Volume 1, 2025, Pages 61-71 *Journal of Computer and Communication Networks*
| Regular Article | Open Access

Routing and MAC Layer based Framework for Secure and Reliable Communication in Mobile Ad Hoc Networks

Lyingluo Wang
Department of Mechanical Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, P.R. China.
wangluo@mail.xjtu.edu.cn

Zhu Jiping
Department of Modern Mechanics, University of Science and Technology of China, Hefei, Anhui province, China.
jipingmech@ustc.edu.cn

Article Info
Journal of Computer and Communication Networks
https://www.ansispublications.com/jccn /jccn.html

Received 18 January 2025
Revised from 28 February 2025
Accepted 25 March 2025
Available online 24 April 2025
Published by Ansis Publications

https://doi.org/10.64026/JCCN/2025007

Corresponding author(s):
Lyingluo Wang**,** Department of Mechanical Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, P.R. China.
Email: wangluo@mail.xjtu.edu.cn

Abstract – The research outlines three novel methods of detecting malicious nodes, which include Cumulative Frequency Detection, Data Forwarding Behaviors Detection, and MAC-based Authentication. These algorithms are used in ensuring reliable security for the Mobile Ad hoc Networks (MANETs). The purpose of Cumulative Frequency Detection is to determine indications of activities as a DoS attack or a heavily loaded channel. This is achieved by adding the total number of clear to send (CTS) and request to send (RTS) packets relayed by the channel over a particular time interval. The Data Forwarding Behaviors Detection is a database-based trust values to find the relationship between forwarding nodes and to modify the routing algorithm based on it and exclude the suspicious or untrusted nodes. The MAC Based Authentication process uses the Message Authentication Codes (MACs) in the shared key cryptographic system to authenticate the request and the response. The issues that are associated with the unauthorized nodes may be resolved in line with the application of the above Combined Solution for Routing and MAC (CSRM) layer attacks, as explained in the paper. Therefore, there is less control overhead and low loss of packets during the transmission in wireless communication. This also improves the security aspects and makes a connection to another MANET irrespective of the hostile, dynamic and unpredictable nature of the network environment.

Keywords – Mobile Ad Hoc Networks (MANETs), Combined Solution for Routing and MAC Layer (CSRM), Message Authentication Codes (MACs), Denial of Service (DoS), Clear to Send (CTS), Request to Send (RTS).

I. INTRODUCTION

Ad hoc networks are a specific form of network that is used in circumstances such as conflicts (e.g. warfare) and natural catastrophes (e.g. earthquakes). Nodes may exhibit diverse topologies based on their interconnections. The effortless installation of these networks is attributed to the nodes' self-configuring nature, eliminating the need for any infrastructure to be established. A Mobile Ad hoc Network (MANET) is a decentralized network, which operates without a centralized infrastructure [1] (see **Fig. 1**). Centralized security management becomes challenging due to its reliance on security measures implemented by individual mobile nodes [2]. When designing safe ad hoc wireless networks, it is necessary to consider the components in **Table 1**.

Among the key considerations, which can interfere with the major operation of various networks, is the security for an ad hoc wireless network. It is therefore important to address all security concerns so as to guarantee the integrity, confidentiality and availability of data as well as services in a network. Ad hoc wireless networks have numerous security risks and are susceptible to attacks due to their features like the absence of centralized administration & monitoring, cooperative algorithms, lack of specified defensive mechanisms, open medium, dynamic topological changes etc. Ad hoc wireless networks eliminate the need for a central authority by allowing nodes to communicate with each other through trust. This renders them more prone to an attack as compared to other network types. In addition, wireless links in ad hoc networks

establish weak spots that can be exploited by intruders who can penetrate the system and gain access to real-time communication data [12, 13, 14]. Active participation in the network is possible for mobile nodes because they are situated within reach of wireless connectivity as well as ability to overhear information.

Table 1. Components of a Safe Ad Hoc Wireless Network

Component	Description	Literature
Vulnerabilities	The security level between wireline communication and wireless communication is different because attackers can easily eavesdrop and spoof the latter without any physical barrier.	[3, 4]
Infrastructure	MANETs cannot utilize security mechanisms that consist of specific secure parts with assigned functions such as key servers and trusted third parties due to absence of infrastructure.	[5, 6, 7, 8]
Requirements for cooperation	In a decentralized system, common nodes of the network perform basic network functions and services. Therefore, if there are hostile or intrusive nodes, or if nodes do not cooperate with each other, routing integrity is compromised.	[9, 10, 11]

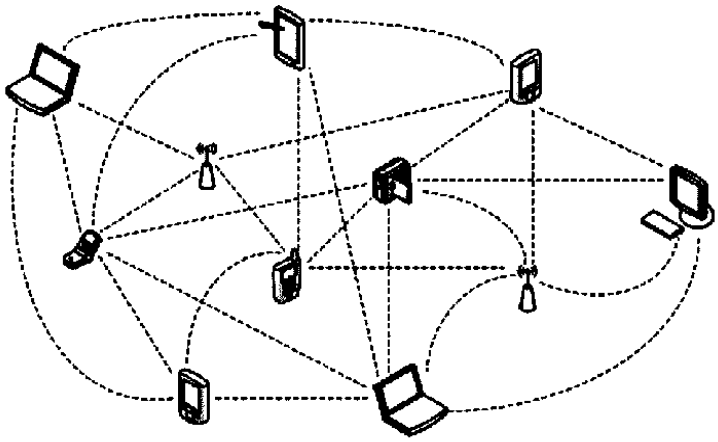

Fig 1. Mobile Ad Hoc Network Architecture (MANET).

The frequent attacks on these networks have made security a significant concern. Nevertheless, users have been more cautious in recent times. To effectively provide safer communication and transmission in ad hoc wireless networks, designers must possess knowledge of various forms of attacks and their corresponding repercussions. Ad hoc wireless networks are vulnerable to several forms of attacks, including Denial of Service (DOS) attacks, impersonation attacks, black hole attacks, flooding attacks, selfish node misbehavior, and routing table overflow attacks.

The article focuses on the direct need to enhance communication security and reliability in MANETs, which are susceptible to several security threats because of their distributed nature as well as dynamism. The study aims at minimizing negative impacts caused by malicious nodes as well as enhancing general network performance. In doing so, three novel methods are introduced, which include MAC-based Authentication, Data Forwarding Behavior Detection, and Cumulative Frequency Detection. The solution put forward improves upon current methods for ensuring trustworthy communications within MANETs, which take into account their dynamic settings when considering various security concerns.

