Detecting and Predicting Malicious Nodes in Mobile Ad-hoc Networks using a Secure Technique

Imran Khan
Research Scholar
Department of Computer Science & Engineering
IES, IPS Academy Indore, India

Pratik Gite
Associate Professor
Department of Computer Science & Engineering
IES, IPS Academy Indore, India

ABSTRACT
Mobile Ad Hoc Networking (MANET) is a rapidly growing area of interest in the realm of communication frameworks. Due to the fact that the MANET lacks a basis, it exhibits the dynamic character of a self-assertive network architecture. Security concerns are critical in these networks. Nodes in MANETs may launch a variety of assaults or become conspicuously self-centered in order to preserve their advantage. These nodes may be considered malicious. Identification of such malicious nodes is critical for the successful operation of MANETs. A collection of networks has been presented, but each one has its own set of constraints. The scope of this proposal is to do research on black hole, worm hole collaborative malevolent, and flooding attacks, and to establish a network of counteractive action by using responsive directing conventions. For execution analysis and replication, an AODV, NS-2 organized test network is used. To prevent black hole, worm hole collaboration malevolent, and flooding attacks, a countermeasure is used in which the Trust value is calculated based on the route request, route response, and information packet. Following the count, place stock in values ranging from 0 to 1. If the trust esteem is more than 0.5, the node is solid and permits access to the network as a whole. The suggested convention secure Ad hoc On-demand distance vector (SAODV) is evaluated in terms of network execution. When compared to the usual AODV convention, the result reveals execution change. By increasing the duration a dip in throughput, SAODV's throughput is superior to that of joint malicious assault AODV and current protocol. SAODV's packet delivery ratio is superior to that of joint malicious attack AODV and the established AODV protocol. SAODV's End to End Delay is superior than joint malicious attack AODV and the current AODV protocol.

Keywords
Mobile Ad Hoc Networking, AODV, SAODV, NS2, End to End Delay, Packet Delivery Ratio, Throughput

1. INTRODUCTION
Multi-hop network pathways may be built in a Mobile Ad Hoc Network (MANET), where each node serves as a router, without the requirement for a telecommunications backbone. When a wireless network is used in place of a wired network, it is ideal for military and emergency rescue operations, as well as for short-term classroom or conference events. The security of such a network must be given high importance. The openness of the wireless medium allows outsiders to observe and interfere with network activity as a consequence of its use by criminals. Such considerations may expose sensors to a broad variety of assaults [1] as a result of their implementation. These malicious nodes are capable of launching both passive and aggressive assaults on the network from their positions. On the other hand, active assaults may require the rogue node to spoof or reject real messages in addition to just listening in on them. Wormhole attacks are a common kind of active security attack that has the potential to do significant harm. An attacker collects packets from one site in a network and delivers them to another malicious node, which then repeats the packets in its own network, thereby causing the network to crash. This active assault poses a threat to wireless security systems and routing protocols, as well as aggregated and clustered data storage systems. The active attack may also be initiated even if no cryptographic keys have been given.

MANET is a wirelessly linked network of mobile nodes that may operate independently of one another and communicate with one another. It is not built on any type of strong basis. The router function is performed by each node in the centre of the network in this scenario. When a node moves from one location to another, MANET ensures that the device remains available and that it can adapt to the new environment. Routing packets from the source node to an adjacent node allows them to be routed until they reach their ultimate destination. [2] [2]. A lack of constant wireless connections between mobile nodes in an ad hoc network is a problem for communication participants due to a lack of sufficient energy to allow the nodes in the network to move around freely. Another stumbling issue is the topology of the dynamic network itself. Nodes in MANETs have the ability to join or leave the network at any moment, as well as travel independently of one another. MANETs do not have a predefined topology because of the nature of the network type. If nodes are not physically safeguarded, they have the potential to become malevolent and cause network performance to suffer. These networks are especially vulnerable to malicious assaults because of their key characteristics, which include dynamic topology, wireless medium, and bandwidth limitations [3].

