JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Detection and Prevention of Attack using the Trust-Based Routing System on Underwater Mobile Adhoc Network

Uma Singh
M Tech Scholar
Department of Digital Communication
Patel College of Science and Technology Indore
umasingh137@gmail.com

Prof. Krishnakant Sharma
Assistant Professor
Department of Digital Communication
Patel College of Science and Technology Indore
Kksharma18685@gmail.com

Abstract: The correspondence framework sector is increasingly concentrating on mobile ad hoc networks, which are becoming more prevalent (MANETs). The absence of a strong foundation for MANET's dynamic self-assertive system structure is the result of the lack of a solid foundation. Researchers will conduct study on wormhole and flooding assaults, and a counteractive action mechanism will be implemented using responsive directing conventions. The AODV and NS-2 arrange test systems are used to carry out the execution inspection and replica of the programme. This hypothesis proposes that by adding an undesirable node to the current AODV steering convention and any records linked with it, the AODV steering convention may be made better. A variety of performance indicators, including PDR, throughput, and end-to-end latency, as well as TCP and UDP packet inspection, may be used to evaluate the system's overall performance at this point. The results are shown in NAM. A swarm of worm hole nodes, which is used to attack mobile promotion selling platforms, is simply a cluster of worm hole nodes that are connected together. When such an attack is carried out, it is referred to as a communitarian atrocity. The tunnel constructed by two hostile nodes is referred to as a "blackhole attack," and it is named as such. By engaging in overly active behaviour, an attacker causes a snag in the system and prevents it from working properly. The aggressor node is well-known for pouring massive volumes of useless data into the network without any regard for the consequences. This causes the system to get jammed with thousands of pounds worth of unwanted parcels. The information packets transmitted by the valid node in the RREQ, RREP, or RERR packages are impeded in their delivery. One kind of countermeasure that Trust values is based on the principles of course ask, course answer, and information packets, and it is designed to prevent the occurrence of such assaults as wormholes, node openings, community-based wormhole attacks, and flooding attacks. Following the count, stock is allocated to a number between 0 and 1. Whenever the trust esteem is more than 0.5, the node is regarded solid and may be utilised on a larger scale throughout the whole system. The system execution of the recommended convention's trustworthy AODV steering convention is currently being examined. When the findings are compared to the standard AODV convention, the results reveal that the execution has changed.

Keyword: MANET, AODV, TAODV, NS2, UDP.

I. INTRODUCTION

Unlike a traditional network, a MANET is self-organizing and does not need a preexisting system basis. Since the system association and message conveyance are exchanged among the nodes, MANET is sometimes referred to as an appropriated arrangement. Remote connections link the system's nodes in a discretionary topology. Node development within the system is flexible, and as nodes join or leave the system, the topology alters in unexpected ways. Figure 1.1 shows how these adaptable nodes communicate both directly with their immediate neighbour and indirectly with the far-off nodes through intermediary nodes via multi-jump correspondence. Individual sophisticated help or portable workstations are commonplace remote versatile nodes [1].

On one hand, the midpoints act as a switch and provide information about movement to other nodes. The ability to use a fitting and-and-convey system administration approach is made possible by the system's minimal setup requirements and rapid system configuration. Once these systems find uses in

situations where assets are unavailable or there is not enough time to introduce and configure a system, such as military systems and investigation and safeguard activities, they become very useful [2].

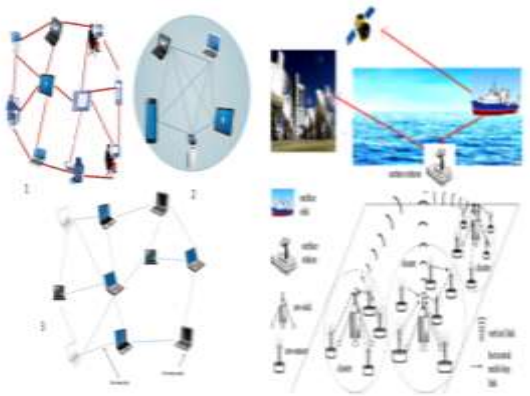

Figure 1 Mobile Ad hoc Network

1.2 Attacks in MANET

Detailed understanding of portable impromptu systems and security challenges is provided in this section [3]. Unauthorized access to and control of information may be impossible with the portable system since it does not verify the personality of the client before allowing access. In comparison to a wired system, MANET is much more vulnerable [4]. The primary assault occurs when a user directs traffic via a designated system [5]. While assaults at the second level attempt to compromise the system's security. MANET attacks may be divided into two categories [6]. Figure 1.2 shows what I'm talking about. 1) Attacks that don't have an effect 2) Attacks that do

