Fuzzy Heuristics for Detecting and Preventing Black Hole Attack

Elamparithi Pandian
Department of Computer Science and Engineering,
AAA College of Engineering and Technology,
Anna University, India
elamparithi@aaacet.ac.in

Ruba Soundar
Department of Computer Science and Engineering,
Mepco Schlenk Engineering College,
Anna University, India
rubasoundar@gmail.com

Shenbagalakshmi Gunasekaran
Department of Computer Science and Engineering,
Mepco Schlenk Engineering College,
Anna University, India
shenbagalakshmi@mepcoeng.ac.in

Shenbagarajan Anantharajan
Department of Artificial Intelligence and Data Science,
Mepco Schlenk Engineering College,
Anna University, India
shenbagarajan@mepcoeng.ac.in

Abstract: *Mobile Ad-hoc Networks (MANET) is a set of computing nodes with there is no fixed infrastructure support. Every node in the network communicates with one another through wireless links. However, in MANET, the dynamic topology of the nodes is the vital demanding duty to produce security to the network and the black hole attacks get identified and prevented. In this paper, a novel fuzzy inference system is designed for black hole attack detection depending on the node authentication, trust value, Certificate Authority (CA), energy level, and message integrity. Before initiating the route discovery process in MANET, the proposed work mainly concentrates on node authentication. The simulation gets carried out using the Network Simulator (NS2), wherein the fuzzy inference system designed shows better performance by providing a certificate to only the trusted nodes. This helps the malicious nodes detection and prevents the black hole attack. The improvement in Packet Delivery Ratio (PDR) enhances throughput and the end to end delay gets reduced through better performance results. This proves that the system is more reliable and recovered to be used in military applications.*

Keywords: *Mobile Ad-hoc networks, fuzzy inference system, trust value, black hole attack, node authentication, certificate authority.*

Received September 28, 2022; accepted May 23, 2023
https://doi.org/10.34028/iajit/21/1/8

1. Introduction

In the last decade, many researchers concentrate more on the potential applications of Mobile Ad-hoc Networks (MANET) which are deployed in harsh or unattended environments. MANET communicates with the thousands of mobile nodes to each neighborhood wireless links in a wireless state and less infrastructure environment [23]. The network is more vulnerable to attacks that are a wide range. Bandwidth constraints, scalability, wireless links, lack of centralized management, and limited resources [22]. MANETs are prone to various vulnerabilities and both passive and active attacks by malicious nodes due to dynamic topology. Here, the problem of identifying and prevention of black hole attack for effective utilization of network resources are addressed. In most of the cases, a dynamic network makes it simple for mobile nodes to move, disconnect from, or reconnect to it [5, 19, 24] without any restrictions. Every node performs the role of a router and manages a routing method for communications between networks. Therefore, node security plays an important part in MANET [8]. Concerning the proposed work, each node authentication is achieved before initiating the route discovery process.

The important components of a security mechanism are Confidentiality, Integrity, and Availability (CIA). As stated in literatures, the fundamental problem of security is authentication [6, 16]. In wired networks, the concept of issuing certificates, public key management are adopted for node authentication. Therefore, it clearly represents the need for common centralized servers which are capable of handling processes like certificate generation, renewal, and revocation. Sadasivam and Yang [16] used X.509 certificates for handling public key infrastructure. The overall process is a divergence for ad hoc networks due to the restricted centralized management system and infrastructure-less network.

In addition, the dynamic topology and mobility of the nodes cause link failures, which leads to re-authenticate the node and makes it communicate periodically with the certificate server / authority. Based on the discussion, all the drawbacks are taken into consideration and the proposed methodology is carefully designed. The proposed work contains algorithms to detect the malicious node using a fuzzy-based analyzer and ensure secure communication between the nodes using Certificate Authority (CA).

The structure of the proposed work is as follows: Section 2 depicts the existing algorithms and methods in the related work and discusses the black hole attack identification. Section 3 deals with detecting the black hole attack. Section 4 discusses the required simulation parameters. Section 5 depicts the simulation results. Section 6 describes the proposed methodology's conclusion and future scope of research.

2. Related Work

In most of the literature, the node's trust value is mainly concentrated to attain higher security in the network. Pirzada and McDonald [14] provided a pure trust model that calculates trust by monitoring the data delivery in the network. The value of the trust ranges from -1 to +1 and is evaluated by considering the direct communication among the nodes. The trust value is changed periodically and reduced to negative when more failures occur in the network. Thachil and Shet [21] proposed the MANET-based associative approach that enables Ad hoc On-Demand Distance Vector (AODV) protocol for the black hole attack identification. It is achieved by comparing the trust threshold value, which is used for trust value manipulation periodically. When the trust value exceeds the node-based threshold value, it is referred to be a malicious attack. Later, Option based trust model is proposed by Macedo *et al*. [10] that calculates trust at different levels in the network. The nodes available in the network identifies the trustworthiness of other nodes as they behave in a promiscuous manner. The trust model calculates the direct trust-based nodes' opinion and the indirect trust-based opinion of other nodes, where some nodes act as supervisor nodes. These supervisor nodes behave maliciously in certain period of time.