Reactive, proactive, or a mix of the three [4] types of MANET protocols can be found. MANET routing technology is all about making routes between mobile nodes that are both energy-efficient and meet quality of service needs like bandwidth and end-to-end latency, which are important to the way the technology works. In the MANET protocols, you can use AODV, DSR, RAODV, AOMDV, and TORA, as well as many other things, to get information from one place to another quickly (TORA). AODV is better than other reactive routing protocols when it comes to important quality of service (QoS) criteria when it comes to modeling black holes [5]. [6] People use the AODV and DSR protocols the most

when they use a MANET. Integration of DSR and DSDV routing protocols is also part of the package. This gives you the best of both worlds.

When using the AODV protocol, there must be ways to find and manage routes to avoid routing loops. Denial-of-service (DoS) attacks are the most common type of attack on MANETs [7]. They use the most electricity. Using another strategy, [8] worked to build a wireless sensor network cluster algorithm based on the Queen-Bee (QB) algorithm, and they used that to build the algorithm. Its ability to figure out the best value for the local minimum is helped by the method's quick convergence, which makes it a more efficient algorithm. Normal and severe mutations are thought to make future generations more diverse and able to ignore early differences. The results show that the proposed QB algorithm is more energy efficient than the genetic algorithm (GA), which means the network will last longer in the long run.

According to [9], they developed a hierarchical clustering algorithm (HCAL) and a protocol for massively parallel MANETs (LMANET). When table-based and on-demand routing weight matrices are combined, a collection of the network's most important nodes is obtained. The LMANET network was constructed using the node count and timeout values for each connection. Additionally, it was determined how long it took to run, how much time it took to run, how much overhead was required, and how much PDR was required. The new HCAL protocol performs better than its predecessors in terms of functionality. Dynamic Doppler velocity clustering is compared to clustering based on signal characteristics, dynamic link duration, dynamic mobility, and dynamic link duration.

Section 2 is called "Literature Work." The rest of the paper is broken down like this: Section 3 proposes a method, Section 4 shows how it was done and what happened, and Section 5 sums up our paper.

2. LITRACTURE WORK

Personal area networks (PANs), and Bluetooth are all instances of ad hoc networks when it comes to wireless communication [10, 11]. Ad hoc networks are also used in other types of wireless communication, such as wireless LANs. When it comes to providing reliable communication between nodes, especially under demanding settings, there is an increasing need to investigate MANETs [12]. These networks, on the other hand, contain a number of security weaknesses that must be addressed. Many researchers have proposed a broad variety of solutions [13, 14] to enhance MANET security during the past few years, including but not limited to cryptographic approaches, protocol tweaks, and intrusion detection systems (IDS). Their solution for MANET IDS is based on a neuro-fuzzy approach, which they discuss in full in [15]. For intruder detection and identification, [16] was a pioneer in the use of a fuzzy method, which is still in use today. It was recommended in [17] that an enhanced trust detection technique be used for detecting and blocking dangerous attackers in MANETs, which boosted the effectiveness of the strategy.

Using this technique, malicious maliciousnodes are avoided in MANETs, network performance is increased, packet loss is minimized, and power consumption is reduced when harmful malicious nodes are present. Another possibility mentioned in [18] is the use of detection algorithms that have a low network overhead. This method has the potential to enhance the density of dense networks by 45.6 percent while increasing the sparsity of sparse networks by 41 percent. Furthermore, it reduces the amount of lost packets by 75% in dense networks and by 63% in sparse networks when used in conjunction with other techniques.

A honey pot-based security solution is provided in order to enable improved packet delivery with fewer packet losses, as well as reduced end-to-end latency and network strain from one end to the other. The authors of this study suggest a dynamic destination sequence number threshold value that identifies and disables maliciousnodes while outperforming the malicious assault while also outperforming the malicious attack. [19] Another research group has developed mathematical approaches for recognizing and avoiding malicious nodes in MANETs, which they believe may be useful in the future. Furthermore, there are a variety of approaches that have been developed to solve the security flaws of MANETs.

