IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 June 2023, accepted 13 August 2023, date of publication 22 August 2023, date of current version 30 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3307394

RESEARCH ARTICLE

A Hybrid Approach Against Black Hole Attackers Using Dynamic Threshold Value and Node Credibility

S. LAKSHMI[1], E. A. MARY ANITA[2], (Senior Member, IEEE), AND J. JENEFA[2]
[1]Department of Information Technology, AMET University, Kanathur, Tamil Nadu 603112, India
[2]Department of Computer Science and Engineering, CHRIST (Deemed to be University), Bengaluru, Karnataka 560074, India

Corresponding author: J. Jenefa (jenefa.j@christuniversity.in)

ABSTRACT Detecting black hole attackers is tedious in Vehicular Ad Hoc Networks due to vehicles' high mobility. The main consequence faced because of these attackers is an increase in the number of dropped packets which converts secure and fastest paths to compromised ones. Since these attackers can act individually and collaboratively as a group, early detection of these attackers must be feasible to preserve the network's performance. The majority of current methods rely on predetermined threshold and trust score values, which are ineffective in accurately identifying black hole attackers. Hence, this paper proposes a hybrid approach using dynamic threshold value and node credibility for early detection of black hole attackers. RSUs periodically compute the dynamic threshold value and categorize the vehicles into categories 1, 2, and 3. Vehicles classified as Category 1 are legitimate, whereas Category 3 vehicles are attackers. Vehicles in Category 2 are suspicious, requiring further analysis using node credibility values to identify attackers. It is protected against single, multiple, and collaborative black hole attackers. The NS2 simulation results demonstrate that the suggested method is optimal concerning PDR, Throughput, Delay, and Packet Loss Ratio compared to recent techniques. Since the proposed scheme efficiently identifies the attackers, it has 89.67% PDR, which is higher when compared to other schemes.

INDEX TERMS Collaborative black hole attackers, multiple black hole attackers, single black hole attackers, trust values.

I. INTRODUCTION

Vehicles and other vehicular infrastructure can communicate through the VANETs [14]. It contributes to the development of autonomous vehicles which can send/receive Cooperative Aware Messages (CAM). Because of unique features like frequent disconnection, dynamic topology, and high mobility, VANETs are susceptible to various security attacks. Therefore, communications (Vehicle-to-Vehicle Communication, Vehicle-to-RSU Communication, and RSU-to-Vehicle Communication) must be provided safely in a vehicular environment to ensure security against attacks. VANETs pursue many preventive measures for the secure exchange of CAM and other warning messages to vehicles and Road Side Units (RSUs). The basic vehicular environment is illustrated in Figure 1. The different kinds of vehicular communications are also clearly highlighted in the given figure.

Vehicular communications are possible with the help of Application Units (AUs) and On-Board Units (OBUs) [15]. These units are mounted in the vehicles by the manufacturers. OBUs are responsible for exchanging CAM, routing packets in the fastest and most reliable route to the destination, congestion control, secure data transmission, etc. AUs are accountable for utilizing the applications provided by the service provider to perform various tasks as per the user's requirements. It also uses the OBU's capability to ensure communication with other vehicles/RSUs. These two units play a vital role in providing secure communications, which help in assisting drivers and reducing accidents by exchanging life-critical messages.

The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Mueen Uddin.

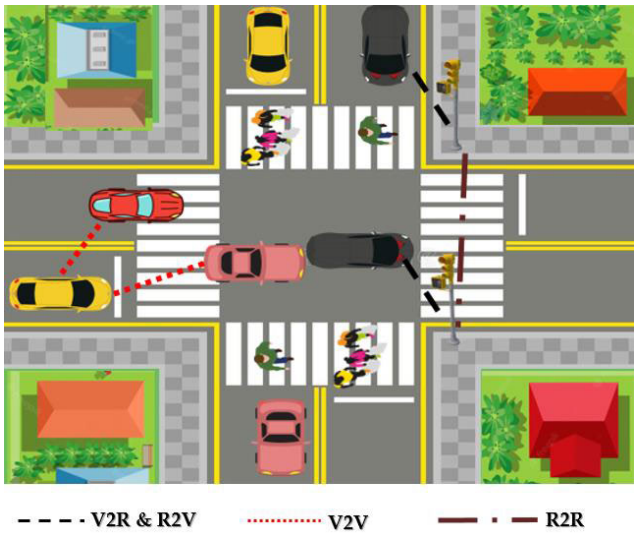

FIGURE 1. Basic VANET environment.

VANET is a sub-class of Mobile Adhoc NETwork (MANET) [16], and it extends all the features of MANET. Some shared features include an absence of infrastructure, dynamic topology, restriction in the communication range, etc. Since the vehicles cannot communicate long-range with other vehicles, they must depend on the intermediate vehicles to send and receive packets. Some of the unique features of VANET [19] are structured routes, high mobility, frequent disconnections, etc. Because of these unique characteristics, establishing secure communication in a vehicular environment is tedious. Since vehicles are mounted with OBUs, information like location and speed can be acquired efficiently, which also leads to the disclosure of private information. It is also prone to many security and routing attacks. Hence many schemes are recommended to ensure security from intrusions in the vehicular environment.

II. BLACK HOLE ATTACK

Ensuring security against gray hole attacks, black hole attacks, Denial of Service (DoS) attacks, and Sybil attacks are tedious in vehicular environments with frequent disconnections. Black Hole attackers drop the captured packets instead of passing them on to their neighbors. Since the transmitted Cooperative Aware Messages are critical alert messages, dropping them causes the network's performance and security capabilities to decline. It also disturbs the information-sharing mechanism of the vehicles. An example scenario for the black hole attack is given in Figure 2.