Holland and Hellaby [7] a novel trust-based approach uses fuzzy logic to enhance the secure communication among the nodes using quantifiable trust values. These trust values are used in finding the secure route during the route discovery process. Kumar *et al*. [9] provided a Node Transition Probability (NTP) routing algorithm determines the routes using a control packet. NTP along with fuzzy logic effectively adapts to frequent changes in the routing table. Banerjee *et al*. [2] provides the trust value-based AODV protocol that involves three fuzzy logic-based membership functions like PI membership function triangular membership function, and Gaussian membership function. A better throughput was achieved by calculating the trust value based on multi-criterion decision-making.

Madhurya *et al*. [11] using a cryptographic algorithm, encrypts the data packets for ensuring security. In this technique, a shared decision-making system is designed as Disturbance Detection System (DDS) where data exchange in the network is carried out using multiple threshold values. To identify the attackers Singh *et al*. [18] proposed the trust management approach by using Elliptic Curve Cryptography (ECC) algorithm. This method eliminates the malicious nodes and detects three different attacks namely dropping attack during the selective packet, flooding attack, and black hole attack. Shams and Rizaner [17] stated the SVM-based IDS detects network attacks and is capable of high detection accuracy in eliminating malicious nodes. When the numbers of malicious nodes get to increase, the decrement of Packet Delivery Ratio (PDR) significantly in the system. Abdullah *et al*. [1] provided enhanced-AODV uses numerous routing metrics throughout the route discovery process to overcome network lifetime, higher stability, and reliability in MANETs.

The discussed literature review helps to detect several techniques that help the black hole attack identification and prevention. The main contributions of the proposed work are as follows:

- Trust managers used to find the trust value, message integrity value, and energy level of the nodes to ensure the node is trustable.
- CA to ensure secure packet transmission among the nodes
- Fuzzy rule descriptor to predict whether the node is normal or malicious which in turn ensures node trustworthy/node authentication.

The key objective of the proposed work mainly concentrates on the node authentication before enabling the route discovery process in MANETs. In this work, a fuzzy inference system is designed for black hole attack identification, which depends on node authentication, trust values, CA, energy level, and message integrity.

3. Proposed Work

Figure 1 shows the architecture of the proposed work. It consists of four phases Trust Manager, CA, node authentication, and fuzzy inference system. The trust manager aids in managing to determine the trust value based on the trust agent's direct observation. The trust is initially determined by considering the successful packet transfer between the nodes. By using three parameters-battery level, trust value, and message integrity value-the final trust manager provides a summary of the trust value. Finally, the CA chooses the high trust value-based mobile node.

The CA manages to issue a certificate to the requested nodes based on the fuzzy analysis. Simultaneously, the fuzzy inference system calculates the trustworthiness of the nodes based on the inference rules that are categorized as "normal node" and "malicious node". Based on the fuzzy output, the normal node will be provided with the certificate for routing by the CA.

When the node declared by the fuzzy analysis is found to be malicious, the CA will not revoke or issue a certificate to the requested node and CA will alert by sending an alarm to the other network nodes. Thereby, the overall process uses malicious node detection that

causes a black hole attack and intercepts it from being part of secured routing. The integration between the CA and fuzzy analysis helps to categorize the nodes effectively and identify the malicious node. Table 1 shows the trust value reference to specify the node is normal or malicious node.

Table 1. Trust value reference.

Trust index	Trust rating	Trust range (value)
1	No Trust	0.0 to 0.20
2	Poor Trust	0.21 to 0.40
3	Fair Trust	0.41 to 0.60
4	Good Trust	0.61 to 0.80
5	Full Trust	0.81 to 1

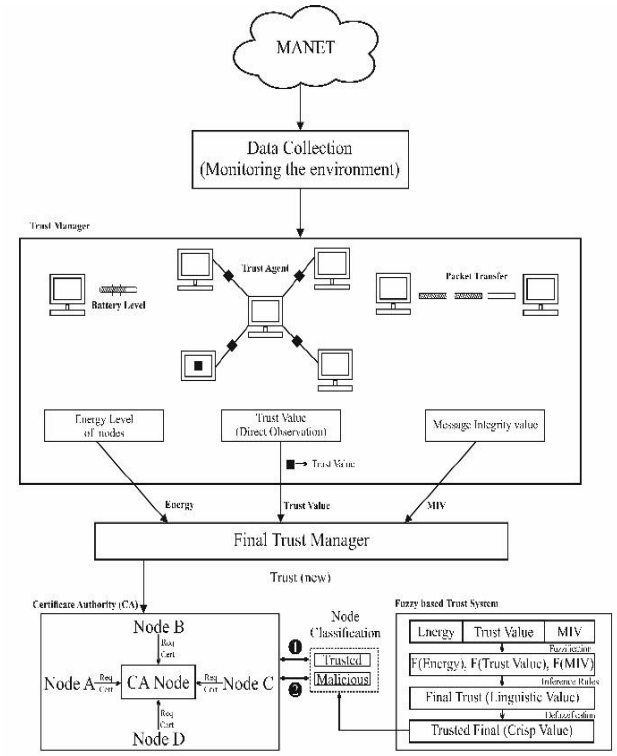

Figure 1. System architecture.