The rest of the research is arranged in the following manner: Section II presents a review of relevant research concepts, such as MANETs and Denial of Service (DoS) attacks in MANETs. The literature related to this study is reviewed in Section III. Section IV describes the materials and methods used for conducting this research. Section V provides an appraisal of the findings and simulation results, including those based on attackers as well as node count. Section VI discusses in detail the key concepts and methods such as effectiveness of CSRM, simulation results, data forwarding behavior-based detection method, cumulative frequency-based detection method and MAC-based authentication. Lastly, Section VII presents a summary to the research and proposes future research towards enhancing communication reliability and security in MANETs.

II. OVERVIEW OF CONCEPTS

Mobile Ad-Hoc Network (MANET)

MANET refers to a wireless communication and networking system that consists of two or more devices known as nodes [15]. These nodes do not need a central administrator to communicate with each other. Also, they can create an immediate network between them and communicate even when there is no fixed network infrastructure available. The rapid growth of computer communications has been observed by many people in this century than any other period due to the increased advancement in wireless communication technology and computers. Such a wireless network, which comprises of nodes

that directly transmit data packets among themselves without relying on any infrastructure is termed as MANET. The network has limited bandwidth and is dynamically structured.

Personal Digital Assistants (PDAs), computers, MP3 players, digital cameras, and cell phones are some of the devices that can be used as nodes. The nodes are located inside their respective accessible areas and are capable of establishing direct communications with each other, as seen in **Fig. 2**. Singlehop ad hop networks are the most basic kind of ad hoc networks, where the various nodes are within each range. This allows individual nodes to interact directly with each other, without the need for any intermediary nodes. The nodes are not required to be in a single position, but they have to stay within the dimension of the various nodes. This implies that the complete network might move together as a group without impacting communications networks.

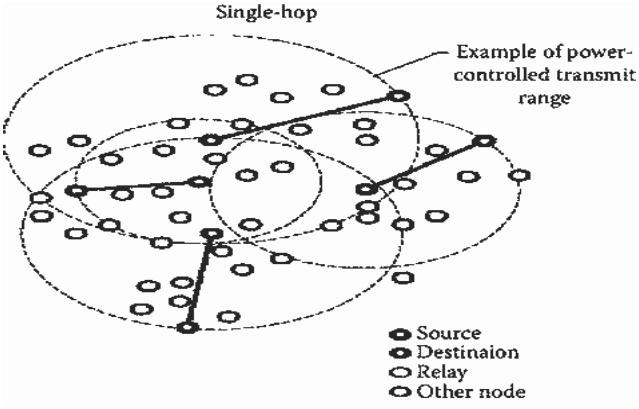

Fig 2. Single-Hop Ad Hoc Network.

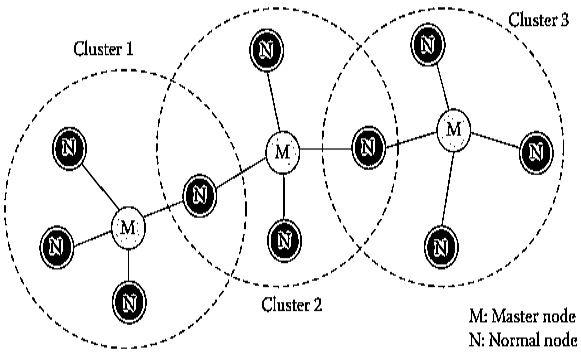

Fig 3. Hierarchical Ad Hoc Networks.

On the other hand, hierarchical ad hoc networks are composed of many clusters, with each cluster representing a separate network. These clusters are interconnected, as indicated in **Fig. 3**. The nodes in these networks may be classified into two distinct types as shown in **Table 2**.

Table 2. Nodes in Hierarchical Ad Hoc Networks

Node	Description
Master nodes	These nodes oversee the cluster and distribution of data to the other nodes in the cluster.
Normal nodes	These nodes, also known as slave nodes, communicate directly with each other within the clusters and with the nodes available in other clusters, with the assistance of master nodes.

DoS Attacks in MANETs

The layered networks reference models indicate that MANETs are susceptible to DoS attacks at both the network and link layers. A DoS attack is categorized as a connection layer attack when it is carried out by exploiting threats in data-linked layer protocols. For instance, a malevolent person might exploit an IEEE 802.11 binary exponential back-off approach to obstruct nearby devices from accessing the wireless channel [16]. There are three specific forms of DoS threats that focus on the network layer: attacks that interfere with routing, attacks that interfere with forwarding, and attacks that aim to consume network resources. These attacks take advantage of the threats within the network layer protocols. Examples of such attacks include wormholes (Rushing) [17], black holes [18] that disrupt routing, jellyfish that abuse directional antennas [19], dynamic power abusing attacks that disrupt forwarding, control packet floods [20], and packet injection attacks [21] that use resources. A DoS attack is an occurrence, which eliminates or reduces the capacity of the network to effectively perform its projected function.

The existing link layer protocol utilized for MANETs is IEEE 802.11 Medium Access Control (MAC) protocol that is susceptible to DoS attacks [22]. In [23], the authors have examined the susceptibility of IEEE 802.11 MAC to DoS threats that employ the method known as binary exponential back-off. When a node continually sends data, it dominates the channel because the successful transmission causes a smaller contention window for other nodes who must keep going off. Solution to this problem is through adoption of modified back-off approach as suggested in [24] whereby receiver decides when to back-off. Also observed was the fact that RTS/CTS frames are susceptible to DoS attacks due to some additions regarding NAV (net allocation vector) field. A small number of bits transmitted by one malicious actor with minimal energy can disrupt ongoing link-layer frames. This node has knowledge of how long the current transmission will last in its vicinity. After conducting extensive research, it was revealed that using LDPC (low density parity codes) for binary modulation) technique is the most efficient way of combating DoS attack.

Three common DoS attacks on the network layer are forwarding denial, routing drop-off, and resource exhaustion. A malevolent node can issue some additional data and control packets into a network as part of a resource starvation attack. For example, in MANET that employs the AODV (Ad hoc On-Demand Distance Vector) routing protocol, an evil node may periodically send multiple RREQ (Route Request) messages to its neighbors. An attacker who is able to change sequence

numbers or tamper with destination addresses for every transmission can convince his neighbors that bogus requests are legitimate ones. Consequently, these entities must keep forwarding those messages towards their immediate neighbors and beyond. The local nodes near this malicious one will be forced to expend significant resources e.g., CPU cycles, battery power, and bandwidth just to process these deceptive signals when they freely come from these neighboring nodes. In [25], a modified upgrade of this attack was described, where malicious nodes consistently start the queries of route discovery at a reduced rate, whereas disregarding any responses it receives.