In the AODV protocol, the source node checks the routing table when it intends to deliver a message to a target node. If a route leads to a destination node, it uses that path or discovers the new path by broadcasting RREQ with the sender & receiver address information. Intermediate nodes receiving RREQ [18] messages check their routing table. If there is a path for reaching a target, it sends an RREP message to the sender, or the RREQ message can be forwarded to the nearby

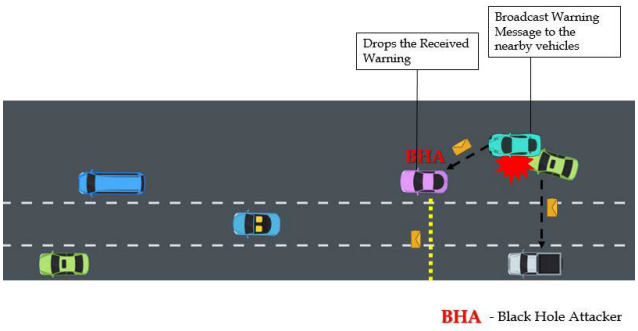

FIGURE 2. Black hole attack.

nodes. On receiving RREP messages from its neighbors, the sender accepts messages with the highest sequence number & less hop count and discards all other messages. It then sends the message in the received route to the destination node.

When a BHA (Black Hole Attacker) [17] is present in the network, as soon as it gets an RREQ message, it transmits an RREP message with the highest sequence number and less hop count without first checking its routing table. Since the RREP message sent by BHA has the highest sequence number and less hop count, the sender will accept the message and send messages to the attacker node. The attacker drops the packet without forwarding it, affecting the network's performance. As shown in Figure 3, vehicle S broadcasts an RREQ message to its immediate neighbors to find the route for destination D. When it receives the RREP message from attacker C with the highest sequence number and less hop count; it accepts the message. Vehicle S sends the message to vehicle C, considering it as the direct neighbor of destination D. Instead of forwarding the received packets, attacker C drops them, which also affects the message-sharing capability of the network and its performance.

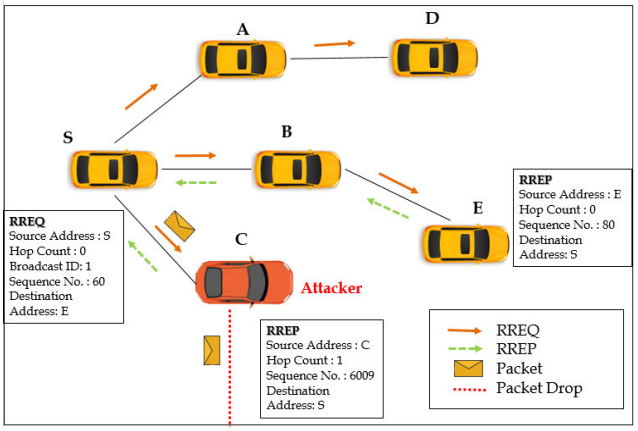

FIGURE 3. An example scenario of a black hole attack.

III. RELATED WORKS

Since the aftermath of the black hole attack drastically reduces the network's performance, many researchers proposed different solutions [4], [7], [13], [20], [21], [22], [23],

[24], [25], [26], [27], [28], [29], [30], [31] to provide security against attackers. Some of the recent solutions proposed are discussed in this section. George et al. [1] presented a watchdog concept-based intrusion detection mechanism. Each vehicle updates the trust values of the nearby vehicles in a table. The trust value increases when a vehicle forwards a message and decreases when it is dropped. If a trust value falls below a certain level, it is identified as an attacker. Since the vehicles continuously monitor the neighbor vehicles for updating the trust values, it has additional overheads. Vamshi et al. [2] proposed another watchdog approach for detecting black hole attackers. It uses a similar mechanism for identifying the attackers and has the same drawbacks.

Ameneh et al. [3] provided a technique for detecting attackers in a vehicular environment (DMV). It identifies almost all the attackers, and it uses a clustering mechanism. The network is segmented into various clusters, each headed by a cluster head who will be elected periodically. Each cluster has a verifier that monitors the behavior of the new vehicle entering a region. It increases/decreases the trust value of the new vehicle if it forwards/drops the messages. If a trust value falls below a certain level, it is reported to the certification authority through cluster heads and isolated from the network. Even though it identifies the attackers efficiently, it consumes more time and has high overheads.

Malik et al. [4] proposed a detection and prevention mechanism against black hole attackers. It detects the attackers early during the route recovery using a fake RREQ message. It has three phases: connectivity, detection, and prevention phase. The connectivity phase illustrates the vehicular environment using graph theory. The detection phase detects the attackers using a dynamic threshold value computed using the RREP messages received by its neighbors. In the prevention phase, it sends a false RREQ message bearing an invalid IP address, accurately detects attackers, and blacklists them. Even though it detects black hole attackers, it has high overheads.

Kumar et al. [5] proposed an enhanced AODV protocol with a cryptographic approach to resist black hole attackers. This approach maintains a lookup table for storing the RREP and RREQ messages. It also uses RSA for encrypting and decrypting RREQ messages. It is insecure against multiple and collaborative black hole attackers. Remya et al. [6] proposed a dynamic threshold value scheme against cooperative black hole attackers. The threshold value is determined by using linear regression. Each node's analysis of the lost packets is carried over by using the proposed technique. Using linear regression also reduces the false positive rate to a greater extent. It still has high overheads.