It is very difficult to maintain network security in a MANET since there are no defined boundaries, opponents inside the networks continue to operate uninterrupted, and there is no centralized management. As a result, MANETs are vulnerable to a wide range of different types of assaults. This includes, but is not limited to, attacks such as the black hole, eavesdropping, and man in the middle attacks, as well as wormholes, impersonation, and other similar techniques. These assailants might be violent or calm in their approach. It was discovered that the malicious assault was one of the most lethal attacks carried out by these perpetrators. Attacks on MANETs may be prevented in one of two ways: either by being proactive or by reacting to an attack. However, once an assault has been launched, there are a variety of options for responding to it. There are many approaches that may be taken to prevent an attack from being launched in the first place. It is necessary to utilize both detection and prevention techniques, as well as a response component, in order to create a comprehensive security solution. There are several mitigating and preventative security measures that may be ensured to offer secure routing. Figure 1 illustrates the security vulnerabilities that might arise with MANET systems.

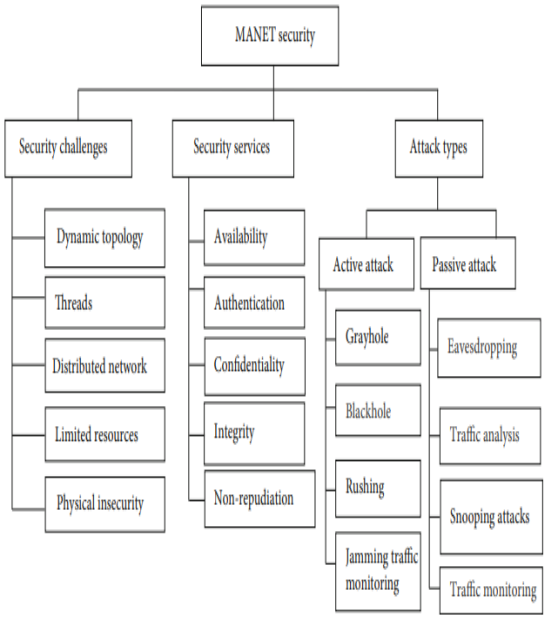

Figure 1 Attack's in MANET

3. PROPOSED METHOD

3.1 Proposed Architecture of Secure AODV

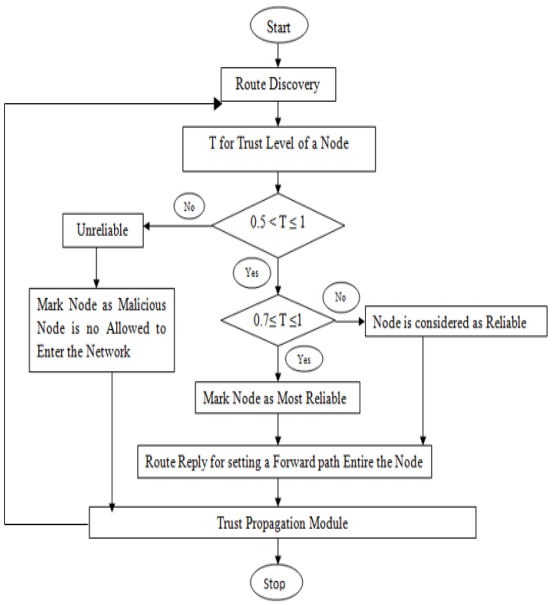

Figure 2 Flow Chart for Secure AODV Model

Secure AODV, a secure routing system based on trust display, may be implemented in mobile ad-hoc networks. Secure AODV has a broad variety of key characteristics, such as the following: Secure routing protocols are often deployed by nodes based on their connections with other nodes and the trust they have in one another. After a while, a malicious node will be found and removed from the network as a precaution. Each route node has the potential to contribute to improved network processes.

a) The degree to which a node is secure

The AODV routing protocol as well as the trust function are implemented in this piece of work. It is only via the cooperation and trust of their neighbours that nodes in a mobile ad-hoc network may become members. There are many sorts of nodes that may be classified based on their neighbour trust and threshold levels:

"Unreliable" is the term used to describe a node that is not trustworthy. A node with a low degree of trust is seen as being untrustworthy by the other nodes. When a node initially enters the network, it does not have any trust linkages with its neighbours, and as a result, it is tagged as unreliable by the network.

These are the nodes that have a trust rating that is in the centre of the range between "most trustworthy" and "least dependable." In the case of receiving two or three packets from a neighbouring node, it decides that the neighbouring node is trustworthy.