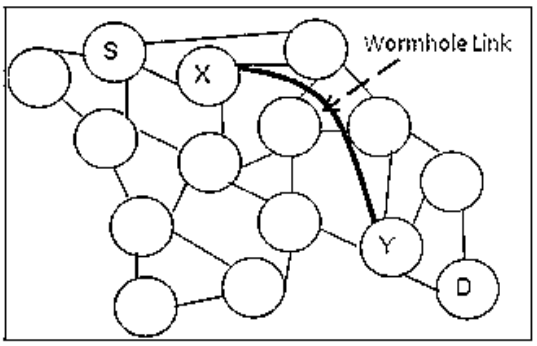

Fig 4. Wormhole Attacks.

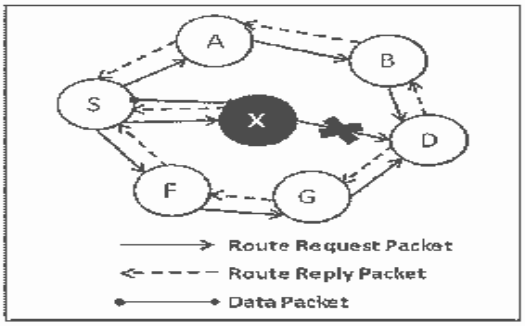

Fig 5. Blackhole Attacks.

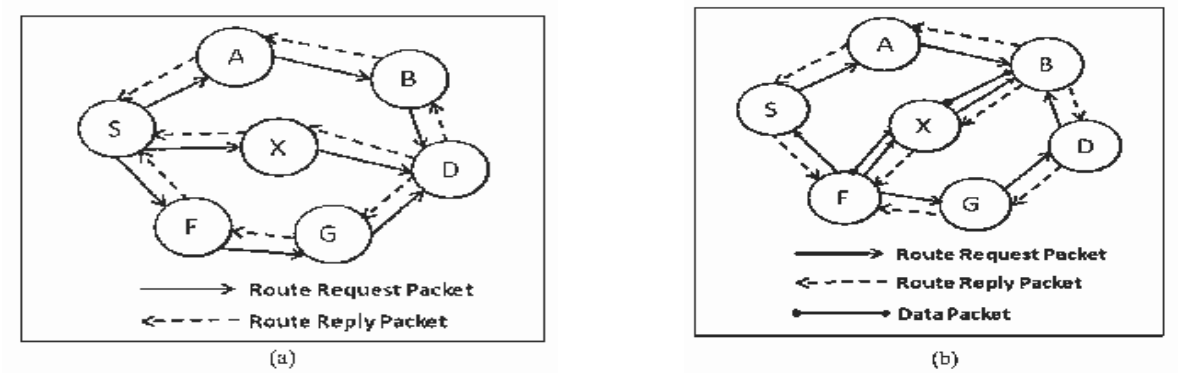

Fig 6. Grayhole Attacks.

The simulation findings shown in [26] demonstrate that the malicious control packet flooding attack has a detrimental impact on the performance of the network. In addition to the control packets flooding attacks, malevolent node may also engage in the injection of a substantial volume of spurious data packet into the route, with the intention of depleting the resources of intermediate routing nodes. The attack mentioned in [27] was analyzed, and a mechanism named SAF was suggested to address it. SAF is a hop-by-hop and on-demand source authentication protocol designed to neutralize this attack.

Fig. 4 illustrate the occurrence of a Wormhole attack on the MANET, initiated by two hostile nodes named X and Y. There is a Wormhole connection with a high speed that connects nodes D and S, allowing traffic to be tunneled between X and Y. When S wants to interact with D, it usually requires numerous intermediate steps for a packet to be sent between them. When worms Y and X are around, D and S begin to believe that they are next to one other. **Fig. 5** illustrates an instance of a Blackhole attack against the AODV protocol. Assume that source S wants to establish communication with node D. S begins the route discovery procedure by transmitting RREQ (route request) packets to its neighboring nodes. The destination (D) node or any intermediary nodes with a recently established path to the destination may respond by sending a RREP (route reply) packet to S. Since there are no intermediary nodes with a new path to D, they send RREQ packets directly to the target. Since X is a malevolent node, it intentionally does not pass on the request packet to the next node. Instead, it deceitfully responds to S by claiming to have a legitimate and up-to-date route to D.

Fig. 6(a) depicts a MANET employing the AODV protocol. Initially, Node X functions as a regular node and passes various packets from source (S) to a particle destination (D) node. Subsequently, as seen in **Fig. 6(b)** Node X exhibits malicious behavior by intentionally discarding packets transferred from S to D. After a certain period, X resumes its function as a regular node, just as before. As a result, X acts maliciously for a certain amount of time. Because AODV lacks security measures, malicious nodes might carry out a variety of attacks by ignoring the protocol limitations.

III. RELATED WORKS

The dynamic and decentralized structure of MANETs presents a major obstacle to secure communication and rogue node prevention, according to Singh et al. [28]. Security, as a concept, has been approached differently by various scholars with

most of them focusing on how to prevent attacks on the MAC layer and routing. This paper focuses on a comprehensive approach that simultaneously identifies and eliminates all forms of threats using three different methodologies at once.

According to Yu, Zhou, and Su [29], there are three steps that aim to reduce routing and mac layer attacks. These three processes are based on detecting the cumulative frequency, identified according to its data forwarding behaviors, and identified using MAC authentication. Detection technique uses a measure of how often each frame is sent across to detect possible intrusion at the built-in MAC layer. By analyzing such parameters as receiving RTS packets, CTS packets and other indications, channel activity detection looking for retransmissions or congestion is able to reveal anomalies like denial of service (DoS) attacks or even channel congestion. As described in [30], this technique consists in comparing thresholds for different states derived from MAC layer events happening during discovery process. Medium Access Control (MAC) Layer is used by MANETs to ensure fair and efficient distribution of wireless medium. Nevertheless, the dynamic nature of this level exposes it to DoS attacks through channel congestions due its inherent self-configuration and self-organization property. Scholars have suggested several methods of detecting using cumulative frequencies as a base point.