Younas et al. [7] suggested a collaborative detection mechanism for identifying black hole and gray hole attackers. It uses neural networks to identify the attackers. Initially, the sender floods with fake RREQ messages to identify the attackers. Data is retrieved from the network to train and test the model with ANN. Though it has high PDR, it has high overheads due to flooding. Remya et al. [8] proposed a Smart Black hole and Gray hole mitigation scheme. It uses dynamic time wrapping to analyze the time difference between the dropped packets. Attackers are identified by using the analyzed time difference. It can be used in AODV and OLSR protocols, but monitoring all vehicles by RSUs is mandatory to analyze the time series difference of the dropped packets.

Ankit et al. [9] proposed an updated AODV protocol for detecting BHA. The proposed modifications are in RREP and RREQ messages. Cryptographic encoding and decoding enhance security, which authorizes the sender and receiver. It detects the black hole attackers efficiently but can't prevent them from intruding on the network. Yang et al. [10] proposed a novel approach combining Signature-based and Anomaly-based IDS. Though it achieves higher accuracy, it increases the overheads using two intrusion detection schemes.

TABLE 1. Summarization of existing schemes.

Ref.	Methodology	Limitations
[1]	IDS uses the Watchdog approach, Trust value-based scheme	High overheads
[2]	Watchdog approach	High overheads
[3]	Clustering mechanism, Trust value-based scheme	The Cluster Head selection process will increase the overhead.
[4]	Dynamic Threshold Value based scheme	The reliability of the proposed scheme needs to be evaluated.
[5]	Enhanced AODV protocol with RSA-based encryption and decryption	Insecure against multiple and collaborative black hole attackers.
[6]	Dynamic Threshold value computed by using Linear Regression.	High overheads.
[7]	Neural Network-based scheme	Flooding incurs high overheads
[8]	Dynamic time wrapping technique	Insecure against multiple and collaborative black hole attackers.
[9]	Enhanced AODV protocol with cryptographic encoding and decoding	Insecure against multiple and collaborative black hole attackers.
[10]	Signature-based IDS & Anomaly-based IDS	High overheads
[11]	Hash value-based scheme	Hash values of the receiver must be known beforehand to establish communication
[12]	Trust Value-based scheme	High overheads

Lakshmi et al. [11] proposed a hash value-based black hole detection and prevention scheme. It uses a modified AODV protocol where the destination vehicle's hash value will be

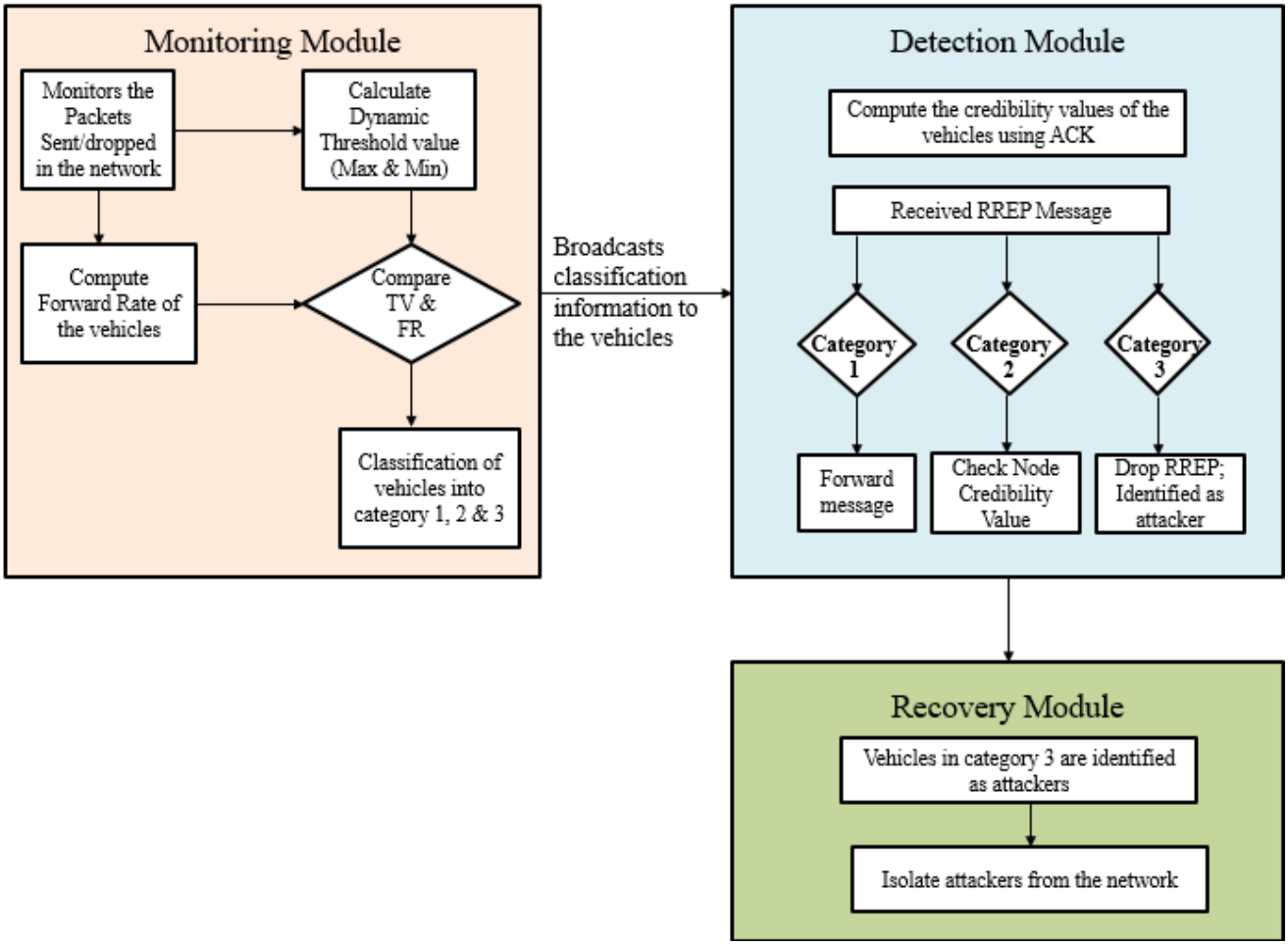

FIGURE 4. System design.

