ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2025.0518

IDPSA: AN IMPROVED DETECTION AND PREVENTION SOURCE AUTHENTICATION OF BLACK HOLE ATTACK IN VANETS

A. Muthusamy[1], P. Lakshmi[2], D. Maheshwari[3] and R. Rajeswari[4]
[1]*Department of Computer Technology, Kongu Engineering College, India*
[2]*Department of Computer Science, SRM Institute of Science and Technology, India*
[3]*Department of Computer Technology, KPR College of Arts Science and Research, India*
[4]*Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, India*

Abstract

Vehicular Ad-hoc Networks (VANETs) are susceptible to black hole attacks, which compromise the integrity and reliability of vehicular communication. Existing solutions often fall short in detecting and preventing these attacks. To overcome this issue, the proposed system presents an Improved Detection and Prevention Source Authentication (IDPSA) algorithm with AODV routing protocol to counter black hole attacks in Vehicular Ad-hoc Networks (VANETs). The IDPSA algorithm aims to enhance the security of VANETs by accurately detecting and preventing source authentication attacks, thereby ensuring the integrity and reliability of communication among vehicles and infrastructure. The proposed algorithm leverages advanced techniques to identify and mitigate black hole attacks, which are a significant threat to VANET security. By implementing IDPSA, the proposed system significantly improves the resilience of VANETs against such attacks and ensures the safety and efficiency of vehicular communication. According to the experimental findings, the suggested IDPSA performed better than the current techniques in terms of throughput metrics, routing overhead, and packet delivery ratio (PDR).

Keywords:

VANET, RSU, AODV, Detection, Prevention, V2V Communication

1. INTRODUCTION

VANET (Vehicular Ad-hoc Network) is a communication network that enables vehicles and infrastructure to exchange information, enhancing road safety. The network consists of On-Board Units (OBUs) installed in vehicles and Roadside Units (RSUs) that periodically exchange messages to ensure safe, smooth, and comfortable driving. VANET applications can be categorized into two types: safety applications, such as emergency braking, light warnings, and blind spot alerts, and non-safety applications, including infotainment services like weather forecasts and internet access. [1]

A Black Hole Attack in VANET is a type of security threat where a malicious node absorbs and drops data packets, disrupting communication between vehicles and infrastructure, leading to data loss, network congestion, increased latency, and compromised safety applications, as the attacker falsely advertises itself as a shortest path or reliable node, attracting and then discarding data packets, which can have devastating consequences in safety-critical applications like emergency braking or collision avoidance, where timely data exchange is crucial, making it essential to defend against such attacks to ensure the reliability and security of VANET [2]-[3].

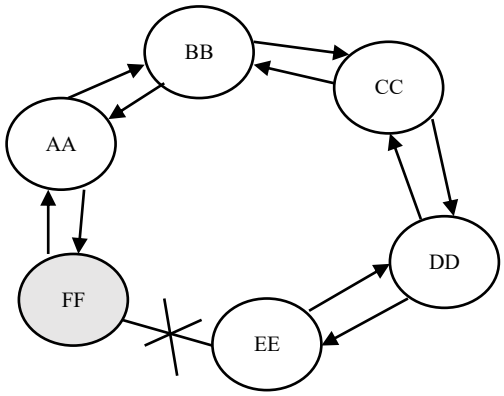

Fig.1. Black Hole attack

Modern vehicles often come equipped with mapping facilities for effortless route discovery. However, if a vehicle's system is compromised, it may not receive reliable routing information. In a Blackhole attack, a malicious node exploits this vulnerability by advertising itself as a shortcut to the destination [4-5]. The attacker intercepts route requests and responds with false replies, broadcasting the shortest route and manipulating sequence numbers. When a vehicle initiates route discovery, the malicious node seizes the opportunity to send a fake reply, redirecting the vehicle's messages through itself. Consequently, all messages routed through the attacker are dropped, compromising the vehicle's communication and safety.

The Fig.1 illustrates a Blackhole attack in VANET, where vehicles AA, BB, CC, DD, EE, and FF are labeled nodes. Vehicle FF is the malicious attacker. When vehicle AA intends to send data packets to vehicle EE, vehicle EE initiates a Route Discovery Request message. Upon receiving this message, the malicious vehicle FF responds with a Route Reply Message, falsely claiming to be the shortest path to the destination, deceiving vehicle AA into believing that FF is the optimal route. Consequently, vehicle EE sends all messages through vehicle CC, but the malicious vehicle FF intercepts and drops all messages received from vehicle EE, compromising the communication.