The term "most reliable" refers to the nodes that are the most trustworthy, or the nodes that have the highest degree of confidence. When a node's trust level is high, it is more probable that other nodes in the network have successfully accepted or exchanged packets with that particular node.

While the route discovery phase is in progress, AODV Routing keeps track of the trust values of each node's neighbouring nodes. All of your neighbours are evaluated as Most Reliable, Reliable, or Undependable by the trust evaluation technique at the conclusion of the process.

Because each node in this system maintains a copy of the Trust table, it is possible to keep a look out for suspicious activity. In order to maintain track of a node's relationships with other nodes, it is necessary to utilise the Trust table. The Trust table is made up of two components. The name of the node that surrounds an individual node, as well as the relationship status, which might be Most Reliable, Reliable, or Unreliable. Alternatively. Each time a packet is received, it is removed from this table and placed elsewhere.

For starters, every new node is seen as untrustworthy by the system as a whole. Unreliable has a high danger of being attacked, while Most Reliable has a low chance of being attacked.

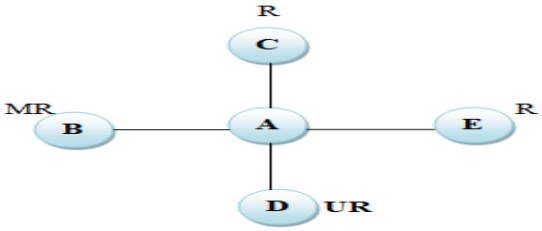

Figure 3 Trusts for Node

Table 1 Trust for Node A

Neighboring Nodes	Trust Status
B	Most Reliable
C	Reliable
D	Unreliable
E	Reliable

As seen in Fig. 3, node B is the most trustworthy, followed by nodes C and E, and finally node D, which is the least reliable. We choose a path for each node that begins at B, the node with the highest level of dependability. If there is no node with the Most Reliable status, we feed the requirement to Reliable nodes but never give an Unreliable node the opportunity to establish a route in this circumstance.

c) The Threshold Value of a Node: Neighbors vary in their reliability; some are more trustworthy than others, and some are more unreliable than others. There are three levels of reliability: unreliable, reliable, and most reliable. Each level has a threshold value of Tmr, Tr, and Tur.

We provide a Trust estimate job that can be used to calculate trust value.

$$T = \tanh(R1+R2)$$

Where,

tanh is a hyperbolic tan function, which has value

$$Tanh\ x = (e^{x} - e^{-x})/(e^{x} + e^{-x})$$

T = Trust value

R1= Ratio between the number of packets really sent and number of packets to be sent.

R2=Ratio of number of packets got from a node however started from other to signify number of packets got from it.

c) Trust Status Updating of a Node:

It is only after receiving an RREP from each neighbour that the source node is able to identify which route is the most efficient. We send out a large number of erroneous packets in order to re-establish trust. The stock statuses of nodes are computed and, if necessary, updated as part of the packet-processing process. A node must first achieve the threshold trust level of Tr before it can be considered visibly Reliable to its neighbour. It is necessary for a node to first achieve the dependability level of Tr before attempting to attain the threshold trust level of tmr. The Trusts will be referred to as such for the time being.

A (node x → node y) = Most Reliable when T ≥ t1
A (node x → node y) = Reliable when t2 ≤ T < t1
A (node x → node y) =Unreliable when 0<T ≥t2
Where,
A= Trust
T=Threshold
and t1 and t2 are the threshold values which will be decided in implement

d) Graph Representation of Trust Values of a Node:

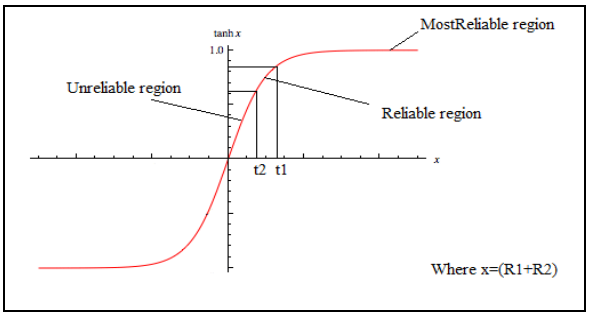

Figure 4 Representations of Trust Values of a Node

In the above graph value of x is always greater than **0**, because **R1** and **R2** will always remain positive so **T** belongs from (0, 1).