The researchers have allocated trust levels to their nodes on the basis of the frequency of packet forwarding with a view to making data transmission more dynamic. The Internal Tables (IT) enable packets to be delivered and received, so that nodes can change their trust level accordingly. This technique alters the reliability values, inserts route request (REQ) packets, identifies and penalizes external organizations' neighboring devices in order to guarantee route reliability. Veeraiah et al. [31] developed the most effective protocols for data transmission in MANETs taking into account trust related criteria. This technique aims at increasing security and dependability of packet forwarding. Trust-based protocols in this case allow nodes to assess the reliability of their neighbors' forwarding actions and modify routing decisions so as not to use those dangerous or untrustworthy nodes. Trust values are essential since they assign different priorities for packets depending on how good they are at transmitting information across the network. Such an approach protects against any attempts at forging or tampering with routing information.

The metrics we use in evaluating the effectiveness of this article are control overhead, packet drop ratio, packet delivery ratio, and end-to-end delays. We evaluate our methodology by simulating it using Network Simulator (NS2). A comparison was made between our CSRM solution that involves a combination of routing and MAC layer attack prevention with a popular method known as Packet Droppers (PD). This is compared to other common methods used for routing and MAC layer attacks. This clearly shows how this new approach can be used to minimize or mitigate against the harmful effects of bad nodes. Nevertheless, one should also bear in mind that there might exist other equally good options too. The CSRM system delivered more packets than PD program but less losses were experienced. Thus, wider control overheads should be accompanied by some security measures else wise they could lead into danger themselves as well.

IV. MATERIALS AND METHODS

We employed three techniques to detect any nodes, which are behaving unusually at the same time. (see **Table 3** below). To effectively reserve a channel, nodes transmit Clear to Send (CTS) and Request To transmit (RTS) packets that specify the desired time duration for channel reservation. These are targeted by DoS intruders to achieve full control of it or overwhelm it with fraudulent packets. Status data from the MAC layer was employed, as described by Bianchi [32], to identify and detect DoS attacks: Frequency of receiving Clear to Send (CTS) and Request to Send (RTS) packets, frequency of detecting busy channels, retransmissions number for data packets and RTS, and round trip durations for CTS and RTS packets. Every status corresponds to a certain step of the RTS/CTS packet process. During the first stage, if the number of TS/RTS packets exceeds a threshold value OV_{th}, it suggests that there is a high concentration of nodes within the range of transmission within the channel. When the channel becomes too crowded, a node in the backoff phase will halt counting Channel Passages (CP). If the duration of the stop exceeds the maximum sensing threshold, denoted as U_{th}, it indicates that there is a greater number of nodes inside the interference range.

Table 3. Methodologies Used in The Study

Methodology	Description	Literature
Detection approach based on cumulative frequency	To identify MAC layer attacks, we use a detection approach based on cumulative frequency.	[33]
Data forwarding behavior	To identify packet losses at the routing layer.	[34, 35, 36]
MAC-based authentication mechanism	To modify packets at the routing layer.	[37, 38]

When the number of retransmissions exceeds the threshold value RT_{th} during the retransmission period, it will be classified as channel congestion. In the last phase, the sender and receiver may calculate the TT (Time Taken) to carry out one consecutive transmission as well as reception of the CTS-RTS handshake. A total of TT seconds is needed for the RTS frame's transmission from the source to the recipient and the CTS frame's acknowledgement transmission. The detection system may be implemented with little extra resources as these status variables are present in the protocol stack. Nodes will assign a Channel Busy (CB) Bit to each data packet after evaluating the following criteria during the response stage:

$$\text{If RTS/CTS packets is} > OV_{th} \quad (1)$$

$$\text{If Stime is} > U_{th} \tag{2}$$

$$\text{If RTS/DATA retransmission is} > RT_{th} \tag{3}$$

$$T_{T_M} - T_{T_{s-r}} - T_{T_{m-s}} = T_T \tag{4}$$

The variable $T_{T_{s-r}}$ represents the duration it takes for a real-time streaming (RTS) frame to go from the sender to the server. $T_{T_{m-s}}$ is the duration it takes for a real-time streaming (RTS) frame to go from the transmitter to the receiver. The variable T_{T_M} represents the duration of an RTS-CTS handshake between receivers and senders, as perceived by server.

The rate data used to alter the flow is derived from the CB value. While bad nodes could exploit other malicious nodes, they do not impact the rate themselves. The following is a method for identifying data forwarding behavior: for each destination D and source S, let $\{TV_1, TV_2,...\}$ stand for the first trust ratings of the nodes $\{N_1, N_2,...\}$. Internal Table (IT) on every node transforms the trust value based on packets it receives. When everything is just starting off, the nodes have no idea how reliable their neighbors are. Source S communicates with nearby nodes by sending Route Request (REQ) packets when it wishes to transport packets to node D. In the first instance of receiving the RREQ packet, an intermediary node determines the total number of packets received over its channel. It sends a TV back to the preceding node if it receives packets from that node correctly. We consider N_x and N_y, two intermediate nodes, where N_x relays the message to Ny. The trust value of node N_x is increased every time node N_y obtains packets from node N_x.

$$TV_x = TV_x + 1, x = 1, 2 \tag{5}$$

Subsequently, the information technology (IT) of N_y is updated with TV_x values. In a same manner, information transfer (IT) is calculated independently by each node, and packets finally arrive at destination D. A technique known as "MAC-based authentication" uses a device's MAC address to confirm its authenticity. We employ a Secure On demand Routing (SOR) system [39] to build an authentication method based on a MAC. The source generates a MAC using sharable keys between the destination and source (MS) and calculates the C_{maci} (cumulative MAC) employing the shareable key between the destination and source via MS. Each source in this system transmits a request packet (REQ) containing the Destination id (D_{id}), sequential source Number (Ns), Source id (S_{id}), and a MAC. Shareable keys of the source as well as the intermediary nodes' shared key are appended to the C_{maci}, modifying it. The cumulative addition of C_{maci} is continuously accumulated and held until it gets to the respective destination, alongside the node for b_t (backward transmission).

Upon arrival at node D, the legitimacy and currency of the requested information is checked. Upon successful verification of the Message Sequence (MS), the system proceeds to transmit a Rep to its initial hop. This Rep contains an incrementing and distinct N_{rep} (reply number) as well as a MAC. The MAC is generated by shared keys between the destination (D) and the source (S), and is based on cumulative MAC and N_{rep} from the received Request (Req). During the transmission procedure from D-S, each intermediary entity performs a series of actions include checking the Rep, verifying the information, and recording it. The structure of the reply and request packets produced or sent by intermediate node I is defined by equations (6) and (7). Microsoft allows the recipient to proactively identify and reject duplicate requests at an early stage without responding to them:

$$REQi = \{REQ, S_{id}, D_{id}, N_s, MS, C_{maci}\} \tag{6}$$

$$REPi = \{REP, S_{id}, D_{id}, N_s, N_d, Nd, PathList, C_{maci-d}\} \tag{7}$$

When a node fails to transfer its packet, either because of node misbehavior or node failure, Err (error packets) are created and sent to nodes. The Err comprises the N_{err} (error node) identifier, the NN_{id} (identifier of the next node), the S_{id} (source identifier), and the MAC error (M_{err}):

$$Err = \{Err, NN_{id}, S_{id}, M_{err}\} \tag{8}$$

In order to prevent hostile nodes from transmitting false Err packets, MAC employs a shared key between N_{err} and S for protection. Upon receiving an Err, the source verifies the validity of the error and notifies the source of the state of the nodes.