3.1. Trust Value Calculation

Firstly, the trust manager finds the trust value among the nodes by direct neighbor nodes observation. The trust value refers to the successful packet sent and received from a particular node. Figure 2 considering the network, each node stores the neighbor nodes with the trust value depending on the trust value table, sample instance of Node is shown in Table 2. It considers only the packet transmission between the nodes and therefore, the trust value. Node *A* calculates the trust value of node *B* as given in Equation (1),

$$Trust_{AB} = \frac{(P_s)_A}{(P_r)_B} \quad (1)$$

Node ID	Source	Destination	Packet sent	Packets Received	Packets Dropped	Trust Value

Figure 2. Trust table format.

Table 2. Trust table for smple instance of node.

Trusted node	Malicious node	Trusted node
1	0.12	1
0	224	0
512	32	1024
512	256	1024
5	127	243
1	32	112
12	78	124

Here, $Trust_{AB}$ referred as the estimated trust value of node *A* on node *B*. $(P_s)_A$ denotes the successfully sent packet from node *A* and $(P_r)_B$ is the overall successful received packets by node *B*. *I* it has a Source node List (SL) that keeps track of the packet's origin for forwarding. The number of information packets that have already been forwarded to reliable network nodes is denoted by the term Forwarded Packet (F). When Node A discovers that Node B has successfully received the packet that has already been forwarded, Node B's 'To Forwarding (TF)' is incremented by 1. Algorithm (1) shows packet transmission.

Algorithm 1: Packet Transmission

Input: Source Node List, Node Trust Value, $(P_s)_A$, $(P_r)_B$
Output: Malicious Node with Trust Value
Step 1: If $[(F)_{node\ B}$ *and SL]*
Step 2: $(F)_{node\ B}{}^{++}$;
Step 3: $(TF)_{node\ B}{}^{++}$;
Step 4: $(F)_{node\ B} \geq Threshold\ Limit$
Step 5: Else calculate $Trust_{AB} = \frac{(P_s)_A}{(P_r)_B}$ *// New Trust Value Calculation*
Step 6: Declare Malicious Node.

In a black hole attack, the normal node promotes the reliable path from the source to the target path rather than forcing each packet to be examined individually, which leaves it vulnerable to producing false information. As a result, the packet transmission format and suggested technique assist the malicious node in identifying the bogus information. Figure 3 shows the identifying blockhole attack and dropping remaining packets.

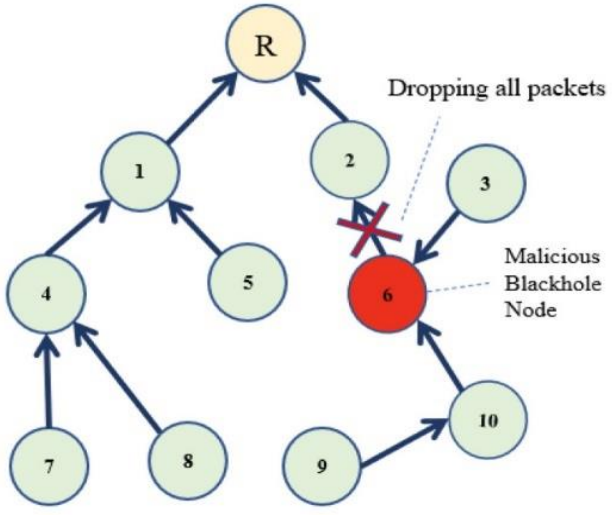

Figure 3. Dropping all packets.

In wireless Ad-hoc networks, the energy resource is crucial for stable node behaviour. The availability of constrained resources when nodes behave egoistically without packet forwarding and the power saver implemented in the battery to immediate nodes are the causes of this. The level of energy of the nodes that are monitored periodically [4], for sending and receiving the data and packets control, which helps to the consumed energy. Each node-based trust value that is worked as energy (node) gets to effect the battery as a result of the sent and received packets. Each node monitors the behaviour of each neighbour node to determine whether any packets are forwarded or dropped in the network, in accordance with the watchdog method. The trust manager verifies the neighbouring nodes by enabling communication for detecting network packets such as drop, forward, and delay.

3.2. Calculation of Message Integrity Value (MIV)

The identified packet is deleted once the neighbour node modifies the identified message's content, maintaining the integrity of the packet. The node's data integrity value, $MIV_{(node)}$, is initially positive and indicates whether any packets have been requested for modification by the node. The node's $MIV_{(node)}$ value is then decreased.

According to its key and the hop count field's exception, each node gives information in the form of a digital signature. To access the network, each node and the hop count enable reduced malicious network in terms of hop count metric in the request of information packets the get too concerned the hop count metric and the hash chains gets [13].