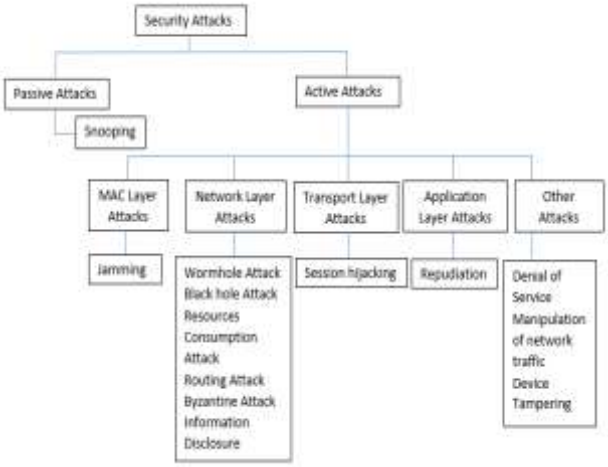

Figure 2 Classifications of Attacks [7]

II. LITERATURE REVIEW

Professors Silvia Krug and colleagues One common approach is to expand the network and make following interactions as effectively as possible in order to provide better service. However, it is clear that DTN conventions do not have the ability to assure this since they are unaware of relationships that have lasted for a reasonably long period of time and provide a stable network in this way. A key effect of DTN convention general plan assumptions is that crossover MANET-DTN configurations may now be implemented. Here, we conduct an audit of the situation and offer a hybrid arrangement notion for DTN conferences based on layer 3 benefit disclosures and a contact-mindful utility score component, and we put our concept into practise in a single DTN conference as an example of hybrid arrangement. We can show by replicas that this combination of components may provide improved overall performance in the context of long-term stable connections [8].

K. Thamizhmaran and colleagues. These developers have created a new approach to the IDS known as EA3ACK that utilises EAack with Secure Hybrid Shortest Path Routing (SHSP), which is specifically designed for MANETs to minimise delay. In addition to correcting deficiency aftereffects of previous work, recognise approach is implemented to redress any assaults on the system using SHSP steering computation. Using EA3ACK with SHSP computation, a protected communication is finally provided with reduced overhead, delay, and parcel misery in this suggested approach [9].

The proposed method by Amit Kumar Roy et al. protects WMN AODV routing protocols against wormhole attacks. It was shown that utilising the NS-3 simulator to simulate our proposed work made it more effective at detecting wormhole attacks than the other current detection methods [10].

SnehalDeshmukh-Bhosale et al are included in this grouping. A Wormhole attack and attacker intrusion detection system (IDS) implementation is provided in this study. RPL network's 6LoWPAN adaptation layer is under assault via a wormhole attack. A pair of attacker nodes creates a tunnel between two other nodes, making it seem as though they are physically linked, in order to sabotage network activity. Cooja Simulator is used to simulate the proposed IDS in Contiki OS. The received signal strength indicator (RSSI) has been utilised to identify the attack and the node that launched it [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.

$$RRR = (RREQS - RREQF) / (RREQS+RREQF) \ldots\ldots\ldots (1)$$

$$RPR = (RREPS - RREPF) / (RREPS + RREPF) \ldots\ldots\ldots (2)$$

$$RDR = (DATAS - DATAF) / (DATAS + DATAF) \ldots\ldots\ldots (3)$$

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.

$$TV = (RRR + RPR + RDR) / 3 \ldots\ldots\ldots (4)$$

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

I.**Unreliable:** The depended node of the system is delegated Unreliable node. These nodes have least trust esteem.