V. RESULTS

Simulation Findings

Parameters and Simulation Model

To put our suggested algorithm through its paces, we use Network Simulator (NS2). The mobile hosts' channel capacities are all set to 2 Mbps in our scenario. **Fig. 7** shows that C++ and OTcl (Object-oriented Tool Command Language) are the two standard languages that make up NS2. Configuring and assembling the items and planning discrete occurrences are all

done by OTcl to set up simulation, whereas C++ describes the underlying approach (backend) of simulation items. Using TclCL, the C++ and OTcl are connected.

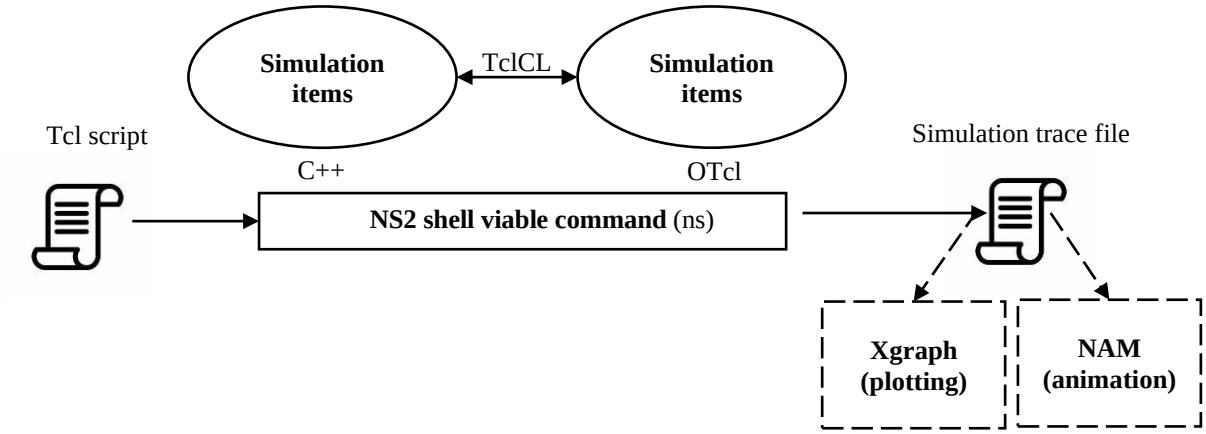

Fig 7. Basic Architecture of NS.

We implement the media access control layer according to the IEEE 802.11 standard for wireless LANs, which include the DCF (Distributed Coordination Function). For MAC, the IEEE 802.11 WLAN standard—which Wi-Fi is a part of—primarily employs the DCF. In addition to CSMA/CA (carrier-sense multiple accessibility with collision avoidance), DCF employs the binary exponential backoff approach. Stations that use DCF must listen for channel states during DIFS intervals before they may transmit. The station applies a broadcast delay during the DIFS (Distributed Inter-Frame Space) interval if it detects that the channel is in use.

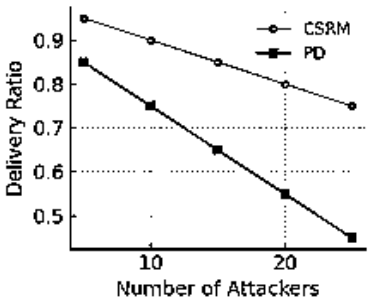

Fig 8. Attackers Vs Delivery Ratio.

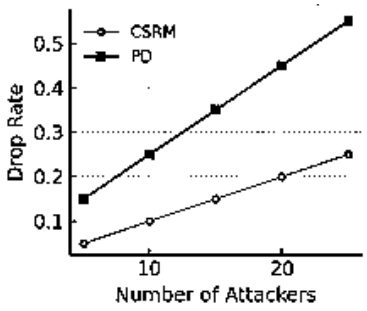

Fig 9. Attackers Vs Drop.

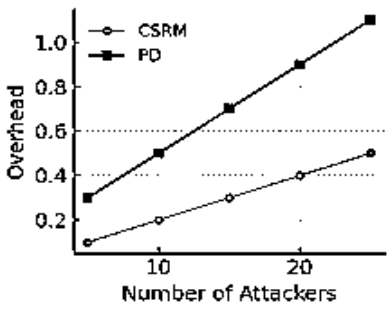

Fig 10. Attackers Vs Overhead.

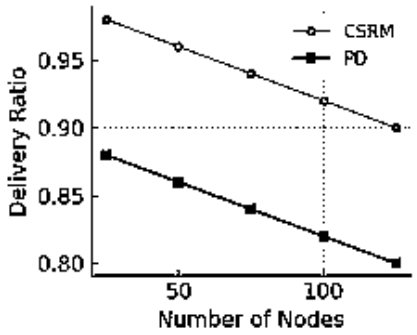

Fig 11. Nodes Vs Delivery Ratio.

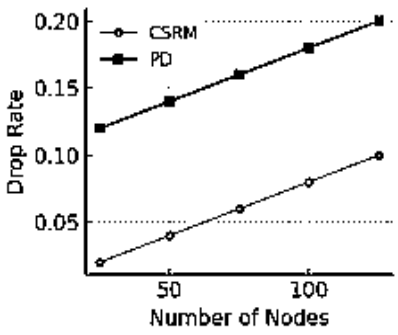

Fig 12. Nodes Vs Drop.

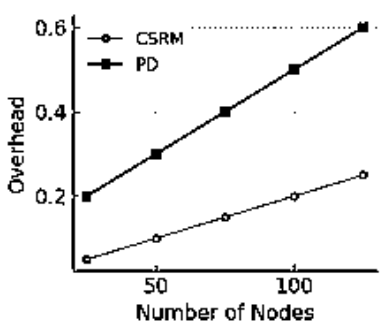

Fig 13. Nodes Vs Overhead.

