput = (No. of Packets ∗ Packet Size) / Total Time

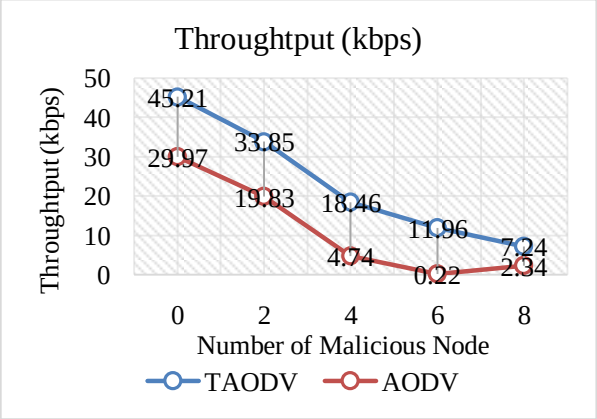

Fig 12. Throughputs for 20 Nodes.

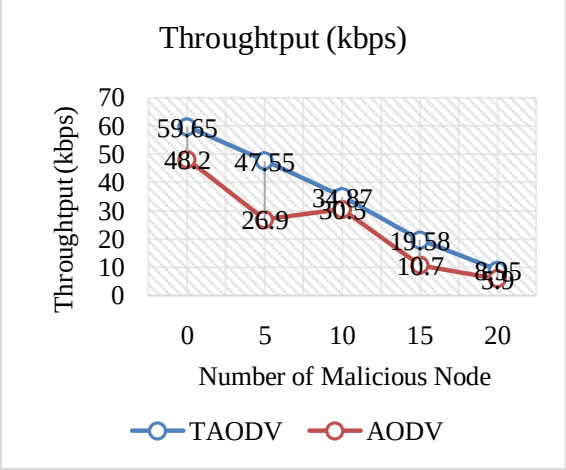

Fig 13. Throughputs for 50 Nodes.

2.4 Comparison between Existing and Proposed Protocol:

Table 6. Comparisons between Existing Protocol (EP) and Proposed Protocol (PP).

Parameters	Simulation Result For 50 Nodes, Number of Malicious Node: 0		2		4		6		8	
	TAODV	AODV	TAODV	AODV	TAODV	AODV	TAODV	AODV	TAODV	AODV
Throughtput (kbps)	45.21	29.97	33.85	19.83	18.46	4.74	11.96	0.22	7.24	2.34
End-to-End Delay (ms)	0.29	0.52	0.55	0.62	1.49	2.32	6.37	10.2	13.11	17.62
Packet Delivery Ratio (%)	31.85	25.08	24.45	14.0	18.36	13.7	15.89	12.3	8.66	4.26
Packet Delivery Ratio (%)	43.98	32.86	36.78	21.75	19.42	5.20	9.65	0.24	12.36	7.89

Parameters	Simulation Result For 50 Nodes, Number of Malicious Node: 0		5		10		15		20	
	TAODV	AODV	TAODV	AODV	TAODV	AODV	TAODV	AODV	TAODV	AODV
Throughtput (kbps)	59.65	48.2	47.55	26.9	34.87	30.5	19.58	10.7	8.95	5.9
End-to-End Delay (ms)	1.38	2.70	2.48	5.56	3.21	3.45	5.39	7.73	6.58	10.08
Packet Delivery Ratio (%)	31.85	25.08	24.45	14.0	18.36	13.7	15.89	12.3	8.66	4.26
Packet Delivery Ratio (%)	43.98	32.86	36.78	21.75	19.42	5.20	9.65	0.24	12.36	7.89

VII. CONCLUSION

The target of this review is to upgrade the execution of the system by maintaining a strategic distance from or keeping the brought together attack. The portable impromptu system is a dynamic foundation of the correspondence. The conveying gadgets in this system are connected through the remote connections. These remote connections empower a client to move inside the system arbitrarily in different bearings. In this way the course disclosure and administration are duty of the specially appointed system directing conventions. On the off chance that any versatile node needs to convey, it initially plays out the course disclosure, and after that the moderate switches are chosen for correspondence. Also, if any course is ruptured then another way is found in the system for correspondence. Along these lines amid this procedure the protected directing is required.

In this paper, an up degree is being actualized by TAODV over AODV convention. Attacks imply more than one attack in the meantime propelled against MANET. We have utilized, situation of attacks mimicked utilizing NS2, in situation comprised of dark opening attack, wormhole attack and shared dark gap attack all the while on the system.

In the situation, arranged work TAODV demonstrates execution advance of system measurements like bundle

conveyance proportion, end to end postpone and throughput over AODV directing convention.

FUTURE SCOPE

The proposed plan is utilized to evade the brought together attacks in MANET. This system can be utilized to evade different other system layer attacks and enhance the execution of the system.

REFERENCE

[1] Madhu Sharma, Ashish Jain, "Wormhole Attack in Mobile Ad-hoc Networks", IEEE, Symposium on Colossal Data Analysis and Networking (CDAN), 2016, Page No. 1-4.

[2] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016. 7570908.

[3] U. Singh, V. Vankhede, S. Maheshwari, D. Kumar, and N. Solanki, Review of Software Defined Networking: Applications, Challenges and Advantages, vol. 98. 2020.

[4] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015. 7375649.

[5] A. S. Chouhan, V. Sharma, U. Singh, and R. Sharma, "A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212740.

[6] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212719.

[7] A. Bhawsar, Y. Pandey and U. Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2020, pp. 809-814, doi: 10.1109/ICESC48915.2020.9156009.

[8] Silvia Krug, Matthias Aumüller and Jochen Seitz, "Hybrid scheme to enable DTN routing protocols to efficiently exploit stable MANET contacts", EURASIP Journal on Wireless Communications and Networking, 2018, Page No. 214:237.

[9] K. Thamizhmaran, M. Anitha, Alamelu Nachiappan, "Reduced End-To-End Delay for Manets using SHSP-EA3ACK Algorithm", https://doi.org/10.26634 /jcs. 7.3.14309, Periodicity: May - July'2018, Page No. 102-114.

[10] Amit Kumar Roy, Ajoy Kumar Khan, "RTT based wormhole detection for wireless mesh networks", International Journal of Information Technology volume 12, pages 539–546 (2020).

[11] Snehald Eshmukh-Bhosale, santosh S.Sonavane, "A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things", Elsevier, Volume 32, 2019, Pages 840-847.ary, Sylhet, Bangladesh.