used instead of the destination address. The messages can be decrypted only by the destination vehicle. Though the proposed scheme is simple, it is not efficient. Anita et al. [12] proposed a self-cooperative detection scheme to detect simple and collaborative black hole attackers. Self-detection

process is used for identifying the simple black hole attackers, and the collaborative detection process is used for determining the collaborative black hole attackers in the network. Trust values of the vehicles are predicted using the previous destination vehicles through which attackers are detected. It has high overheads because of the exchange of trust information. Table 1 summarizes the existing schemes with their limitations. As shown, most schemes incur high overheads, and early detection of black hole attackers is not possible. Hence an efficient hybrid approach is proposed, explained in detail in the next section.

IV. PROPOSED SCHEME

The proposed hybrid approach based on the dynamic threshold value and node credibility is explained in this section. Figure 4 depicts the overall architectural design of the proposed scheme. The system has three modules: a monitoring module, a detection module, and a recovery module. RSUs are responsible for the monitoring module, which monitor the vehicles in their range using a watchdog approach. Through monitoring, RSUs classify the vehicles into three categories based on their forward rate, computed using a dynamic threshold value. It then sends the information to the vehicles in its range. In the detection phase, vehicles use the classification information and the node credibility value to identify the black hole attackers. The identified attackers are isolated from the network in the recovery phase.

A. MONITORING MODULE

RSUs are responsible for monitoring all the vehicles in their range. The actual process carried out in the monitoring module is depicted in Figure 5. RSUs act as a watchdog and observe all the packets forwarded/dropped by the vehicles. When a packet is sent by a vehicle, it stores it in its buffer and checks whether the neighbors forward it. If it is forwarded, it increments the count of forwarded packets of the network. The forwarded packets count of the neighbors who forwarded

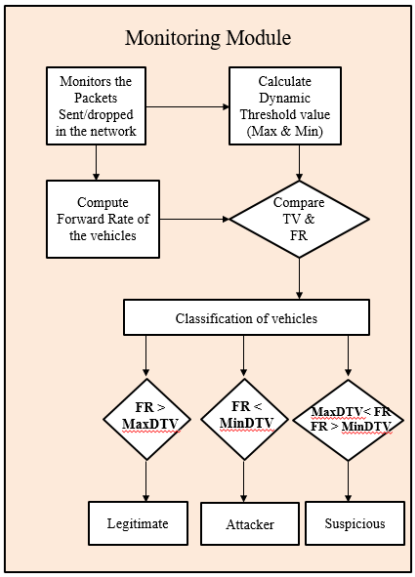

FIGURE 5. Monitoring module.

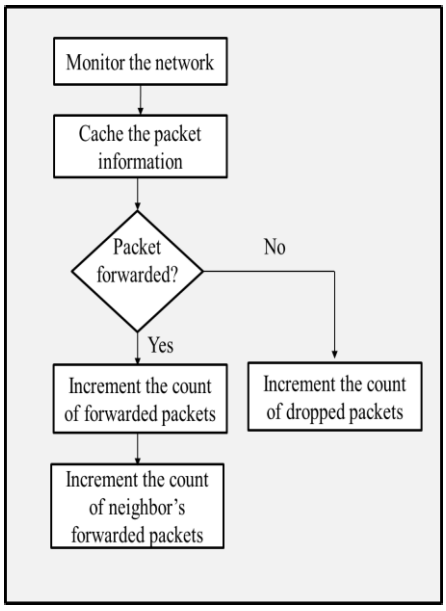

FIGURE 6. Monitoring process.

the packets is also incremented. This process is depicted in Figure 6.

It computes the Dynamic Threshold Values (DTV) periodically according to the status of the packets for that specific duration. Maximum DTV(MaxDTV) and Minimum DTV(MinDTV) values are calculated as per the given expressions. MaxDTV is the maximum threshold value. It is the ratio of the number of forwarded packets to the total packets.

$$\text{MaxDTV} = \text{Number of Forwarded Packets}/\text{Total Packets} \quad (1)$$

where the number of forwarded packets is the total count of the packets forwarded in the network, and the total packets are the total number of packets transmitted in the network for a particular duration. MinDTV is the minimum threshold value. It is the ratio of dropped packets to the total packets as given in equation 2.

$$\text{MinDTV} = \text{Number of Dropped Packets}/\text{Total Packets} \quad (2)$$

where the number of dropped packets is the total count of the packets dropped in the network, and the total packets are the total number of packets transmitted in the network for a particular duration. Using equation 3, RSUs also compute the Forward Rate (FR) of all the vehicles. It is the ratio of a vehicle's forwarded packets to the total number of received packets.

$$\text{Forward Rate (FR)} = \text{Number of forwarded packets}/\text{Number of received packets} \quad (3)$$

where the number of forwarded packets is the total count of the packets forwarded by the vehicle to its neighbors, and the number of received packets is the total number of packets received by the vehicle from its neighbors.

With the computed values, RSUs classify the vehicles into three categories, as listed below.