Assuming there are several stations competing for the same wireless medium, if some of them see that the channel is in use and postpone their access, the other stations will almost certainly see that it is accessible and try to take it. Therefore, mishaps might happen. Furthermore, DCF requires a random backoff technique to avoid these collisions; this mechanism forces a station to postpone channel access for an extra duration. The 802.11 DCF protocol utilizes a substantial portion of available communication time, whereas the 802.11 control messages often carry little amounts of information. As an

example, the transmission of an ACK message requires a total period of 60 μs, which encompasses the necessary airtime to send 3240 bits at a rate of 54 Mbit/s. Within this timeframe, the ACK message carries just one bit of significant information.

The IEEE 802.11 standard integrates a PCF (point coordination function) as an optional access technique [40]. PCF enables the accessibility point that operates as a coordinator of the network, to oversee and control channel accessibility. The amendment of IEEE 802.11e improves the DCF and the PCF by introducing a novel coordination mechanism called the HCF (Hybrid Coordination Function) [41]. It is capable of informing the network layer about the occurrence of a connection breakdown. During our simulation, mobile nodes traverse a territory of 1000×1000 meters for a duration of 50 seconds. It is presumed that every node travels autonomously with an equal mean velocity.

Every node has an identical transmission dimension of 250 meters. Within our simulation, the velocity of the node is 10 meters per second. The traffic simulation is using a CBR (Constant Bit Rate) model. The settings of simulation and variables are outlined in **Table 4**.

Table 4. Simulation Settings

Misbehaving nodes	**5, 10, 15, 20, 25**
Speed	10 m sec^{-1}
Size of packet	512
Traffic source	CBR
Simulation period	50 sec
Radio range	250 m
Mac	802.11
Size of area	1000 by 1000
Nodes	25, 50, …. 125

Packet Delivery Ratio, Performance Measures, Packet Drop, Mean End-to-End Delays, and Control Overhead

We primarily assess performance based on the specific indicators. The control overhead is quantified as the proportion of the overall amount of routing control signals to the general quantity of transferred information packets. When calculating the average end-to-end latency, various packets of data that made it from their origins to their destinations are considered. As a percentage of all packets transmitted, the "packet delivery ratio" measures how many packets were successfully received. The metric shows the mean packet numbers ignored by the nodes that are not operating properly. The simulation findings included a comparison between our CSRM scheme and the Packet Droppers (PD) method [42] in the context of an adversarial node environment.

According to Attackers

In the initial experiment, we manipulate the quantity of assailants, ranging from 5 to 25, inside a network consisting of 100 nodes. **Fig. 8** displays the outcome of the mean ratio of packet delivery as the quantity of misbehaving nodes rises. **Fig. 9** displays the outcome of the average rate of packet loss as the quantity of misbehaving nodes rises. As the quantity of misbehaving nodes rises, **Fig. 10** illustrates the control overhead outcome for the strategies. Based on the findings, it is evident that the CSRM scheme exhibits a notably reduced packet loss rate, minimized overhead, and higher delivery ratio compared to the PD scheme. Its improved security features against MAC and Routing layer attacks are responsible for this.

According to the Quantity of Nodes

For the initial experiment, the quantity of nodes from 25 to 75 to 100 to 125 was considered while maintaining a constant number of attackers at 10. Results of the mean packet delivery ratio with increasing quantity of nodes are indicated in **Fig. 11**. As the nodes rises, **Fig. 12** depicts the mean results of packet drops. As the quantity of nodes rises, **Fig. 13** indicates the results of the control overhead for the systems. Results show that when comparing packet loss, delivery ratio, and overhead, the CSRM method clearly wins out over the PD scheme. This is because the CSRM technique has better protections against MAC and Routing layer attacks.

VI. DISCUSSION

The current study introduces a novel method for addressing MAC layer and routing attacks in MANETs. In our approach, we employ the three methods, which include cumulative frequency detection, MAC authentication, and data forwarding behavior detection. Cumulative frequency applies the RTS/CTS case together with Channel Busy (CB) bit to discover and figure out rogue nodes. To detect evil nodes, an innovative technique has been developed that depends on incentives provided for information transmission. The worse a node's performance in achieving its rewards is, the more malicious its behavior gets. MAC-based authentication determines the error bit that identifies either dormant or faulty nodes. In this case, therefore, the research proposes a joint strategy that effectively minimizes packet loss/delay as well as enhancing packet delivery ratio by minimizing overheads. This study demonstrates this improvement through simulations. This paper discusses three new ways of recognizing and dealing with malfeasance in MANET such as: mac authentication; frequency aggregation; and action-based detection of data transfer. By using routing protocols which provide MAC level capabilities we can enhance communication security to some extent even though it's still limited due to its dynamic decentralized nature.

Cumulative Frequency-Based Detection Method

MANETs can be analyzed for security issues using the cumulative frequency technique as a substitute measure [43]. The system uses certain indicators such as the number of CTS and RTS packets, congestion in the channel among others to identify any abnormal behavior that could indicate malicious intent or systems failure. The major strength of this method is its ability to detect security vulnerabilities at an early stage. For instance, it keeps track on the number of RTS and CTS packets transferred by the system over time so that any deviation from normal transmission rates can always be recognized with accuracy. Some of these deviations might show either significantly higher or lower amounts of transmissions which are an indicator that may mark out initiation of DoS attacks and other forms of malice. Besides, it also finds areas with increased traffic by looking at channel activity indicators hence enabling it to ensure network slowdowns are minimized and performance remains optimal throughout.

Data Forwarding Behavior-Based Detection

Dynamic, flexible and dependability-based nodes' packet forwarding approach is used in MANETs [44, 45]. Traditional static models of trust are unable to rightly show node's changing behavior over time. Evaluative processes have been proposed in this paper that examine past operations, employ internal tables and confidence levels to modify routing decisions accordingly. The advantage of behavior-based detection systems for data forwarding is their ability to respond quickly to different network scenarios including other points as well. Avoidance of vulnerable or malicious nodes as routes thus changes the route selection at each level of trust for packet forwarding nodes based on established performance characteristics in this path.

MAC-Based Authentication

Securing communications within MANETs is highly reliant on MAC-Based Authentication [46]. It authenticates routing requests and responses. The method will make sure the network's passage does not break. Moreover, it also verifies where orders come from, if they are from authorized sources or not. MAC-Based Authentication is one of the methods of guaranteeing the cryptographic integrity of distributed communication which in turn increases the level of confidence in routing. This task entails confirmation of the validity of the routing queries and responses provided in the process of the routing. This way, through the usage of MAC addresses, it is possible to confirm the legitimacy of packets that come through the network. Sneak attacks in the network systems are efficiently prevented.

