International Journal of Innovative Research in Technology and Science
ISSN: 2321-1156 www.ijirts.org Volume 11 Issue 6, December 2023

Prevention of Sybil Attack in Vehicular Ad Hoc Network using Network behaviour Analysis (SAPNB)

Purnima Singh, Neelesh Shrivastava
Computer Science and Engineering Department
Vindhya Institute of Technology & Science,
RGPV University, Bhopal, Madhya Pradesh
purnimasingh1227@gmail.com, shrivastava.neelesh@gmail.com

Abstract- A vehicular ad hoc network or VANET is a self-organised group of vehicles connected by wireless links in an infrastructure-free network. This type of network is standalone and cheaper than other networks. In VANET, security is a primary issue to ensure secure data delivery between sender and receiver in a hostile environment. There are some challenges still related to VANET that need to be surmounted in the field of security. This paper presents a security scheme to communicate securely during a Sybil attack on VANET. The Sybil attacker is very harmful, and their reorganisation is also difficult if the network connection is not static and node movement is not fixed. The property of this attack is to present two different identities in the network. The proposed Sybil Attacker Prevention using Network Behaviour (SAPNB) security scheme will detect the attack identification and block their whole misbehaviour activity. The Sybil attacker is identified through their multiple identities and by the number of nodes performing the same activities as the attacker in a dynamic network. The attacker's misbehaviour is enhanced according to time, and after some time, the performance of the whole network is dumped in a dynamic network. The attacker has been considered in simulation, and in both scenarios, the Sybil attacker is active in misbehaviour. The proposed security scheme provides better results and completely turns off attacker nodes in VANET. The proposed SAPNB security scheme provides better results and completely turns off attacker nodes in VANET.

Keywords: Sybil Attack, Security, VANET, Routing, Misbehaviour

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) represents a specialised subset within the broader domain of Ad-hoc Networks, where the communication nodes predominantly consist of vehicles. This unique network type is designed to operate seamlessly with numerous highly mobile nodes, often dispersed along various routes. In VANET, vehicles establish communication not only amongst themselves (V2V) but also with the infrastructure or Roadside Units (RSUs) for additional communication services (V2I or V2RSU) [1]. The infrastructure, represented by RSUs strategically positioned along roads, facilitates communication between vehicles and RSUs through Wireless Access in the Vehicular Environment (WAVE) technology. WAVE communication plays a pivotal role in enhancing passenger safety by updating vehicle information and managing traffic flow, thereby improving pedestrian and driver safety and the overall efficiency of the traffic management system. Typically, VANET design encompasses three key components: Trust Authority (TA), Roadside Unit (RSU), and On-Board Unit (OBU). The TA, acting as a third party, is utilised by both the RSU and OBU, assuming responsibility for controlling and managing the entire network.

Notably, current collaborations between vehicle manufacturers and the transportation industry involve equipping each vehicle with wireless capabilities to facilitate communication between vehicles and infrastructure. VANETs, rooted in Mobile Ad-hoc Network (MANET) principles, leverage vehicle nodes within the system to establish communication between vehicles and fixed infrastructure. Within the context of VANETs, fast-moving vehicles executing large-scale operations in urban areas, suburbs, and highways are a defining characteristic. The behaviour of vehicles, influenced

by or in response to transmitted messages, plays a crucial role [1][2]. The distinctive features of VANET, including high mobility, rapidly changing network topology, limited routes, and bandwidth constraints, are shaped by the swift movement of nodes. Frequent network fragmentation and signal attenuation caused by obstacles contribute to the dynamic nature of VANETs. Security emerges as a paramount concern, given the infiltration of malicious entities aiming to disrupt network performance [4][5]. Of all VANET security concerns, one that has garnered relatively less attention is the unique composition of typical VANETs, involving RSUs, OBUs, proxy servers, administration application servers, vehicles, registration authorities, and location-based applications. This article unfolds in six sections. Section 1 provides an introduction, while Section 2 delves into the related work on VANET security. Section 3 explains the proposed SAPNB mechanism, addressing security concerns related to Sybil attacks. Section 4 outlines the SAPNB algorithm, and Section 5 elaborates on the outcomes. Finally, Section 6 encapsulates the conclusion and outlines future work for the proposed SAPNB system.