CATEGORY 1 - Legitimate
CATEGORY 2 - Suspicious
CATEGORY 3 - Attacker

1) CATEGORY 1 - LEGITIMATE

If the computed forward rate (FR) exceeds MaxDTV, it is classified as CATEGORY 1. These are legitimate vehicles. When a receiver receives messages from the vehicles in CATEGORY 1, it directly accepts them without any verification.

2) CATEGORY 2 - SUSPICIOUS

If the computed forward rate (FR) is in between MinDTV and MaxDTV, it is classified as CATEGORY 2. These are suspicious vehicles. When a receiver receives messages from the vehicles in CATEGORY 2, it checks the node credibility value and accepts them if the vehicle's credibility value is '1'.

3) CATEGORY 3 – ATTACKER

If the computed forward rate (FR) is lesser than MinDTV, it is classified as CATEGORY 3. These are malicious vehicles. When a receiver receives messages from the vehicles in CATEGORY 3, it directly rejects them without any verification.

After classifying the vehicles into different categories, it updates the Status Record (SR) details and broadcasts it to all the vehicles within its range. The sample Status Record is given in Table 2.

B. DETECTION MODULE

The actual process carried out in the detection module is depicted in Figure 7. Vehicles maintain the neighbors'

TABLE 2. Status Record (SR).

Node	Category
S	1
X	3
A	2
D	1

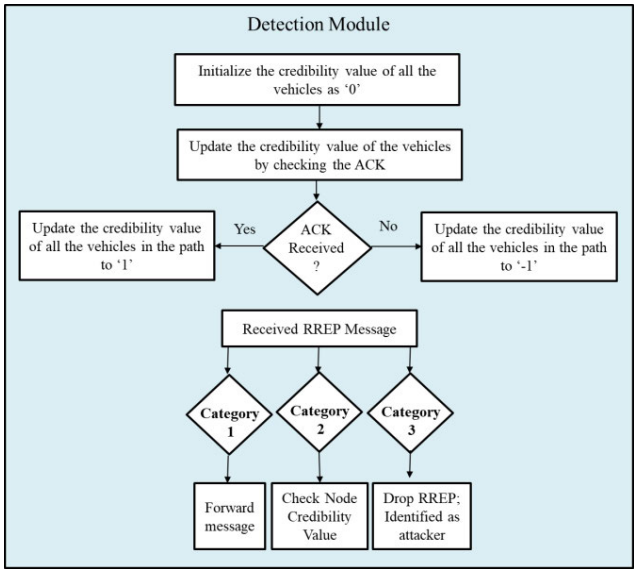

FIGURE 7. Detection module.

credibility value in the Node Credibility Information Record (NCIR). Initially, all the vehicles' node credibility value is '0' since the node credibility values are not obtained at the initial stage. When the destination vehicle receives the forwarded messages, it returns the ACK message in the same path. After receiving an ACK message, the sender will update the node credibility values of all the vehicles in its range as '1', indicating them as legitimate vehicles. If the sender does not receive the ACK message, it updates the value of all the vehicles as '-1', indicating them as possible attackers. The sample Node Credibility Information Record (NCIR) is given in Table 3.

TABLE 3. Node Credibility Information Record (NCIR).

Node	Category	Credibility Value
S	1	1
X	3	0
A	2	-1
D	1	1

When a vehicle has to send a message to the destination vehicle, and if no path is available in its routing table, it discovers the path by broadcasting RREQ messages to its neighbors. When receiving RREP messages from its neighbor, it checks the neighbor's category in the Status Record (SR). If it is in Category 1, it will send the message to the neighbor, as stated in section IV-A, whereas if it is in Category 3, the received RREP messages are discarded.

The node's credibility value will be used if the neighbor is in Category 2. In that case, the sender will check the credibility value. If it is '1', it will send the message to the neighbor, whereas if it is '-1', it discards the message. If the node credibility value is '0', it sends the message and waits for the ACK to update the credibility values. The node credibility values are also shared among the vehicles by sharing the updated NCIR periodically. In this way, the vehicles detect the attackers in the network with the help of RSUs.

C. RECOVERY MODULE

Since the attackers are identified using the DTV and Node credibility value, the attackers are isolated from the network. The classification information of the vehicles is periodically broadcasted by the RSU, which helps the vehicles to maintain the NCIR and eventually discards the messages from the attackers. Hence prevents the attackers from establishing communication in the network. The actual process involved in the recovery module is given in Figure 8.

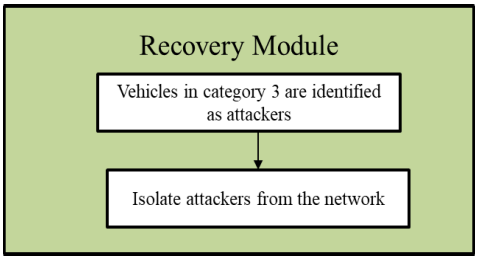

FIGURE 8. Recovery module.

V. PERFORMANCE ANALYSIS

The proposed scheme is implemented, and its performance is analyzed in NS2. A vehicular scenario is created with 150 vehicles, 3 RSUs, and 1 TA. The simulation parameters are listed in Table 4. The vehicular environment is created with a random mobility model for vehicles with different destination locations. The simulation is done with vehicles moving from one place to another in a structured route at different speeds: 10m/s, 20m/s, 30m/s, 40m/s, 50m/s. It is carried over in independent runs with 25, 50, 75, 125, and 150 vehicles, respectively. The sample simulation map with 3 RSUs, and vehicles are given in figure 9. The figure shows that vehicles move from their source to target destinations at the assigned speed based on the random mobility model. Each RSU is responsible for the vehicles in its range. RSUs can also communicate with other RSUs, and TA controls all the RSUs.