Each node initially verifies the validity of the information it receives, by monitoring the content of digital signatures. It decrypts the public key by originating the information, which is equivalent to the receiving packets field. In this method, if a middle node or malicious node examines the information content to discover changes by getting the information of the next node, the packet is deleted and its MIV $_{(node)}$ is decreased. To hash the packet, the MD4 algorithm is used as it consumes less energy.

3.3. Final Trust Value Calculation

The final trust manager has solicited the target node's final trust value evaluation based on the energy level, values of information integrity, and trust values. According to the calculated results, the final trust value is evaluated, and also found the timeout value [12]. The overall final trust value is calculated using in Equation (2).

$$Trust_{(new)}=Energy_{(node)} + TrustValue_{(old)} + MIV_{(node)} \quad (2)$$

where,

$$Energy_{(node)}=\frac{\sum(PR+PF+BP)}{Node_{iton}} \quad (3)$$

Here, *PR*, *PF*, and *BP* represent the packet received, packet forwarded and battery power respectively. The number of nodes in the network ranges "from *i* to *n*" in a particular route. Whenever the final trust manager is solicited by the CA, refinds the trust value and updates the $Trust_{(new)}$ to the CA.

3.4. Certificate Authority (CA)

The election algorithm used by the CA helps to choose the node with the best trust value as applied in [20]. The other nodes in the network might request the CA node to provide certificates in order to exchange data. Figure 4 shows the steps involved in secured communication and the process of nodes eligibility. The certificates will expire after a period of time and the nodes will be allowed to renew if it is trusted node. By this process the trust manager is able to differentiate the malicious node from the trust nodes in the network. The certificate authority authentication algorithm is depicted as in Algorithm (2).

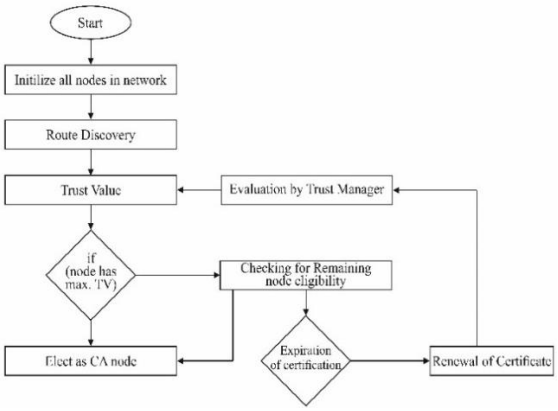

Figure 4. Election of CA.

Algorithm 2: Election of Certificate Authority

Step 1: Initially generate the shared keys of the node $(S.Key)_S$
Step 2: The source node initiates the communication and request CA to provide

$$\left[S, Req\left(S_{ID}, D_{ID,} Trust_{(new)}\right)\right]_{(s,key)_s}$$

Step 3: CA decrypts S.Req and obtains the S_{ID} *in the ID Repository*
Step 4: CA checks $if\ (S_{ID} = ID\ repository)$ *then CA checks* $D_{ID,}$ *is in its range*
Step 5: If $(D_{ID} = range)$ *go to step 7*
Step 6: Else Initiate communication again
Step 7: Generate $(P.Key)_s$, $(Pr.Key)_s$, $(P.Key)_d$, $(Pr.Key)_d$,$(S.Key)_d$
Step 8: The certificate authority, therefore, provides a certificate as,

$$Certificate\ A = [\ S_{ID}, (P.Key)_s, (Pr.Key)_s, Trust_{AB}, Trust_{(new)}\ ]$$

Step 9: CA sends E [(Certificate A) $S.Key_s$*] to the source node*
Step10: CA sends E [(Certificate B) $S.Key_d$*] to the destination node*
Step 11: Else Quit or Stop.

The main role of the CA node is as follows:

1. It ensures secure transmission between the nodes.
2. The eligible nodes for packet transmission are elected by a CA (CA node).
3. When the CA node is out of communication, another node with the highest trust value is elected as the CA node.

The replacement of CA's is used to save the single point failure when the node moves out of range in the MANET which prevents the security bottleneck. The nodes communicate with each other whenever the issued certificate is valid.

3.5. Node Authentication using Fuzzy-Based Analyzer

The increases in the reliable nodes that enabled its trust values, when the trust values illustrate the constructive way, and the reliable nodes get reduced when the trust level illustrates the pessimistic concern. Fuzzy logic has trust values ranging from 0 to 1 as in [3, 15].

In the proposed system, Figure 5 shows the fuzzy approach structure with four inputs and one output. In the fuzzy structure, the Direct Trust of node (DT(u)), nodes Energy Value (EV(u)), nodes Trust Value (TV(u)), and Message Integrity Value of the node (MIV(u)) is referred as input to the fuzzified action approach and the output is the defuzzification enabled node type (crisp). By concern, the Rule base builds the crisp inputs into the inference engine brings the input. The several methods in the inference engine enable the results to depend on the network limitation that is specified and stored in the rule base.