II. **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.

III. **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.

4.1 Flow Chart of Proposed Work

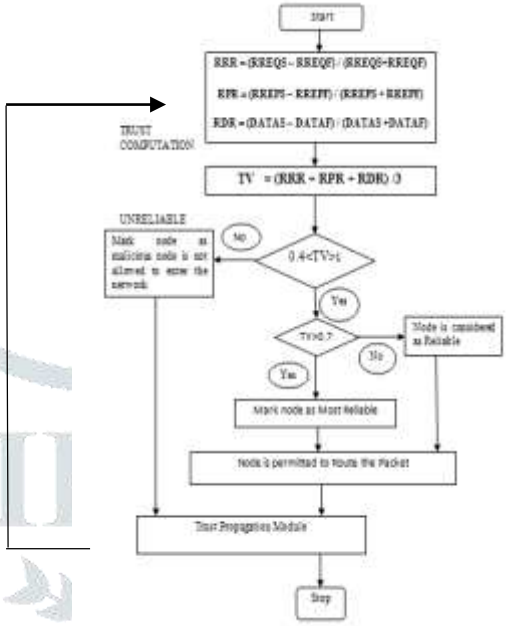

Figure: 3 Flow Chart of Proposed Method

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.

TRUST VALUE	ACTION	NODE BEHAVIOR
0 - 0.4	Block	Unreliable node
0.4 - 0.7	Allow	Reliable nodes
0.7 – 1	Allow	Most Reliable

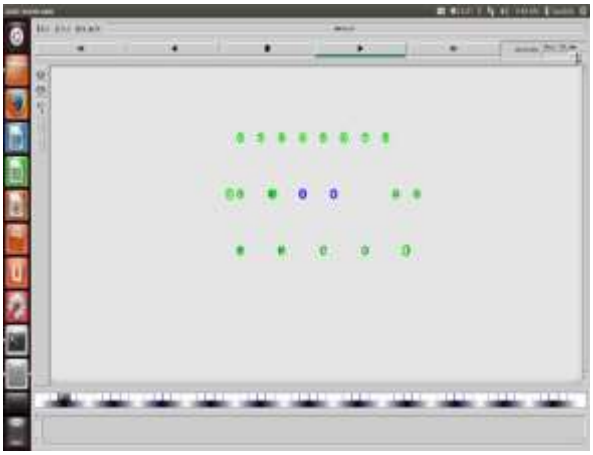

Figure 4 Creating Nodes on NS2 Tool

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.

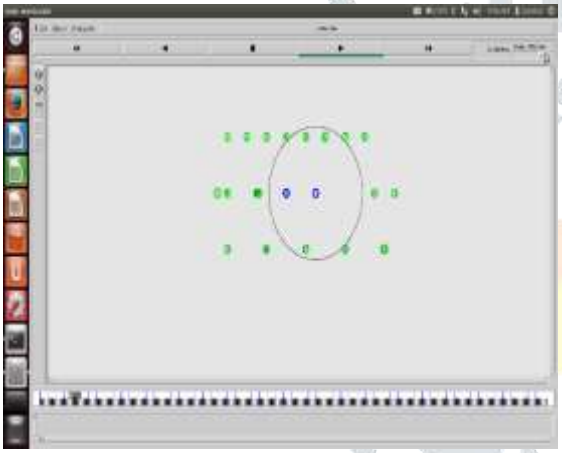

Figure 5 Display Malicious Nodes during Commutation

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.

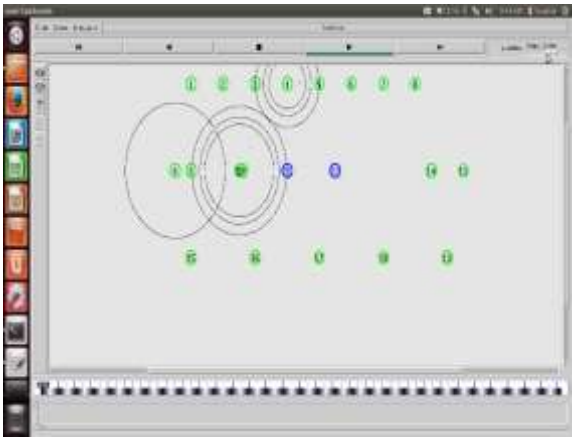

Figure 6 Detection of Worm Holes Attacker Using TAODV

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.