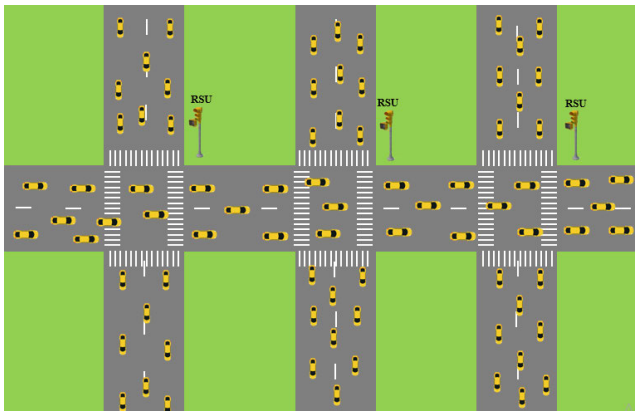

FIGURE 9. Sample simulation map.

TABLE 4. Simulation parameters.

Parameter	Value
Simulation Tool	NS 2.35
Simulation Area	5000m x 5000m
RSU	3
Vehicles	25, 50, 75, 100, 125, 150
TA	1
Simulation Time	500s
Black Hole attackers	6%
Routing Protocol	AODV
Packet Size	512

Black hole attackers are manually assigned to the network. For each run, 6% of black hole attackers are assigned to the network. If the number of vehicles is 25, then two vehicles (6%) are set manually as attackers; if it is 50, then three vehicles (6%) as attackers, and so on. The performance is evaluated by comparing it with other recent schemes [4], [5], [9], [11], [12], [13]. The simulation is carried out with different traffic densities of vehicles ranging from 25 to 150. Each vehicular scenario comprises 6% of black hole attackers. The performance metrics used for analysis are Packet Delivery Ratio (PDR), Throughput, Delay, Packet Loss Ratio, Routing Overhead, and Detection Ratio.

A. PACKET DELIVERY RATIO

PDR is the ratio of the sum of the received packets to that of the packets originated from the sender. It is computed by using the given equation.

$$\text{PDR} = \text{Sum of the received packets} / \text{Sum of the originated packets} \quad (4)$$

where the sum of received packets is the total count of the packets received by the vehicles from its neighbors, and the sum of the originated packets is the total count of the packets sent by the vehicles to its neighbors. PDR simulation results concerning the number of vehicles are depicted in Figure 10. Due to the impact of the packet drops in the network, PDR decreases gradually as the number of attackers increases. In the proposed scheme, with the help of DTV and Node credibility value, vehicles efficiently detect the attackers early in the network and isolate them from the network. Hence the proposed scheme has better PDR than the other related schemes. The PDR on average in [4], [5], [9], [11], [12], and [13] and the proposed scheme are 85.6%, 29.67%, 36.3%, 77.6%, 77.3%, 80.5% and 89.67% respectively. Since the proposed scheme efficiently identifies the black hole attackers in the network, it has a higher PDR when compared to the other schemes.

B. AVERAGE THROUGHPUT

Throughput computes the average success rate of the packet delivery to the destination node. It is the ratio of the sum of the received packets to that of the simulation time. It is computed by using the given equation.

$$\text{Throughput} = \text{Sum of the received packets}^{*}\text{Packet Size} / \text{Time} \quad (5)$$

where the sum of the received packets is the total count of received packets of the vehicles, packet size is the size of the packets exchanged between the vehicles, and time is the specified duration in which the vehicles exchange messages.

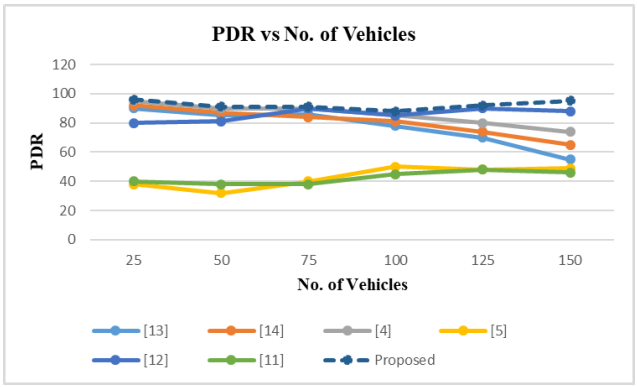

FIGURE 10. Packet delivery ratio.

Average Throughput simulation results concerning the number of vehicles are depicted in Figure 11. Because of the attackers, the packets are not delivered successfully to the destination vehicle. It leads to a decrease in the throughput. In the proposed scheme, the attackers are isolated from the network at the early stage with the help of RSUs. Hence the proposed scheme has better throughput than the other related schemes. The throughput on average in [4], [5], [9], [11], [12], and [13] and the proposed scheme are 22.38%, 5.0%, 9.61%, 14.14%, 15.41%, 18.36%, and 30.27% respectively.

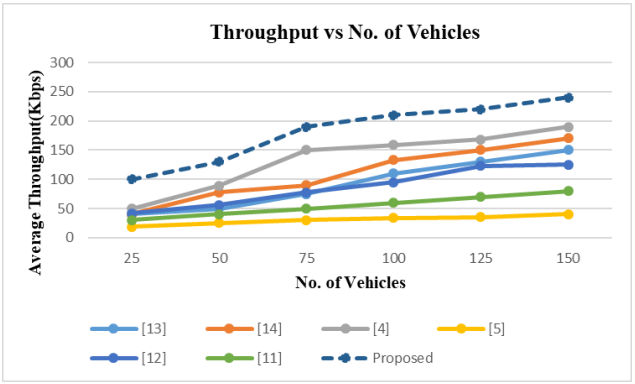

FIGURE 11. Average throughput.