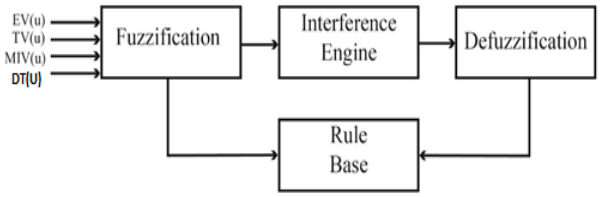

Figure 5. Fuzzy design approach.

Table 3 the rule base is used for the node selection with the higher(u) value in the trustable node and it will be issued with a certificate-by-CA. Finally, the selected node acts as the next forwarder to reach the destination. The membership functions consist of 5 stages Very Low (VL), Low (L), Medium (M), High (H), and Very High (VH) to obtain the output N(u).

Table 3. Fuzzy discrimination.

Fuzzy level	Trust value	Output
		Normal (trusted) node/Malicious node
Very Low	0 to 0.2	Malicious
Low	0.2 to 0.4	Malicious
Medium	0.4 to 0.6	Trusted
High	0.6 to 0.8	Trusted
Very high	0.8 to 1	Trusted

The fuzzy rule base is formulated of IF-THEN, depending on the decisions that get taken. DT(u), EV(u), TV(u), and MIV(u) are the generated fuzzy values by the fuzzification method, which are gets from the inference engine. Therefore, by considering the specified if-then rules, the inference engine acts as fuzzy input based on non-linear mapping of the rule base and generates fuzzy outputs that are similar results. The rule formation and in-between metrics function that has functioned in the AND operation as shown below.

- IF DT(u) is VH AND EV(u) is VH AND TV(u) is VH AND MIV(u) is VH THEN N(u) is VH.
- IF DT(u) is VL AND EV(u) is VL AND TV(u) is VL AND MIV(u) is VL THEN N(u) is VL.
- IF DT(u) is VL AND EV(u) is L AND TV(u) is L AND MIV(u) is L THEN N(u) is L.

The above is the sample fuzzy rule, likewise, the combination of 256 rules was used to find the fuzzy outputs. The fuzzified values are given to the inference engine output that map using fuzzy rules and generated the fuzzy results. For example, to consider from the table, the inference engine learns that if the higher DT(u), higher EV(u), higher TV(u), and higher MIV(u).

Next, the highly trusted node is referred to as the 'Trusted Node'. There are available multiple defuzzification methods, but the usual and helpful defuzzification method is the center of gravity. However, the defusing action performed by the center of gravity, which is defined as Equation (4),

$$N(u)=\frac{\sum_{i=1}^{n} u_i * c}{\sum_{i=1}^{n} c_i} \quad (4)$$

where u_i is the rule base output. c_i is the center of the membership function output.

4. Simulation Parameters

The simulation is done through the NS-2, with varying network speeds. Table 4 represents the network scenario for simulation.

Table 4. Simulation parameter.

Parameters	Value
Area	500m × 500m
Routing Protocol	AODV
Data rate	5 pks/s
Packet Size	64 bytes
Number of nodes	20, 30, 40, 50
Simulation time	600ms
Traffic	CBR
Transmission Range	250m
Node speed	2 ms

5. Results and Discussion

The performance of CA with fuzzy approach was evaluated and compared with AODV with black hole attack and normal AODV depending on PDR, throughput, detection ratio of malicious node, and the end-to-end delay. The performance analysis describes

the number of nodes clustered as 20, 30, 40, 50, and 60 and the malicious nodes as 5, 10, 15, 20, and 25 respectively.

5.1. Throughput

It is defined as the number of bytes transferred/received per second, which is described as T_h in Equation (5).

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i} \quad (5)$$

where the total amount of data b_i that the destination receives them from the source divided by the time t_i it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by t, Figure 6 shows the proposed method performance CA with the fuzzy approach. From the graph, one can observe that the maximum throughput of 82% is given by CA with the fuzzy approach when the number of nodes is 20. Figure 6 shows the performance of throughput with proposed and existing system.

5.2. End-to-End Delay

From source to the destination, end-to-end delay is defined as the time needed to send and receive information packets. It is denoted by d_i. It can be calculated by the difference between the received time of the packet and the sent time of the packet in Equation (6).

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pkdtd_i} \quad (6)$$

where d_i is the end-to-end delay average n is the number of the node.

Figure 7 illustrates the proposed method performance CA with the fuzzy approach. From the graph, one can observe 38% of end-to-end delay CA with the fuzzy approach when the number of nodes is 60. Figure 7 performance of end-to-end delay with proposed and existing system.

5.3. Packet Delivery Ratio

The PDR is the number of successfully delivered packets to the destination node. It is denoted by PD_R. It can be calculated by the ratio of the received packet by the destination node and the source node sending the packets in Equation (7).

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i} \quad (7)$$

Here, $pktd_i$ is the number of packets received by the destination node in the *ith* application, and $pkts_i$ is the number of packets sent by the source node in the *ith* application. The average PDR of the application traffic n, which is denoted by PDR. Figure 8 illustrates the performance of PDR with proposed method and existing method. From Figure 8, one can observe that the PDR of 82% is given by CA with the fuzzy approach when the number of nodes is 60.