In VANET, authentication is crucial to prevent malicious attacks, such as Blackhole attacks, which can compromise V2V and V2I communication. Blackhole attacks in VANET occur when a malicious node falsely advertises itself as a shortest path, intercepting and dropping data packets [6]. To counter this, authentication mechanisms are employed to verify the identity of vehicles and ensure trustworthy communication. Various authentication techniques, such as digital signatures, public key infrastructure (PKI), and symmetric key cryptography, are used to

secure VANET against Blackhole attacks, ensuring reliable and secure data exchange between vehicles and infrastructure [7]-[9].

The routing process in VANET is vulnerable to Blackhole attacks, where a malicious node advertises itself as a shortest path to destination, intercepting and dropping data packets, disrupting the network's integrity, causing packet loss, network congestion, increased latency, and compromising safety applications, and exploiting the routing protocol's trustfulness, making it challenging to detect and prevent, thus securing the routing process is crucial to ensure reliable and safe communication in VANET [10].

2. RELATED WORK

According to Alshammari et al. [11], VANETs have recently emerged as a promising technology for ITSs and smart cities, leveraging wireless vehicular communication to enhance traffic safety and reduce congestion. In this ad-hoc network, each vehicle acts as a high-mobility, dynamic node. However, the continuous movement of vehicles makes VANETs vulnerable to various security threats, necessitating safe communication. Notably, Black Hole attacks allow malicious vehicles to intercept and drop data without forwarding it to other cars, compromising the network's integrity.

Ahmed et al. [12] addressed the issue of optimal RSU placement on a highway-like roadway, proposing a scheme that minimizes network latency. They developed an integer linear programming model to represent the network and applied optimization techniques to determine the RSU deployment that achieves minimum network latency.

Kumar et al. [13] highlighted the vulnerability of VANETs to malicious attacks, emphasizing the need for effective security measures. In VANETs, any node can act as a router, allowing malicious nodes to inject spoofed routing tables and compromise network operations. To address this, the authors proposed a secure AODV routing protocol to detect black hole attacks. The modified protocol enhances RREQ and RREP packets and incorporates cryptography-based encryption and decryption to verify source and destination nodes, ensuring added security.

Malik et al. [14] introduced a novel solution, DPBHA, to enhance the security and performance of VANETs by detecting BHA during the initial route discovery phase. The proposed solution computes active threshold rate and generates a forged RREQ packet to identify and prevent BHA.

Okeke et al. [15] examined the devastating impact of black hole attacks on networks, where malicious nodes can inject false data, broadcast fake routing information, selectively drop packets, and disrupt routing protocols. To counter this, the authors proposed a secure AODV routing protocol integrated with K-means clustering and Particle Swarm Optimization (PSO)-modified RREQ and RREP packets. This defense mechanism employs cryptography to encrypt and decrypt vehicle packet sequence numbers, validating source and destination nodes and ensuring the integrity of the network.

Abdelhamid et al. [16] proposed an anomaly detection system based on Support Vector Machine (SVM) to identify black hole attacks in networks. This system analyzes network traffic and detects anomalies by examining node behavior, leveraging the distinct characteristics of attacking nodes. The authors evaluated their lightweight detection system using the OMNET++ simulator, generating traffic under black hole attack conditions. The system effectively classified traffic as malicious or non-malicious, enabling the identification of malicious nodes.

3. METHODS

The proposed research methodology performs the Black Attack detection and prevention using Improved Detection and Prevention Source Authentication (IDPSA) in VANET process is derived in this section. The overall proposed process flow diagram is illustrated in Fig.2.