4. SIMULATION TOOLS AND RESULT

4.1 Simulation Parameters

The researchers tested the MANET protocols in this work using a simulator named NS2. The researchers developed this simulator. A software named "cbrgen" may be used to detect random traffic between nodes connected through a transmission control protocol (TCP) or a constant bit rate (CBR) connection. It is located in the "ns/independent-utils/cmu-scene-gen" directory. "setdest" may also be used to create node traces by randomly shifting nodes according to their speed to any unfixed location in the wireless range. The "ns" directory contains a file named "setdest." Additionally, it may be found in the directory "ns/independent-utils/CMU-Scen-Gen/SetDest". A small network may be constructed manually by randomly dispersing the network's nodes at each waypoint. Then, traffic connections and node mobility may be accomplished manually. Moving nodes are employed to create the wireless network environment that you see today.

Table 2 Simulation Parameters

Simulation Parameters	Value
Number Of Nodes	20,40,60,80,100
Network Size	1200m*1200m
Simulation Duration	100(Sec)
Primary Energy	100 joule
Txpowers	0.9/sec.
Repowers	0.8/sec.
Idle Power	0.0
Sense Power	0.0175
Source Node	5
Destination Node	5
Intermediate Nodes	15
Malicious Node	5,10,15,20,25
Packet Size	1024byte

4.2 Result

4.2.1 End to End Delay: This is called the End to End Delay. When there are more malicious nodes, the time it takes for AODV to go from start to finish increases. The SAODV's end-to-end delay goes up by an extra step, but it is just as safe as the AODV's.

EED = Total EED / No. of Packets Sent

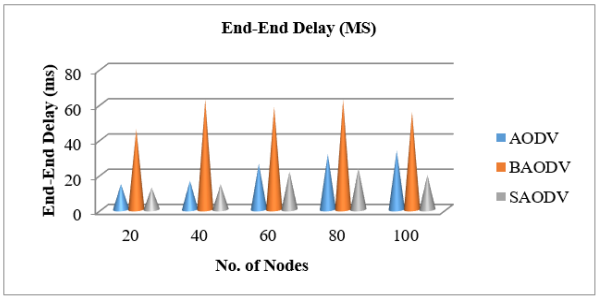

Figure 5. End to End Delay

4.2.2 Packet Delivery Ratio:"application layer" Constant Bit Rate source and Constant Bit Rate source receive less than one packet at a time during their last goal.
PDR = Packets Delivered / Packets Sent

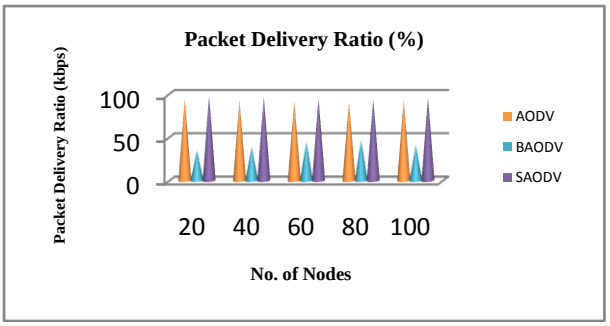

Figure 6. Packet Delivery Ratio

4.2.3 Throughputs

The usual rate of successful packet transmission through a communication channel is referred to as throughput.