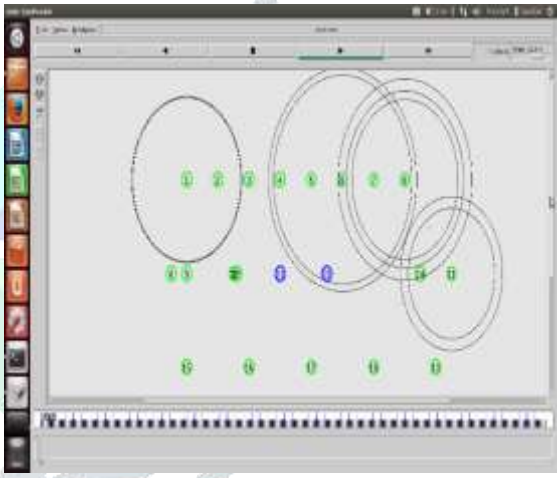

Figure 7 Prevention of Worm Holes Attacker Using TAODV

6.1 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**

Table 5 Simulation Result For 50 Nodes

6.1 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

6.2 Result Analysis

6.2.1 Packet Delivery Ratio (PDR)

PDR =No of packet received / No of Send packets

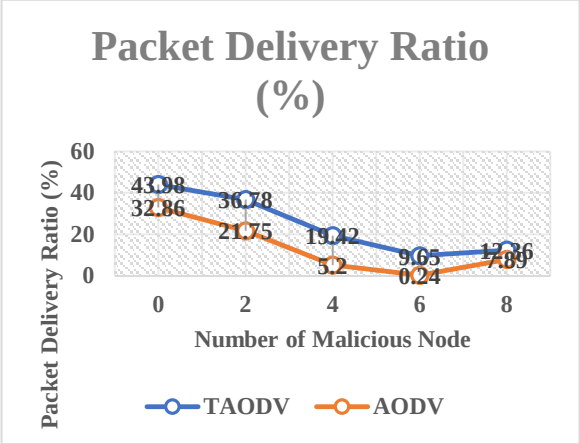

Figure 8 Packet Delivery Ratios for 20 Nodes

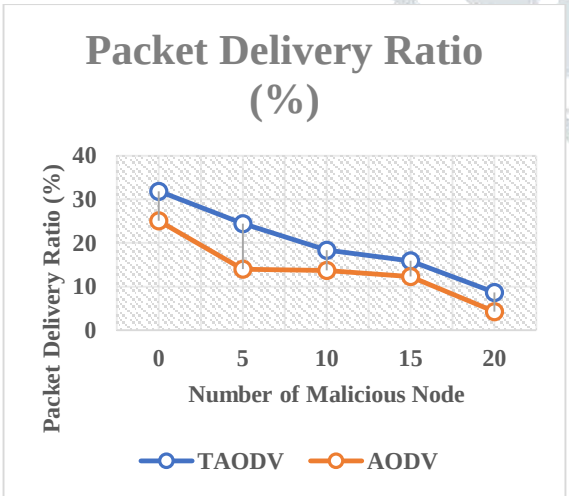

Figure 9 Packet Delivery Ratios for 50 Nodes

6.2.2 End to End Delay

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

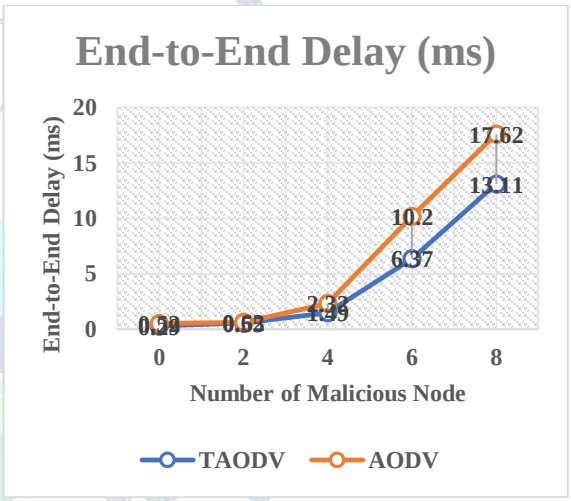

Figure 10 End to End Delay for 20 Nodes

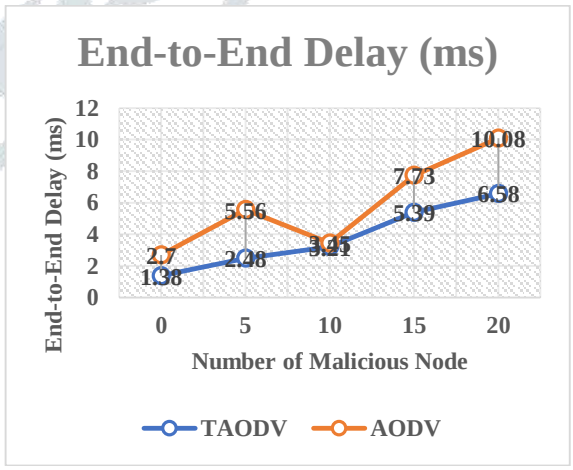

Figure 11 End to End Delay for 50 Nodes

6.2.3 Throughput (kbps)

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

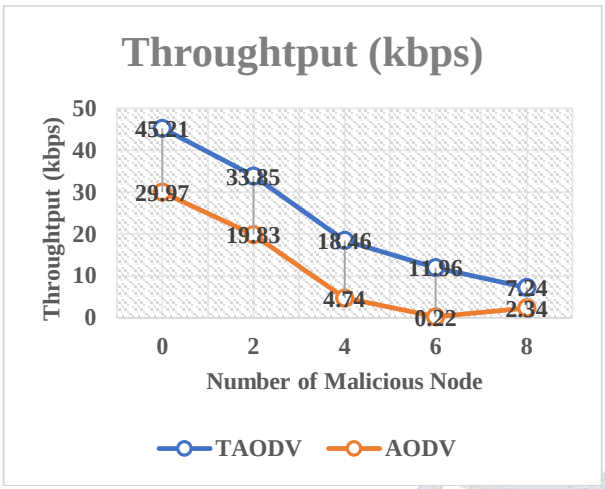

Figure 12 Throughputs for 20 Nodes

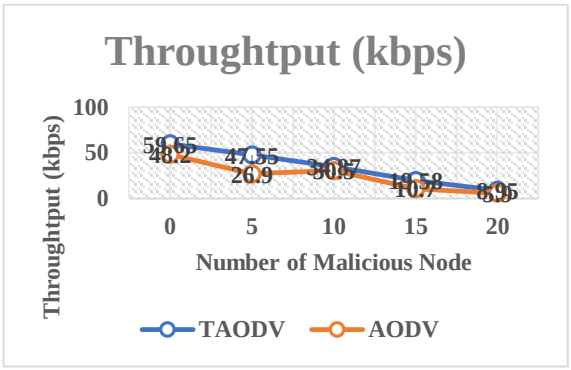

Figure 13 Throughputs for 50 Nodes

6.2.4 Comparison between Existing and Proposed Protocol

Table 4.4 Comparisons between Existing Protocol (EP) and Proposed Protocol (PP).

	SIMULATION RESULT FOR 20 NODES									
	Number of Malicious Node									
Parameters	**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 (%)	43.98	32.86	36.78	21.75	19.42	5.20	9.65	0.24	12.36	7.89

	SIMULATION RESULT FOR 50 NODES									
	Number of Malicious Node									
Parameters	**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

VII. CONCLUSION

7.1 Conclusion: By keeping a strategic distance from or not engaging in a coordinated assault, this evaluation hopes to improve system execution. The mobile impromptu system is the correspondence's dynamic base. The remote connections link the system's conveyance devices. These remote connections allow a user to freely travel about the system in any direction. Specifically designated system directing conventions are in charge of disclosing and administering course information. When a flexible node wants to communicate, the course disclosure is first performed, and then the medium switches are selected for communication. In addition, if a course is interrupted, a replacement method for communication is discovered in the system. For those reasons and more, protective direction is essential throughout this treatment.
TAODV is used to actualize an up degree above the AODV convention in this research. Attacks suggest that MANET is the target of many attacks at the same time. On the system, we have used NS2 to simulate an attack scenario that includes a dark opening attack, wormhole assault, and shared dark gap attack. An organised task TAODV shows that system measures such bundle conveyance percentage, end-to-end delay, and throughput are executed ahead of schedule when compared to AODV direction convention in this case.

7.2 Future Scope

It is recommended that a strategy be used to circumvent MANET's coordinated strikes. This system may be used to thwart assaults on other system layers while also improving the system's performance.

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.