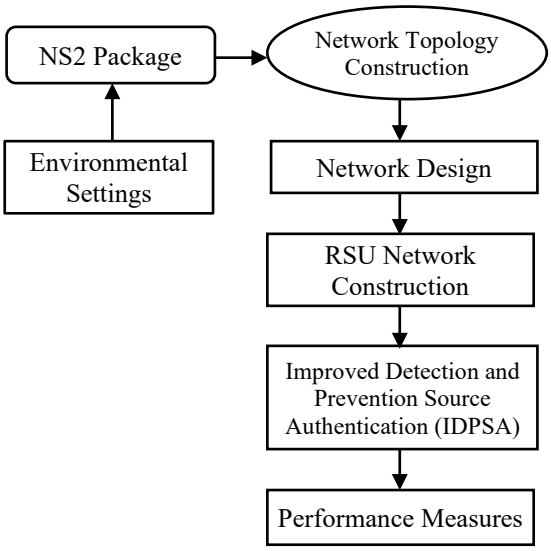

Fig.2. Proposed Flow Diagram

3.1 NETWORK MODEL

The network design model utilizes NS2.34 simulator and Constant Bit Rate (CBR) traffic to simulate a road system consisting of links, connectors, and RSUs (Roadside Units). Each vehicle has a unique ID and moves along links with one or more RSUs, which are designated areas allowing specific vehicle types to enter. Node waypoints are numbered and spaced at least 5m apart to accommodate vehicle length. RSUs are positioned at nodes, interconnected via wireless links with negligible transmission time. The RSU coverage area is configured to ensure vehicles enter the range of an RSU while moving in the lane, enabling data transmission between RSUs and vehicles. In the network scenario, nodes are placed randomly or according to a specific distribution, modeling node mobility using models like Random Waypoint, setting the communication range, configuring node properties, and setting up network protocols like AODV and IEEE 802.11p. The Fig.3 illustrates the network model deployment model.

3.2 RSU NETWORK CONSTRUCTION

The VANET consists of RSUs and vehicles moving in opposite directions on two-way roads. Vehicles are classified as moving left (north/south to west/east) or right (east/west to north/south), ensuring one vehicle moves left and the other right when traveling in opposite directions. For safety applications,

vehicles and RSUs transmit event-driven and periodic safety messages. While RSU messages have equal widths that could vary between RSUs based on the application, periodic messages from cars have a set size.

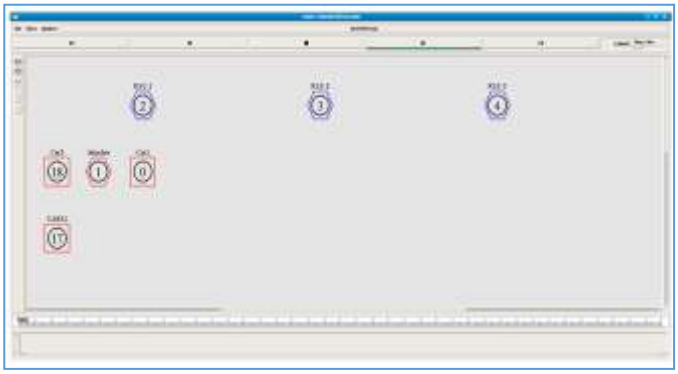

Fig.3. Network model of RSU and Vehicle ID Assignment

To develop a Roadside Unit (RSU) network model, we aim to deploy n RSUs with a transmission range within a network topology spanning an area of E, comprising k intersections. In this model, i denotes an intersection among two paths, and each element $vh_j \in Src_i$ represents a vehicle crossing intersection i. The transmission range of the Roadside Unit (RSU), strategically positioned at the center of the intersection, delineates the boundaries of the intersection. The weight (distance) associated with vehicle vj signifies the duration that the vehicle remains within the intersection. Fig.4 shows the RSU construction with packet transmission of RSU to Vehicle.

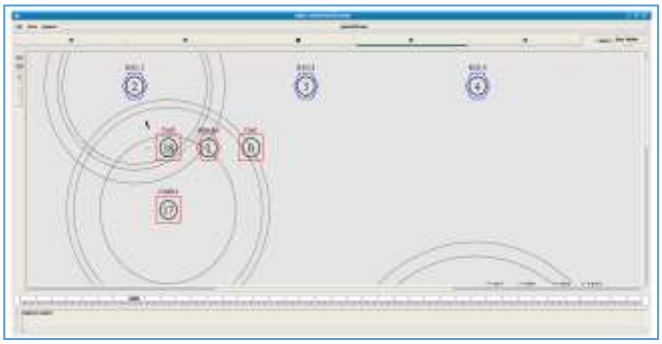

Fig.4. Packet Transmission RSU to Vehicle

Let $V = \{v_1, v_2 \ldots, v_v\}$ be a group of vehicles, and $SB_i \subseteq Vh$ stands for a division of vehicles that enter junction i. The aim is to select at most p sets to maximize the cardinality of the union $S_1 \cup S_2 \cup \ldots \cup S_k$. Consider the matrix $T_{n,v}$, where $T_{i,j} \geq 0$ signifies the whole-time vehicle j expend in intersection i. The time threshold can be defined as:

$$\max \sum_{j=1}^{v} \min\left(\tau, \sum_{i=1}^{n} T_{i,j} y_i\right) \quad (1)$$

$$\sum_{i=1}^{n} y_i \leq k, \quad y_i \in \{0,1\}, \quad \forall i \quad (2)$$

The variable y_i indicates the presence or absence of an RSU at intersection i, with $y_i = 1$ representing an RSU present and $y_i = 0$ representing no RSU. Eq,(1) defines the Maximum RSU Coverage Problem, aiming to maximize RSU coverage, while Eq.(2) constrains the number of selected intersections to at most k, limiting RSU deployment.