II. RELATED WORK

This section mentions the recent previous work proposed by different authors. Here, one is to contribute some new research concepts. Some works against attacks or malicious vehicles are as follows: In this paper [6], the Sybil attack was identified through a two-step process. Firstly, an estimation of the vehicular population on the road was made, followed by an evaluation of network performance by the computation of the packet delivery ratio (PDR) within the network. The calculation of path loss depends on several variables, including the gearbox power, the specific physical phenomena involved, and the alterations in topology resulting from the rapid movement of vehicles. The Road Side Unit (RSU) remains stationary along the road, resulting in consistent transmission power and physical characteristics. This paper [7] proposed a security methodology to mitigate the risks provided by black hole attackers in Vehicular Ad hoc Networks (VANETs). In the context of 6G-VANET, the absence of security guarantees exposes the system to potential risks, wherein certain cars that exhibit misbehaviour or malicious intent might compromise the provision of high-quality services. Furthermore, this vulnerability may extend to endangering the safety of user vehicles. Consequently, identifying misbehaving or hostile vehicles has become a crucial endeavour within the security realm in Vehicular Ad Hoc Networks (VANETs). This paper [8] presents the proposed swarm algorithm for detecting attacks aimed at routing in VANET networks. The algorithm is based on IWD (intelligent water drops) and uses the trust model. IWD has the following advantages: it is used in applications that can adapt to changes and has a high speed of operation. It is very important in dynamic moving networks where nodes move at high speeds, and the network topology is unstable. This paper [9] explains the proposed security framework to secure vehicular communications in ad-hoc networks. This security framework is termed the hybrid key cryptography method and is mainly aimed at securing V ANET in a unique manner through which vehicular communications are secured.

In this paper [10], the author mainly concentrates on the hole generation attack, in which the malicious or attacker drivers inside the network break the links by reducing their speed or boosting their speed to create holes. They proposed a novel Robust Routing Protocol (RRP) for securely sending messages between source and destination by surviving a hole generation attack. This paper [11] proposes a new hybrid position-based secure routing protocol (PBSRP). It compares its security features with the Highest Level in Radius (MFR) and Boundary Node (Highest Level in Radius) routing protocols. (B-LIM). A security module using a key-to-station key agreement protocol has been added to this protocol to prevent various system attacks. This paper [12] proposes a security mechanism that detects black and grey-hole attacks in vehicle delay-resistant networks (VDTNs). In addition, this security system includes an incentive mechanism to support the interaction of nodes or vehicles. This paper [13] proposes an effective and secure method for identifying and protecting against attacks with finite flooding of UDP for various types of IP spoofing.

When malicious actions are detected or identified, they can be further classified by type of random spoofing, subnet spoofing, or fixed spoofing by analysing the hash for the characteristics of the original IP. This paper [14] offers publishing/subscription support for the VANET environment. This hybrid environment consists of stationary or stationary stations for collecting and collecting information and mobile vehicles. This approach does not include GPS or navigation systems or identified or stored vehicle location information in the proposal, and this paper [15] proposed a mechanism for consistent communication in VANET through the proficient routing protocol. Suppose malicious nodes are there in a VANET. In that case, they may try to reduce network connectivity and undermine the network's security by pretending to be cooperative. Still, in achieving this, they are dropping any data they are predestined to pass on. In this paper [16], the conviction calculation is based on the vehicle's position. The sender vehicle broadcasts its route request message (RREQ) to find a secure location within the communication range in the network. The sender vehicle receives the route reply message (RREP) from various vehicles. The source vehicle computes the ratio of vehicles to determine whether a particular location is trusted or not. Computation of trusted location using RSU- Source vehicle now asks RSU about location. In this paper [17], they have understood a VANET in which nearby vehicles can communicate in the same direction only with those available within the network range. Geographical positioning and timing-related conditions are fulfilled with global positioning service receivers. There is no disturbance in getting the time instantaneous at the receiving or sending sides.

III. PROPOSED SECURITY SYSTEM

In the research endeavour titled "Sybil Attacker Prevention using Network Behavior (SAPNB)," the primary objective is to develop a scheme for detecting and preventing Sybil attackers in Vehicular Ad-hoc Networks (VANET). Given the mobile nature of vehicles and the open communication medium in VANET, the susceptibility to various security risks is significantly heightened. The research assumes a scenario with a single attacker, without collisions between malicious nodes, entering the network under a singular identity. Two primary methods for Sybil attacker identification are fabrication of identities and the use of stolen identities (masquerading). The chosen approach focuses on the former, as VANETs lack restrictions on identity creation. Following the implementation of the attack module, a profile table is generated during simulation using the abstract window toolkit. The network behaviour-based technique is then applied to detect misleading nodes and the volume of packets captured by the Sybil attacker node in the network. Subsequently, a cooperative protection system is designed, wherein neighbouring nodes' IP addresses are scrutinised. If a node exhibits suspicious behaviour by sending different identifications to more than two distinct senders' vehicles, the preventer nodes collectively block that node. The accurate information is disseminated to all sender nodes, prompting them to cease data transmission through the identified attacker node. Vehicular ad hoc networks are identified as more vulnerable than existing networks due to their infrastructure-less nature, dynamic topology, distributed network, and on-demand routing. While acknowledging the presence of various attacks in every layer of this platform, the research concentrates on securing the network specifically from Sybil attacks, distinguishing between scenarios where only one of the attacker's identities is active at a given time and simultaneous Sybil attacks. The proposed SAPNB scheme relies on network behaviour analysis in real-time. The prevention module is executed if the scheme identifies multiple identities simultaneously and the attacker captures packets from any sender. The preventer node blocks the attacker node and broadcasts the Sybil attacker's behaviour information to all nodes. This ensures awareness of the attack behaviour, prompting sender vehicles to check the information transfer record. If the attacker's ID is identified, the existing path is disabled, and a route packet is rebroadcasted with messages of blocked node IDs, facilitating the discovery of a fresh route without the participation of the attacker node. The research employs Network Simulator 2 to analyse network behaviour,