5.4. Detection Ratio/Dropped Packets

Detection ratio/dropped packets are the number of failed packets to attain the destination node sent by the sender node. It is denoted by D_r. It can evaluate by the variation among the total number of sent and received information packets in Equation (8).

$$D_r = \sum_{i=1}^{n}(N_i^S - N_i^T) - \sum_{i=1}^{n} N_i^S \quad (8)$$

where D_r is the detection ratio and n is the number of nodes, N^T is the average node received by the receiver and N^S is the average node sent by the sender. Figure 9 shows the performance of detection ratio with proposed method and existing method. From the graph, one can observe that the detection ratio of 42% is given by CA with the fuzzy approach when the number of nodes is 60.

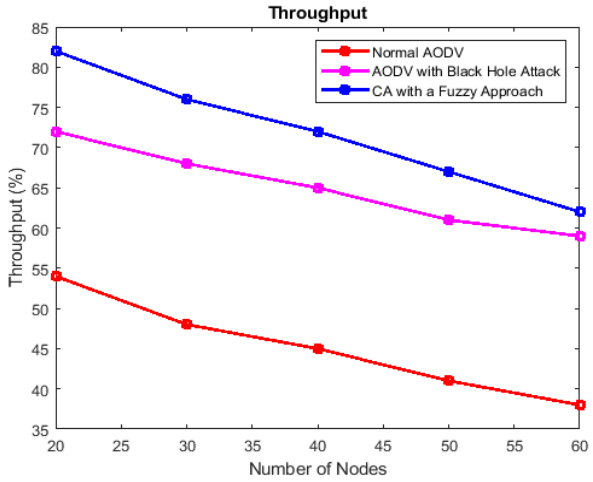

Figure 6. Throughput performance comparison.

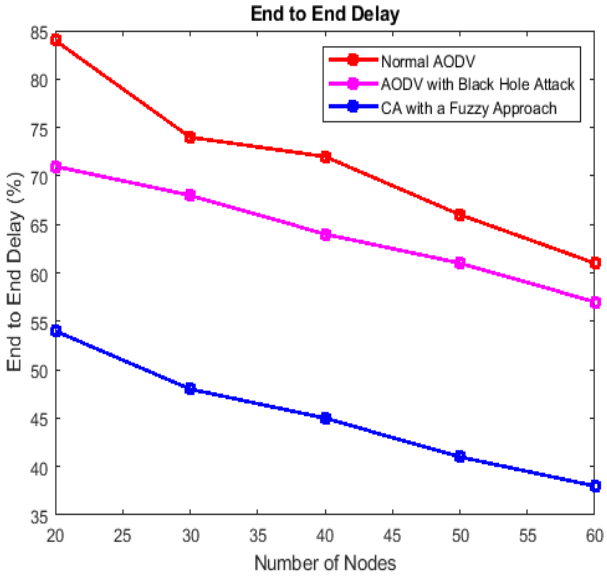

Figure 7. End to end delay performance comparison.

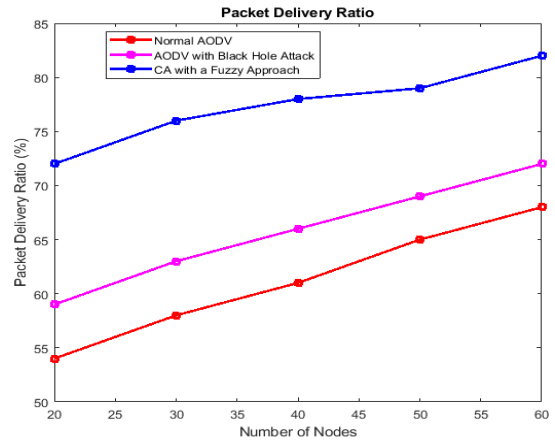

Figure 8. PDR performance comparison.

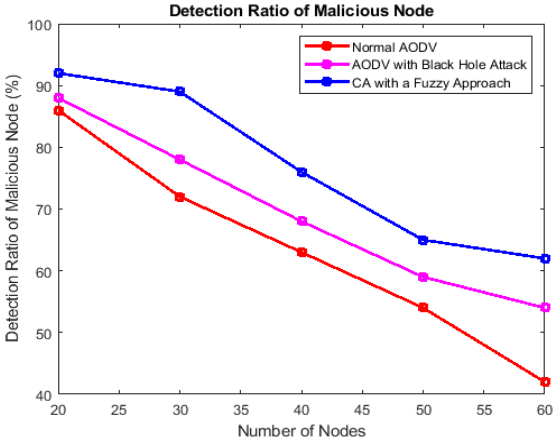

Figure 9. Detection ratio of malicious node performance comparison.