3.3 IMPROVED DETECTION AND PREVENTION SOURCE AUTHENTICATION (IDPSA) IN VANET

The proposed method of IDPSA mechanism is integrated with the Ad-hoc On-Demand Distance Vector (AODV) routing protocol in VANET to enhance the security and reliability of vehicular communications. IDPSA leverages AODV's routing protocol to detect and prevent malicious nodes, particularly black hole nodes, from disrupting the network. The mechanism uses a dynamic threshold-based approach to identify suspicious nodes, which are then confirmed as malicious through a forged RREQ packet technique.

Upon detection, the attacker is added to a black list and an alarm message is broadcasted to alert other nodes in the network. By combining IDPSA with AODV, the security and efficiency of VANET are significantly improved, enabling reliable and secure communication between vehicles. This integrated approach ensures that malicious nodes are promptly detected and prevented from compromising the network, maintaining the integrity of vehicular communications.

During the detection phase, a vibrant threshold value *th* is computed to recognize attacker node in the network. The following actions are taken by the origin node in order to calculate the threshold value *th*:

- Sort all established RREPs in sliding order with value to Destination Sequence Number (DSN).
- Calculate the average of all received RREPs' DSN values, denoted as avg_DSN.
- Calculate the variation among the final RREP's DSN and the routing table's DSN, denoted as diff_DSN.

Compute the threshold value *th* as:

$$th = avg\_DSN + diff\_DSN \quad (3)$$

This threshold value *th* is then used to recognize the attacker node in the network. Let, DSN_last_RREP be the Destination Sequence Number of the last received RREP; DSN_routing_table be the Destination Sequence Number stored in the routing table. Then, the dissimilarity among the last RREP's DSN and its routing table's DSN is defined as:

$$\mathrm{TH} \dashv \mathrm{avg}\left(\sum_{k=1}^{m}\left(\mathrm{DSN}(\mathrm{RREP}_k) - \mathrm{diffDSN}_k\right)\right) + \mathrm{mdiffDSN}| \quad (4)$$

The source node performs the following check for each RREP:

$$DSN\_RREP > th \quad (5)$$

If the condition is true, i.e., *DSN_RREP>th*, then the source node considers the current RREP as a malicious node (black hole node).

During the prevention phase, the source node executes the following steps: (1) Modifies the RREQ packet format by replacing the destination node ID with a non-existing node ID, denoted as ID_fake; (2) Broadcasts the forged RREQ packet, denoted as RREQ_forged. Only an attacker node, denoted as Node_M, will respond to the forged RREQ packet, as it does not perform a routing table lookup for the target. Node_M generates

an RREP packet, denoted as RREP_M. If the node that was marked as 50 percent assumed in the earlier phase, denoted as Node_S, responds to the forged RREQ packet, then it is confirmed as a 100 percent black hole node, denoted as Node_B. This is represented by Equation (7):

$$\text{Node\_B} = \text{Node\_S} \cap \text{RREP\_M} \tag{6}$$

Fig.5. Attacker Vehicle Send Fake packets to CAR 2 Vehicle

Node_B is immediately added to the black list by the source vehicle node, which also sends an alarm message throughout the network by include Node_B's identify in the RREQ packet, which is known as RREQ_alarm. The result of IDPSA showed in Fig.5 and Fig.6.

Fig.6. Car 2 Vehicle Drop the Attacker false packets

Algorithm: IDPSA

Input: Number of Vehicle nodes *m*, RREQ, RREP.