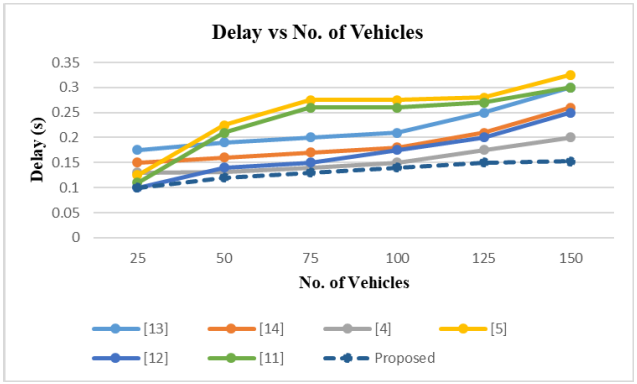

FIGURE 12. Delay.

Since the proposed scheme efficiently identifies the black hole attackers in the network, it has a higher average throughput when compared to the other schemes.

C. END-TO-END (E2E) DELAY

E2E delay computes the time difference between the sent and received packets. It is computed by using the given equation.

$$\begin{aligned}&\text{End-to-End Delay}\\&= (\text{Sum of the time difference between the sent}\\&\quad \& \text{ received packets} * 1000(\text{ms}))/\text{Sum of delivered packets}\end{aligned} \tag{6}$$

where the sum of the time difference between the sent and received packets is the summation of the time differences of the packets, and the sum of delivered packets is the total count of the delivered packets for 1000ms. E2E delay simulation results are depicted in Figure 12. In the proposed scheme, attackers are detected early and isolated with the help of RSUs. Hence, the proposed scheme's delay is gradually less than the other schemes. The delay on average in [4], [5], [9], [11], [12], and [13] and the proposed scheme are 15.4%, 25%, 23.5%, 16%, 22%, 18.8%, and 9% respectively. Since the proposed scheme efficiently identifies the black hole attackers in the network, it has less delay when compared to the other schemes.

D. PACKET LOSS RATIO

Packet loss ratio is the difference between the sum of sent and received packets. Packets are dropped because of the black hole attackers and congestion in the network. It is computed by using the given equation.

$$\begin{aligned}&\text{Packet Loss Ratio}\\&= \text{Sum of the packets sent} - \text{Sum of the packets received}\end{aligned} \tag{7}$$

where the sum of the packets sent is the total count of transmitted packets, and the sum of the received packets is the total count of the packets received by the vehicles. The packet loss ratio simulation results are depicted in Figure 13. Because of

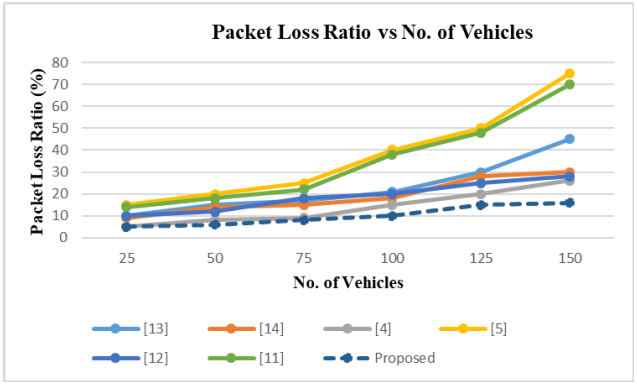

FIGURE 13. Packet loss ratio.

the prevention mechanism used in the proposed scheme, the packet loss ratio is less compared with other schemes. The packet loss ratio on average in [4], [5], [9], [11], [12], and [13] and the proposed scheme are 13.8%, 37.5%, 35.5%, 18.8%, 23%, 19%, and 10% respectively. Since the attackers are isolated, the dropped packets are reduced, and the proposed scheme has less packet loss ratio.

VI. CONCLUSION

A hybrid approach based on the dynamic threshold value and node credibility is proposed in this paper. The dynamic threshold value is computed with the help of RSUs, which are used for categorizing the vehicles. On the other hand, vehicles use the node credibility value to identify the attackers efficiently. PDR, Delay, throughput, and packet loss ratio metrics evaluate the proposed scheme's performance. According to the simulation results, the proposed scheme performs better than other methods and has a high PDR (89.67%) and less delay (9%).

REFERENCES

[1] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.

[2] C. Sayan, S. Hariri, and G. Ball, "Cyber security assistant: Design overview," in *Proc. IEEE 2nd Int. Workshops Found. Appl. Self* Syst. (FAS*W)*, Sep. 2017, pp. 313–317.

[3] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," *Multimedia Tools Appl.*, vol. 66, no. 2, pp. 325–338, Sep. 2013.

[4] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J.-T. Seo, "An efficient dynamic solution for the detection and prevention of black hole attack in VANETs," *Sensors*, vol. 22, no. 5, p. 1897, Feb. 2022.

[5] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," *Wireless Netw.*, vol. 28, pp. 3127–3142, Oct. 2022.

[6] R. Krishnan and P. A. R. Kumar, "A dynamic threshold-based technique for cooperative blackhole attack detection in VANET," *Intelligent Data Communication Technologies and Internet of Things* (Lecture Notes on Data Engineering and Communications Technologies), vol. 101, D. J. Hemanth, D. Pelusi, and C. Vuppalapati, Eds. Singapore: Springer, 2022, pp. 599–611.

[7] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs," *Appl. Sci.*, vol. 12, no. 23, Dec. 2022, Art. no. 12448.