6. Conclusions

Fuzzy inference system design detects the black hole attack depending on the node authentication, CA, message integrity, energy level, and trust value. The proposed work mainly concentrates on node authentication before commencing the route discovery process in MANETs used to remove the black hole attack. A fuzzy inference system shows better performance by providing certificates only to the trusted nodes. The performance of the proposed work CA with fuzzy approach was evaluated with the existing methods like AODV and normal AODV with black hole attack based on end-to-end delay, throughput, detection ratio of malicious node, and PDR. The CA-enabled proposed work with a fuzzy approach provides better throughput, end-to-end delay, PDR, and malicious node detection when compared with other existing techniques. Though there is an enhanced malicious node detection results, the identification ratio of the proposed work is improved by 20% than other works.

References

[1] Abdullah A., Ozen E., and Bayramoglu H., "Enhanced-AODV Routing Protocol to Improve Route Stability of MANETs," *The International Arab Journal of Information Technology*, vol. 19, no. 5, pp. 736-746, 2022. https://doi.org/10.34028/iajit/19/5/5

[2] Banerjee P., Paulchoudhury J., and Chaudhuri S., "Fuzzy Membership Function in a Trust Based AODV for MANET," *International Journal of Computer Network and Information Security*, vol. 5, no. 12, pp. 27-34, 2013. DOI:10.5815/ijcnis.2013.12.04

[3] Boukrim M. and Antari J., "Improvement of Packet Transmission Scheduling and Delivery Rate in Wireless Ad-hoc Networks," *Physical Communication*, vol. 52, pp. 101707, 2022. https://doi.org/10.1016/j.phycom.2022.101707

[4] Chen Z., Tian L., and Lin C., "Trust Evaluation Model of Cloud User Based on Behavior Data," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, pp. 1-10, 2018. https://doi.org/10.1177/1550147718776924

[5] Dromard J., Khatoun R., and Khoukhi L., "A Watchdog Extension Scheme Considering Packet Loss for a Reputation System in Wireless Mesh Network," *in Proceedings of the 20th International Conference on Telecommunications*, Casablanca, pp. 1-5, 2013. DOI:10.1109/ICTEL.2013.6632124

[6] Farahani G., "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks," *Security and Communication Networks*, vol. 2021, pp. 1-5, 2021. https://doi.org/10.1155/2021/8814141

[7] Hallani H. and Hellany A., "Wireless Ad-hoc Networks: Using Fuzzy Trust Approach to Improve Security between Nodes," *in Proceedings of the International Conference on Computer Engineering and Systems*, Cairo, pp. 359-365, 2009. DOI:10.1109/ICCES.2009.5383241

[8] Jain S. and Khuteta A., "Detecting and Overcoming Blackhole Attack in Mobile Adhoc Network," *in Proceedings of the International Conference on Green Computing and Internet of Things*, Greater Noida, pp. 225-229, 2015. DOI:10.1109/ICGCIoT.2015.7380462

[9] Kumar S., Narender M., and Ramesh G., "Security Provision for Mobile Ad-Hoc Networks Using NTP and Fuzzy Logic Techniques," *Global Journal of Computer Science and Technology*, vol. 10, no. 8, pp. 62-67, 2010. file:///C:/Users/user/Downloads/SecurityProvisionForMobileAd-HocNetworksUsingNtpFuzzyLogicTechniques.pdf

[10] Macedo D., Dos Santos A., Nogueira J., and Pujolle G., "A Distributed Information Repository for Autonomic Context-Aware MANETs," *IEEE Transactions on Network and Service*

Management, vol. 6, no. 1, pp. 45-55, 2009. DOI:10.1109/TNSM.2009.090304

[11] Madhurya M., Krishna B., and Subhashini T., "Implementation of Enhanced Security Algorithms in Mobile Ad Hoc Networks," *International Journal of Computer Network and Information Security*, vol. 6, no. 2, pp. 30-37, 2014. DOI:10.5815/ijcnis.2014.02.05

[12] Mo L., "Research on Trust Calculation Mechanism of Wireless Sensor Network of Internet of Things," *in Proceedings of the 3rd International Conference on Automation, Mechanical Control and Computational Engineering*, Dalian, pp. 23-28, 2018. DOI:10.2991/amcce-18.2018.5

[13] Najjar M., "New Technique to Insure Data Integrity for Archival Files Storage (DIFCS)," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 2, pp. 44-49, 2014. DOI:10.14569/IJACSA.2014.050207

[14] Pirzada A. and McDonald C., "Establishing Trust in Pure Ad-Hoc Networks," *in Proceedings of the 27th Australasian Conference on Computer Science*, vol. 26, pp. 47-54, Dunedin, 2004. https://dl.acm.org/doi/pdf/10.5555/979922.979929

[15] Preetha V. and Chitra K., "Fuzzy Based Analysis for Efficient Clustering in MANET and Security Enhancement Approach using Neural Network," *International Journal of Intelligent Computing Research*, vol. 7, no. 2, pp. 706-710, 2016.