Throughput = Number of Packets Sent / Time Taken

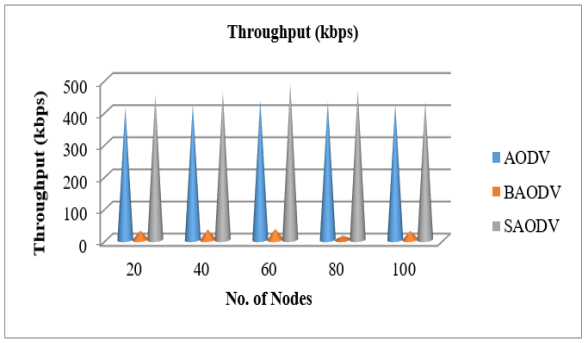

Figure 7 Packet Delivery Ratio

5. CONCLUSION

Slowing down the system's execution by keeping a critical separation will be the primary objective of this evaluation, which will begin by alternately maintaining the combined assault and then proceed from there. SAODV's participation in the AODV meeting is clearly a high point in our evaluation. MANET is being attacked by more than one person, as this incident demonstrates. An assault requires the use of NS-2 simulations to establish the parameters. In order to meet the criteria, both community-oriented and collaborative harmful attacks must be included. SAODV's throughput is better to that of AODV and the current protocol because it increases the length of time a drop in throughput influences throughput. SAODV's packet delivery ratio is much greater than that of AODV and the current AODV protocol. the present AODV protocol and the collaborative malicious attack AODV protocol, SAODV's end-to-end latency is superior to both of them.

6. REFERENCES

[1] I. Mohd Zaki and H. Rosilah, "The implementation of Internet of Things using test bed in the UKMnet environment," AsiaPacific Journal of Information Technology and Multimedia, vol. 8, no. 2, pp. 1–17, 2019.

[2] Z. Ismail and R. Hassan, "A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous MANET," in in the 17th Asia Pacific Conference on Communications, IEEE, 2011

[3] T. Salam and M. S. Hossen, "Performance analysis on homogeneous LEACH and EAMMH protocols in wireless sensor network," Wireless Personal Communications, vol. 113, no. 1, pp. 189–222, 2020

[4] M. S. Hossen, "DTN routing protocols on two distinct geographical regions in an opportunistic network: an analysis," Wireless Personal Communications, vol. 108, no. 2, pp. 839– 851, 2019.

[5] N. Khanna and M. Sachdeva, ''BEST: Battery, efficiency and stability based trust mechanism using enhanced AODV for mitigation of blackhole attack and its variants in MANETs,'' Adhoc Sensor Wireless Netw., vol. 46, nos. 3–4, pp. 215–264, 2020.

[6] R. Fotohi, E. Nazemi, and F. S. Aliee, ''An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks,'' Veh. Commun., vol. 26, Dec. 2020, Art. no. 100267.

[7] A. Nabou, M. D. Laanaoui, and M. Ouzzif, ''New MPR computation for securing OLSR routing protocol against single malicious attack,'' Wireless Pers. Commun., vol. 115, pp. 1–20, Nov. 2020.

[8] N. C. Singh and A. Sharma, ''Resilience of mobile ad hoc networks to security attacks and optimization of routing process,'' Mater. Today, Proc., 2020.

[9] M. Faraji-Biregani and R. Fotohi, ''Secure communication between UAVs using a method based on smart agents in unmanned aerial vehicles,'' J. Supercomput., vol. 76, pp. 1–28, Nov. 2020

[10] Z. Yusen, G. Jingjing, W. J. Shuang, S. Yan, Y. Li, and J. Xin, ''Formal verification approach for false route in MANET,'' Comput. Sci., vol. 39, no. 2, pp. 118–121, 2012

[11] V. Desai and N. Shekokar, ''Performance evaluation of OLSR protocol in MANET under the influence of routing attack,'' in Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN), Dec. 2014, pp. 138–143

[12] B.-T. Xu, Q. Zhu, and H. Hu, ''Analysis of connectivity in ad-hoc network based on interference and fading channel,'' J. China Universities Posts Telecommun., vol. 19, no. 5, pp. 77–82, Oct. 2012

[13] Z. Gong and M. Haenggi, ''Interference and outage in mobile random networks: Expectation, distribution, and correlation,'' IEEE Trans. Mobile Comput., vol. 13, no. 2, pp. 337–349, Feb. 2014

[14] A. Adnane, C. Bidan, and R. T. D. Sousa, ''Trust-based security for the OLSR routing protocol,'' Comput. Commun., vol. 36, nos. 10–11, pp. 1159–1171, Jun. 2013

[15] R.-R. Yin, N. Zhao, and Y.-H. Xu, ''An selective forwarding attack considered routing protocol for scale-free network,'' in Proc. 12th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP), Jul. 2020, pp. 1–6.

[16] C. Li and H. Dai, ''Connectivity of multi-channel wireless networks under jamming attacks,'' in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2013, pp. 706–711.