Output: BlackHole Attack detection and prevention

Preparation:

1. Network Model
2. RSU Construction
3. IDPSA
4. Compute PDR, Revocation Delay (RD), Packet Loss Rate and Authentication Delay

Steps:

While (*m*)

1. Nm← Network Model Construction
2. *Source*→ RREQ to *m*
3. *Destination vNm*→*RREP* to *Source*
4. Initialize routing process
5. Calculate the variation among the final RREP's DSN using Eq.(4)
6. Calculate threshold value using Eq.(5).
7. **If** *DSN_RREP* > *th* **then**
8. GP ←*VID* (RREP) // *where GP is group of vehicles*.
9. **Else**
10. Selects RREP to Destination
11. **End**
12. **If** *VID* (RREP) = *GP*(*VID* (RREP))
13. Blackhole← *GP*|*VID*|
14. Source → Alarm to neighbor vehicles
15. **Else**
16. Source → packets to Destination.
17. **End**

4. RESULTS AND DISCUSSION

The Improved Detection and Prevention Source Authentication (IDPSA) in VANET were employed for result estimation. Simulations were conducted using NS 2.34 simulator on a Windows 10 machine with 8GB of main memory and an Intel I5-6500U series 4.28GHz. The Fig.7 shows the Routing Overhead (ROH) with existing AODV [17], IDBA [18], DPBHA [14] and proposed IDPSA is defined as the percentage of the whole amount of control messages transmitted (N_CP) to the whole amount of data messages transmitted (N_DP), and are calculated using the following equation:

$$\text{ROH} = \frac{N_{\text{CP}}}{N_{\text{DP}}} \tag{7}$$

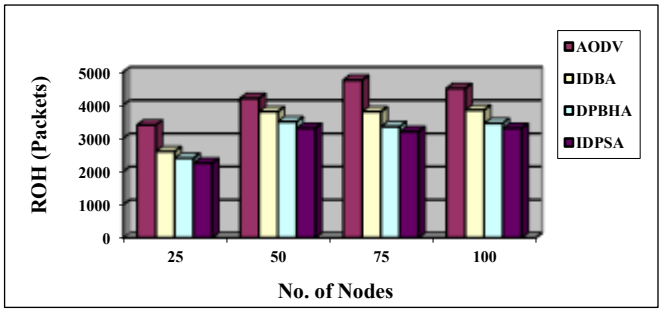

Fig.7. ROH Chart

The proposed IDPSA's improved routing overhead performance demonstrates its potential to enhance network efficiency and scalability in VANETs. By reducing routing overhead, IDPSA can lead to improved network performance. IDPSA decreases routing overhead by 33.8% to 26.7% compared to AODV, 13.5% to 14.3% compared to IDBA, and 6.3% to 4.3% compared to DPBHA.

The Fig.8 shows the throughput (TP) measures is defined as the below equation:

$$\text{TP} = \frac{\text{Total number of packets successfully delivered}}{\text{Total delivery time}} \tag{8}$$

The Fig.9 shows the packet delivery ratio (PDR) is defined as the ratio of the entire amount of packets successfully established

at the destination node (N_rx) to the whole amount of packets originated at the origin node (N_tx), and is calculated using the following equation:

$$\text{PDF} = \frac{N_{\text{rx}}}{N_{\text{tx}}} \tag{9}$$

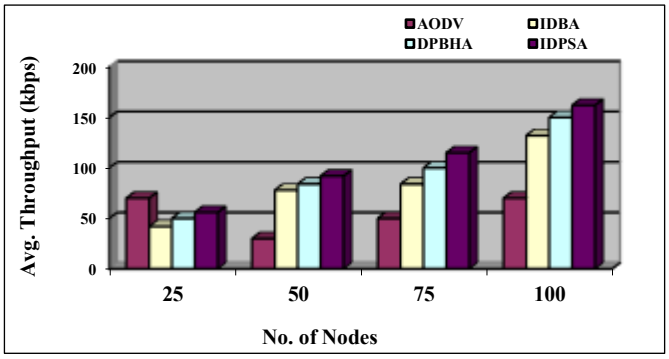

Fig.8. Throughput Chart

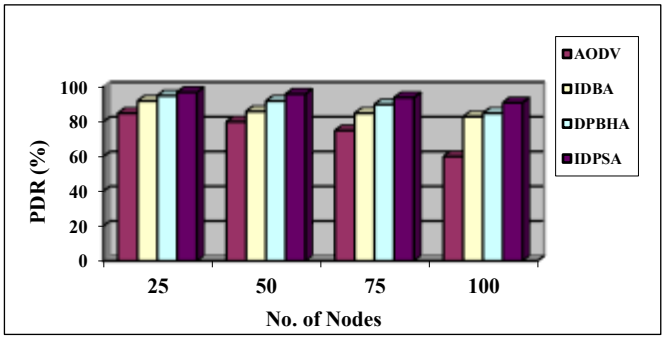

Fig.9. PDR Chart

5. CONCLUSION AND FUTURE WORK

The paper proposed an IDPSA with AODV routing protocol in VANET effectively detects and prevents black hole attacks, ensuring the security and reliability of vehicular communications. By leveraging a dynamic threshold-based approach, sequence number analysis, and forged RREQ packet techniques, IDPSA accurately identifies malicious nodes and updates the black list and routing table to prevent data packets from being routed through them. Overall, IDPSA with AODV provides a robust security mechanism for VANETs, enabling trustworthy data transmission and maintaining network integrity, which is essential for safety-critical applications in intelligent transportation systems. In future, explore optimization techniques, like artificial intelligence, to improve the detection and reduce the computational overhead of IDPSA.