Simulation Results and Effectiveness of CSRM

The simulation results can provide a scientific basis on how CSRM can detect and eliminating malicious nodes in MANETs. Thus, in the real-world application of MANET, this strategy is useful in addressing various problems. The measure of performance for CSRM is the packets' delivery ratio that represents the packets ratio, which successfully reach their respective destination. In this case, the simulation outcomes shown that this system offered more successful packet delivery accomplishments in a consecutive manner than the other previous systems. This means that this technology may help even create reliable communication channels in the enemy territory. Hence, the applications which integrate the mobile ad hoc networks will have a better network performance due to the higher packet delivery ratio than other systems.

VII. CONCLUSION

This paper develops a comprehensive plan to counter the present-day security threats in MANETs. It aims to enhance security and reliability of information dissemination in complex and distributed environments. It also introduces three new techniques that enable the determination of the cumulative frequency based on data forwarding, behavior-based detection and MAC-based authentication. The proposed system takes advantage of MAC layer and routing protocols to self-detect occurrence of lost packets, malicious nodes, DoS attacks and other forms of threats. However, it describes measures that help to deal with these risks. Simulation results have shown that the proposed algorithm (Combined Solution for Routing and MAC layer attacks) is effective in countering the malicious nodes by minimizing the control overheads while at the same time increasing the packet delivery ratios, and decreasing the loss rates. Furthermore, this strategy may be considered as vital for constructing safe and reliable communication over different networks of actual MANETs. Moreover, it has impressive flexibility, performance, and accommodation in different working conditions. However, there is a need for further research to optimize the proposed solutions for the scale of the problem and protect them from complex attacks, as well as to perform usability tests in real-world settings. This future research will help in determining real implementation and operational functioning of MANET systems.

CRediT Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Lyingluo Wang and Zhu Jiping; **Methodology:** Lyingluo Wang; **Software:** Zhu Jiping; **Writing-Original Draft Preparation:** Lyingluo Wang and Zhu Jiping; **Visualization:** Lyingluo Wang and Zhu Jiping; **Investigation:** Lyingluo Wang and Zhu Jiping; **Supervision:** Zhu Jiping; **Writing-Reviewing and Editing:** Lyingluo Wang and Zhu Jiping; All authors reviewed the results and approved the final version of the manuscript.

Data Availability
The datasets generated during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interests
The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding
No funding was received for conducting this research.

Competing Interests
The authors declare no competing interests.

References
[1]. A. Konak, G. E. Buchert, and J. Juro, "A flocking-based approach to maintain connectivity in mobile wireless ad hoc networks," Applied Soft Computing, vol. 13, no. 2, pp. 1284–1291, Feb. 2013, doi: 10.1016/j.asoc.2012.10.020.
[2]. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/j.comnet.2012.12.018.
[3]. P.-W. Yau and C. J. Mitchell, "Security Vulnerabilities in Ad Hoc Networks," CORE, Jan. 2003, [Online]. Available: http://www.chrismitchell.net/sviahn.pdf
[4]. N. Raj, P. Bharti, and S. Thakur, "Vulnerabilities, Challenges and Threats in Securing Mobile Ad-Hoc Network," 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 771–775, Apr. 2015, doi: 10.1109/csnt.2015.101.
[5]. A. Zemlianov and Gustavo de Veciana, "Capacity of ad hoc wireless networks with infrastructure support," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 657–667, Mar. 2005, doi: 10.1109/jsac.2004.842536.
[6]. Jiancong Chen, Shejie Li, S.-H. G. Chan, and Jingyi He, "WIANI: wireless infrastructure and ad-hoc network integration," IEEE International Conference on Communications, 2005. ICC 2005. 2005, vol. 5, pp. 3623–3627, doi: 10.1109/icc.2005.1495092.
[7]. D. M. Shila and Yu Cheng, "Ad hoc wireless networks meet the infrastructure: Mobility, capacity and delay," 2012 Proceedings IEEE INFOCOM, pp. 3031–3035, Mar. 2012, doi: 10.1109/infcom.2012.6195753.
[8]. P. Sakarindr and N. Ansari, "Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 5, pp. 8–20, Oct. 2007, doi: 10.1109/mwc.2007.4396938.
[9]. Vikram Srinivasan, Pavan Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), pp. 808–817 vol.2, 2003, doi: 10.1109/infcom.2003.1208918.
[10]. V. Srinivasan, P. Nuggehalli, C.-F. Chiasserini, and R. R. Rao, "An analytical approach to the study of cooperation in wireless ad hoc networks," IEEE Transactions on Wireless Communications, vol. 4, no. 2, pp. 722–733, Mar. 2005, doi: 10.1109/twc.2004.842950.
[11]. M. Cardei, J. Wu, and S. Yang, "Topology control in ad hoc wireless networks using cooperative communication," IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 711–724, Jun. 2006, doi: 10.1109/tmc.2006.87.
[12]. S. Kumar and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges," Security and Communication Networks, vol. 9, no. 14, pp. 2484–2556, May 2016, doi: 10.1002/sec.1484.
[13]. K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," Journal of Systems Architecture, vol. 105, p. 101701, May 2020, doi: 10.1016/j.sysarc.2019.101701.
[14]. A. Abduvaliyev, A.-S. K. Pathan, Jianying Zhou, R. Roman, and Wai-Choong Wong, "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013, doi: 10.1109/surv.2012.121912.00006.
[15]. B. K. Tripathy, S. K. Jena, V. Reddy, S. Das, and S. K. Panda, "A novel communication framework between MANET and WSN in IoT based smart environment," International Journal of Information Technology, vol. 13, no. 3, pp. 921–931, Oct. 2020, doi: 10.1007/s41870-020-00520-x.
[16]. E. Garcia-Villegas, M. S. Afaqui, and E. Lopez-Aguilera, "A novel cheater and jammer detection scheme for IEEE 802.11-based wireless LANs," Computer Networks, vol. 86, pp. 40–56, Jul. 2015, doi: 10.1016/j.comnet.2015.05.003.
[17]. M. Meghdadi, S. Ozdemir, and I. Güler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks," IETE Technical Review, vol. 28, no. 2, p. 89, 2011, doi: 10.4103/0256-4602.78089.
[18]. M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile Ad Hoc networks," Proceedings of the 42nd annual Southeast regional conference, pp. 96–97, Apr. 2004, doi: 10.1145/986537.986560.
[19]. A. K. Ali, B. Sharma, and U. M. Sharma, "Impact Analysis of JellyFish Attack in MANETs," ADBU Journal of Engineering Technology, vol. 4, Mar. 2016, [Online]. Available: https://journals.dbuniversity.ac.in/ojs/index.php/AJET/article/download/172/181
[20]. S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," IEEE Wireless Communications and Networking Conference, 2005, vol. 4, pp. 2112–2117, doi: 10.1109/wcnc.2005.1424844.
[21]. S. Deng, X. Gao, Z. Lu, and X. Gao, "Packet Injection Attack and Its Defense in Software-Defined Networks," IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 695–705, Mar. 2018, doi: 10.1109/tifs.2017.2765506.
[22]. C. Alocious, H. Xiao, and B. Christianson, "Analysis of DoS attacks at MAC Layer in mobile adhoc networks," 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 811–816, Aug. 2015, doi: 10.1109/iwcmc.2015.7289187.
[23]. V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc networks," MILCOM 2002. Proceedings, vol. 2, pp. 1118–1123, doi: 10.1109/milcom.2002.1179634.
[24]. Z. Wang et al., "A 37-GHz Asymmetric Doherty Power Amplifier With 28-dBm P sat and 32% Back-Off PAE in 0.1-μm GaAs Process," IEEE Transactions on Microwave Theory and Techniques, vol. 70, no. 2, pp. 1391–1400, Feb. 2022, doi: 10.1109/tmtt.2021.3136510.
[25]. R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," International Journal of Communication Systems, vol. 30, no. 7, May 2016, doi: 10.1002/dac.3148.
[26]. Xiaobing Zhang, S. F. Wu, Zhi Fu, and Tsung-Li Wu, "Malicious packet dropping: how it might impact the TCP performance and how we can detect it," Proceedings 2000 International Conference on Network Protocols, pp. 263–272, doi: 10.1109/icnp.2000.896310.
[27]. R. Akbani, T. Korkmaz, and G. V. S. Raju, "HEAP: A packet authentication scheme for mobile ad hoc networks," Ad Hoc Networks, vol. 6, no. 7, pp. 1134–1150, Sep. 2008, doi: 10.1016/j.adhoc.2007.11.002.
[28]. S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," Sustainable Cities and Society, vol. 79, p. 103483, Apr. 2022, doi: 10.1016/j.scs.2021.103483.
[29]. Ming Yu, Mengchu Zhou, and Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449–460, Jan. 2009, doi: 10.1109/tvt.2008.923683.