[8] P. R. Krishnan and P. A. R. Kumar, "Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping," *Wireless Pers. Commun.*, vol. 124, no. 1, pp. 931–966, May 2022.

[9] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. D. A. Kumar, B. K. Panigrahi, and K. C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103352.

[10] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, Jan. 2022.

[11] E. A. M. Anita and J. Jenefa, "A survey on authentication schemes of VANETs," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2016, pp. 1–7.

[12] J. Jenefa and E. A. M. Anita, "Secure vehicular communication using ID based signature scheme," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 1383–1411, Jan. 2018.

[13] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[14] M. K. Saggi and R. K. Sandhu, "A survey of vehicular ad hoc network on attacks & security threats in VANETs," in *Proc. Int. Conf. Res. Innov. Eng. Technol. (ICRIET)*, India, Dec. 2014.

[15] J. Jenefa and E. A. M. Anita, "Secure authentication schemes for vehicular adhoc networks: A survey," *Wireless Pers. Commun.*, vol. 123, no. 1, pp. 31–68, Mar. 2022.

[16] J. Jenefa and E. A. M. Anita, "Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks," *Wireless Netw.*, vol. 27, no. 5, pp. 3093–3108, Jul. 2021.

[17] E. A. M. Anita, S. Lakshmi, and J. Jenefa, "A self-cooperative trust scheme against black hole attacks in vehicular ad hoc networks," *Int. J. Wireless Mobile Comput.*, vol. 21, no. 1, pp. 59–65, 2021.

[18] S. Lakshmi, E. A. M. Anita, and J. Jenefa, *Detection and Prevention of Black Hole Attacks in Vehicular Ad Hoc Networks*, vol. 8, no. 7. India: Blue Eyes Intelligence Engineering and Sciences Publication, May 2019.

[19] J. Jenefa and E. A. M. Anita, "An enhanced secure authentication scheme for vehicular ad hoc networks without pairings," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 535–554, May 2019.

[20] J. Tobin, C. Thorpe, and L. Murphy, "An approach to mitigate black hole attacks on vehicular wireless networks," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–7.

[21] A. Gruebler, K. D. McDonald-Maier, and K. M. A. Alheeti, "An intrusion detection system against black hole attacks on the communication network of self-driving cars," in *Proc. 6th Int. Conf. Emerg. Secur. Technol. (EST)*, Sep. 2015, pp. 86–91.

[22] A. Kumar and M. Sinha, "Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET)," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 4, pp. 453–463, May 2019.

[23] K. C. Purohit, S. C. Dimri, and S. Jasola, "Mitigation and performance analysis of routing protocols under black-hole attack in vehicular ad-hoc network (VANET)," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5099–5114, Dec. 2017.

[24] S. Lachdhaf, M. Mazouzi, and M. Abid, "Detection and prevention of black hole attack in VANET using secured AODV routing protocol," in *Proc. Comput. Sci. Inf. Technol. (CS &IT)*, Nov. 2017, pp. 25–36.

[25] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, "LI-AODV: Lifetime improving AODV routing for detecting and removing black-hole attack from VANET," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 1, pp. 1–14, 2017.

[26] B. Cherkaoui, A. Beni-hssane, and M. Erritali, "Variable control chart for detecting black hole attack in vehicular ad-hoc networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5129–5138, Nov. 2020.

[27] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "A reliable tactic for detecting black hole attack in vehicular ad hoc networks," in *Advances in Computer and Computational Sciences*, vol. 553, S. Bhatia, K. Mishra, S. Tiwari, and V. Singh, Eds. Singapore: Springer, 2017.

[28] B. Cherkaoui, A. Beni-Hssane, and M. Erritali, "A clustering algorithm for detecting and handling black hole attack in vehicular ad hoc networks," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, vol. 520, Á. Rocha, M. Serrhini, and C. Felgueiras, Eds. Pakistan: Little Lion Scientific, 2017, pp. 481–490.

[29] S. Mitra, B. Jana, and J. Poray, "A novel scheme to detect and remove black hole attack in cognitive radio vehicular ad hoc networks(CR-VANETs)," in *Proc. Int. Conf. Comput., Electr. Commun. Eng. (ICCECE)*, Dec. 2016, pp. 1–5.

[30] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, "A reputation system for detection of black hole attack in vehicular networking," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–5.

[31] G. Primiero, A. Martorana, and J. Tagliabue, "Simulation of a trust and reputation based mitigation protocol for a black hole style attack on VANETs," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 127–135.

S. LAKSHMI is currently a Research Scholar with AMET University, Tamil Nadu, India. Her current research interest includes vehicular ad hoc networks.

E. A. MARY ANITA (Senior Member, IEEE) received the B.E. and M.E. degrees from the Government College of Engineering, Tirunelveli, India, and the Ph.D. degree in information and communication from Anna University, Chennai. She is currently a Professor with the Computer Science and Engineering Department, Christ (Deemed to be University), Bengaluru. She has over 33 years of teaching experience and has published more than 80 research papers in international and national journals and conferences. Her research interests include wireless networks, security, and privacy. She is a Life Member of Indian Society for Technical Education (ISTE), Computer Society of India (CSI), IAENG, and ACM. She is a peer reviewer for refereed international journals. Her biography has been included in the 2014 edition of Who's Who in the World, USA.

J. JENEFA received the bachelor's and master's degrees in computer science and engineering, and the Ph.D. degree in information and communication engineering from Anna University, Chennai. She is currently an Assistant Professor with the Department of Computer Science and Engineering, Christ (Deemed to be University), Bengaluru. Her current research interests include network security and vehicular ad hoc networks.