REFERENCES

[1] S. Yousefi, M. Mousavi and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives", *Proceedings of International Conference on ITS Telecommunications*, pp. 1-7, 2006.

[2] B. Cherkaoui, A. Beni-Hssane and M. Erritali, "Variable Control Chart for Detecting Black Hole Attack in Vehicular Ad-Hoc Networks", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 1, pp. 5129-5138, 2020.

[3] M. Arif, G. Wang, M.Z.A. Bhuiyan, T. Wang and J. Chen, "A Survey on Security Attacks in VANETs: Communication, Applications and Challenges", *Vehicular Communications*, Vol. 19, pp. 1-9, 2019.

[4] 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 Personal Communications*, Vol. 97, pp. 5099-5114, 2017.

[5] P. Tyagi and D. Dembla, "Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network", *Wireless Personal Communications*, Vol. 102, pp. 41-60, 2018.

[6] Vimal Kumar and Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network", *Proceedings of International Conference on Intelligent Computing, Communication and Convergence*, Vol. 48, pp. 472-479, 2015.

[7] S. Rand Majeed and Mohammed Abdala,"Blackhole Attack Effect Elimination in VANET Networks using IDA-AODV, RAODV and AntNet Algorithm", *Journal of Telecommunication*, Vol. 36, No. 1, pp. 1-6, 2017.

[8] Anu Bala, M. Bansal and J. Singh, "Performance Analysis of MANET Under Blackhole Attack", *Proceedings of International Conference on Networks and Communications*, pp. 141-145, 2009.

[9] R.S. Al-Qassas, "Routing and the Impact of Group Mobility Model in VANETs", *Journal of Computer Sciences*, Vol. 12, No. 4, pp. 223-231, 2016.

[10] K.N. Tripathi and S.C. Sharma, "A Trust based Model (TBM) to Detect Rogue Nodes in Vehicular Ad-Hoc Networks (VANETS)", *International Journal of Systems Assurance Engineering and Management*, Vol. 11, No. 2, pp. 426-440, 2020.

[11] Abdulaziz Alshammari, A. Mohamed Zohdy, Debatosh Debnath and George Corser, "Real Time Vehicular Traffic Simulation for Black Hole Attack in the Greater Detroit Area", *Journal of Information Security*, Vol. 11, No. 1, pp. 1-7, 2020.

[12] Z. Ahmed, S. Naz and J. Ahmed, "Minimizing Transmission Delays in Vehicular Ad Hoc Networks by Optimized Placement of Road-Side Unit", *Wireless Networks*, Vol. 26, pp. 2905-2914, 2020.

[13] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S.S. Choudhary, V.A. Kumar, B. Panigrahi and K.C. Veluvolu, "Black Hole Attack Detection in Vehicular Ad-Hoc Network using Secure AODV Routing Algorithm", *Microprocessors and Microsystems*, Vol. 80, pp. 1-7, 2021.

[14] 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, pp. 1-27, 2022.

[15] U. Okeke and C. Mbarushimana, "Enhancing Security in VANET Against Blackhole Attacks using AODV, K-Means Clustering and PSO", *Proceedings of International Conference on Electrical, Communication and Computer Engineering*, pp. 1-6, 2023.

[16] A. Abdelhamid, M.S. Elsayed, A.D. Jurcut and M.A. Azer, "A Lightweight Anomaly Detection System for Black Hole Attack", *Electronics*, Vol. 12, pp. 1-10, 2023.

[17] C.E. Perkins and E.M. Royer, "Ad-Hoc on-Demand Distance Vector Routing", *Proceedings of International Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999.

[18] P.S. Gautham and R. Shanmughasundaram, "Detection and Isolation of Black Hole in VANET", *Proceedings of International Conference on Intelligent Computing, Instrumentation and Control Technologies*, pp. 1534-1539, 2017.