[16] Sadasivam K. and Yang T., "Evaluation of Certificate-Based Authentication in Mobile Ad Hoc Networks," *in Proceedings of the International Conference on Networks and Communication Systems*, Krabi, pp. 183-464, 2005. http://www.actapress.com/Abstract.aspx?paperId=19905

[17] Shams E. and Rizaner A., "A Novel Support Vector Machine Based Intrusion Detection System for Mobile Ad Hoc Networks," *Wireless Networks*, vol. 24, no. 5, pp. 1821-1829, 2018. DOI:10.1007/s11276-016-1439-0

[18] Singh O., Singh J., and Singh R., "Multi-Level Trust Based Intelligence Intrusion Detection System to Detect the Malicious Nodes Using Elliptic Curve Cryptography in MANET," *Cluster Computing*, vol. 21, no. 1, pp. 51-63, 2018. DOI:10.1007/s10586-017-0927-z

[19] Srinivas T. and Manivannan S., "Black Hole and Selective Forwarding Attack Detection and Prevention in IoT in Health Care Sector: Hybrid Meta-Heuristic-Based Shortest Path Routing," *Journal of Ambient Intelligence and Smart Environments*, vol. 13, no. 2, pp. 133-156, 2021. https://doi.org/10.3233/AIS-210591

[20] Tanwar S. and Kumar A., "Extended Design and Implementation of Certificate Authorities," *International Journal of Security and its Applications*, vol. 11, no. 8, pp. 13-26, 2017. https://article.nadiapub.com/IJSIA/vol11_no8/2.pdf

[21] Thachil F. and Shet K., "A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET," *in Proceedings of the International Conference on Computing Sciences*, Phagwara, pp. 281-285, 2012. DOI:10.1109/ICCS.2012.7

[22] Vij A. and Sharma V., "Security Issues in Mobile Adhoc Network: A Survey Paper," *in Proceedings of the International Conference on Computing, Communication and Automation*, Greater Noida, pp. 561-566, 2016. DOI:10.1109/CCAA.2016.7813784

[23] Wu B., Chen J., Wu J., and Cardei M., *Signals and Communication Technology*, Springer, 2007. https://doi.org/10.1007/978-0-387-33112-6_5

[24] Younas S., Rehman F., Maqsood T., Mustafa S., Akhunzada A., and Gani A., "Collaborative Detection of Black Hole and Gray Hole Attacks for Secure Data Communication in VANETs," *Applied Sciences*, vol. 12, no. 23, pp. 12448, 2022. https://doi.org/10.3390/app122312448

Elamparithi Pandian working as Assistant Professor in the Department of Computer Science and Engineering at AAA College of Engineering and Technology, Sivakasi. He graduated in Bachelor of Engineering in Computer Science and Engineering at Arulmigu Kalasalingam College of Engineering, Srivilliputhur, affiliated to Anna University Chennai, Tamilnadu, India. He secured Master of Engineering in Computer Science and Engineering at Mepco Schlenk Engineering College, Sivakasi affiliated to under Anna University Chennai, Tamilnadu, India. He secured Ph.D., in Computer Science and Engineering at Anna University, Chennai, Tamilnadu, India. He is in teaching profession for more than 12 years. He has presented 15 papers in National and International Journals, Conference and Symposiums. His main area of interest includes Wireless Networks, Artificial Intelligence and Internet of Things.

Ruba Soundar received the A.M.I.E., degree in Computer Science and Engineering from The Institution of Engineers (India) in 2000. He received the M.E., and Ph.D., degrees in Computer Science and Engineering from Anna University, Chennai in the year 2004 and 2010 respectively. Currently he is Senior Associate Professor in Computer Science and Engineering Department of Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India. He has authored/coauthored over 100 research articles in various Journals and Conferences in the areas of Cloud Computing, Image Processing, Wireless and Wired Networking.

Shenbagalakshmi Gunasekaran working as Assistant Professor in the Department of Computer Science and Engineering at Mepco Schlenk Engineering College, Sivakasi. She graduated in Bachelor of Technology in Information Technology at Arulmigu Kalasalingam College of Engineering, Srivilliputhur affiliated to Anna University Chennai, Tamilnadu, India. She secured Master of Engineering in Computer Science and Engineering at Mepco Schlenk Engineering College, Sivakasi affiliated to under Anna University Chennai, Tamilnadu, India. She pursued Ph.D., in Computer Science and Engineering at Anna University, Chennai, Tamilnadu, India. She is in teaching profession for more than 2 years. She has presented 12 papers in National and International Journals, Conference and Symposiums. Her main area of interest includes Wireless Sensor Network, Internet of Things and Soft Computing.

Shenbagarajan Anantharajan working as Assistant Professor (Senior Grade) in the Department of Artificial Intelligence and Data Science at Mepco Schlenk Engineering College, Sivakasi. He graduated in Bachelor of Engineering in Electrical and Electronics Engineering at P.S.R. Engineering College, Sivakasi affiliated to Anna University Chennai, Tamilnadu, India. He secured Master of Engineering in Computer Science and Engineering at National Engineering College, Kovilpatti affiliated to under Anna University Chennai, Tamilnadu, India. He secured Ph.D., in Computer Science and Engineering at Annamalai University, Chidambaram, Tamilnadu, India. He is in teaching profession for more than 13 years. He has presented 34 papers in National and International Journals, Conference and Symposiums. His main area of interest includes Artificial Intelligence, Internet of Things and Soft Computing.