[30]. H. Shokri-Ghadikolaei, C. Fischione, G. Fodor, P. Popovski, and M. Zorzi, "Millimeter Wave Cellular Networks: A MAC Layer Perspective," IEEE Transactions on Communications, vol. 63, no. 10, pp. 3437–3458, Oct. 2015, doi: 10.1109/tcomm.2015.2456093.
[31]. N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," IEEE Access, vol. 9, pp. 120996–121005, 2021, doi: 10.1109/access.2021.3108807.
[32]. G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," IEEE Journal on Selected Areas in Communications, vol. 18, no. 3, pp. 535–547, Mar. 2000, doi: 10.1109/49.840210.
[33]. J. Chen, M. Yan, F. Zhu, J. Xu, H. Li, and X. Sun, "Fatigue Driving Detection Method Based on Combination of BP Neural Network and Time Cumulative Effect," Sensors, vol. 22, no. 13, p. 4717, Jun. 2022, doi: 10.3390/s22134717.
[34]. N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Ad Hoc Networks, vol. 11, no. 4, pp. 1497–1509, Jun. 2013, doi: 10.1016/j.adhoc.2011.01.018.
[35]. Z. Xia, X. Mao, K. Gu, and W. Jia, "Two-Dimensional Behavior-Marker-Based Data Forwarding Incentive Scheme for Fog-Computing-Based SIoVs," IEEE Transactions on Computational Social Systems, vol. 9, no. 5, pp. 1406–1418, Oct. 2022, doi: 10.1109/tcss.2021.3129898.
[36]. J. Ni, X. Lin, and X. Shen, "Privacy-Preserving Data Forwarding in VANETs: A Personal-Social Behavior Based Approach," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–6, Dec. 2017, doi: 10.1109/glocom.2017.8254013.
[37]. D. Singh, B. Kumar, S. Singh, and S. Chand, "SMAC-AS: MAC Based Secure Authentication Scheme for Wireless Sensor Network," Wireless Personal Communications, vol. 107, no. 2, pp. 1289–1308, Apr. 2019, doi: 10.1007/s11277-019-06336-8.
[38]. H. Sikarwar and D. Das, "A Novel MAC-Based Authentication Scheme (NoMAS) for Internet of Vehicles (IoV)," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 5, pp. 4904–4916, May 2023, doi: 10.1109/tits.2023.3242291.
[39]. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne:," Proceedings of the 8th annual international conference on Mobile computing and networking - MobiCom '02, 2002, doi: 10.1145/570646.570648.
[40]. J. Alonso-Zárate, C. Crespo, Ch. Skianis, L. Alonso, and Ch. Verikoukis, "Distributed point coordination function for IEEE 802.11 wireless ad hoc networks," Ad Hoc Networks, vol. 10, no. 3, pp. 536–551, May 2012, doi: 10.1016/j.adhoc.2011.09.004.
[41]. T. D. Lagkas, D. G. Stratogiannis, and P. Chatzimisios, "Modeling and performance analysis of an alternative to IEEE 802.11e Hybrid Control Function," Telecommunication Systems, vol. 52, no. 4, pp. 1961–1976, Jun. 2011, doi: 10.1007/s11235-011-9477-5.
[42]. D. Djenouri and N. Badache, "On eliminating packet droppers in MANET: A modular solution," Ad Hoc Networks, vol. 7, no. 6, pp. 1243–1258, Aug. 2009, doi: 10.1016/j.adhoc.2008.11.003.
[43]. G. Liu, Z. Yan, and W. Pedrycz, "Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey," Journal of Network and Computer Applications, vol. 105, pp. 105–122, Mar. 2018, doi: 10.1016/j.jnca.2018.01.004.
[44]. D. Ergenç, L. Eksert, and E. Onur, "Dependability-based clustering in mobile ad-hoc networks," Ad Hoc Networks, vol. 93, p. 101926, Oct. 2019, doi: 10.1016/j.adhoc.2019.101926.
[45]. J. Guo et al., "ICRA: An Intelligent Clustering Routing Approach for UAV Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2447–2460, Feb. 2023, doi: 10.1109/tits.2022.3145857.
[46]. S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19–30, Jul. 2017, doi: 10.1016/j.vehcom.2017.02.001.

ISSN: 3080-7484