considering parameters such as packet delivery ratio, throughput, routing overhead, attacker node IDs, and true positives and false positives. True positives indicate the correct identification of a particular node as an attacker, signifying the effectiveness of the proposed protection. The low percentage of false positives, where normal nodes are falsely detected as attackers, underscores the efficacy of the protection module. Overall, the proposed approach proves capable of detecting and protecting against Sybil attackers in various scenarios within VANET.

IV. PROPOSED NCBC ALGORITHM

The Sybil detection and protection algorithm is intricately designed, comprising three distinct sections: input parameters, output, and routine execution. In this algorithm, the Sybil attack node's behaviour involves the illicit acquisition of the destination ID simultaneously or at different times. This deceptive manoeuvre aims to mislead the source node, preventing it from correctly identifying the genuine destination node. Consequently, the source node inadvertently transmits data to the Sybil attacker node, compromising sensitive information. The algorithm is strategically crafted to identify and safeguard against Sybil attacker nodes efficiently. The formal description of the algorithm unfolds in a step-by-step manner, meticulously detailing the execution process. The algorithm guarantees a robust and secure approach against Sybil's behaviour. By systematically analysing the input parameters, defining the expected output, and delineating the routine execution, the algorithm ensures a comprehensive and effective defence mechanism. This systematic and methodical approach underscores the algorithm's capability to detect and protect against Sybil attacks, enhancing the system's overall security.

Algorithm: A New Attack and Prevention Scheme against Sybil Attack in Vehicular Adhoc Network
Input Parameters:
Step1: V: No of Vehicles nodes
S_n: the set of source ϵ V
D_n: the set of destination ϵ V
A_1: Sybil attacks different id at the same time
A_2: Sybil attacker different id at different time
Routing: AODV
SAPNB: Sybil detector and preventer
Radio-range: 550
Output: False positive, True positive, infection percentage, pdr, Sybil node identification, NRL.
Routine:
AODV_ Broadcast-rreq(S, D, AODV)
Step2:While(next-hop! = D_n&& node in range)do
Receives packet
Incr sequence number
Forward-pkt to next-hop
Incr hop-count
Step3:ElseIf (D_n found)then
Established route from S_n to D_n
D_n send ack to S_n
Else
Node out of range
End if
End do
// Sybil attacker node behaviour
Step4: If(S_n>1 &&D_n>1 && time== S_n time)then
A_1 in the middle between S_n and D_n
If (S_n broadcast-rreq&&A_1 is next-hop), then
A_1 send false $D_{n_id}$to S_n
S_n trust and send data A_1
A_1 captures and drops data from all incoming S_n
Else If(S_n>1 &&D_n>1 && S_n time is not equal)then
A_2 sends false D_n ID to S_n at different time
S_n trust A_2 as $D_n$node& send data to A_2
A_2 capture or drop the packet
End if
End if
Protection:
Step5: SAPNB watch history profile of all neighbour
If (profile! = normal) then
{
Identifies packet and S_{id}, R_{id}
If(D_{id} = updated by A_{1_id}&& time == S_n-time)then
Check packet drop or capture
Node id set A_1 categories
Else If(D_{id} = updated by A_{2_id}&&time != S_n-time)then

Check packet drop or capture
Node id set A_2 categories
End if
End if
Step6: SAPNB sense the activity of all neighbour
If (next-hop receives && forward! = true && updated id of A_1== D_n $_{id}$&& time == S_n-time) then
Block the A_1 node.
Else If (next-hop receives && forward! = true && updated id of A_1== D_n $_{id}$&& time != S_n-time) then
Block the A_2 node
End if
Research route from S_n to D_n
Eliminate the A_1 and A_2
Fresh route established
Send data and go to step 5 of SAPNB
Stop

V. SIMULATION PARAMETER

The simulation parameters utilised in this study are outlined in Table 1. These parameters form the basis for evaluating the performance of three protocols: normal AODV routing, routing in the presence of a Sybil attacker, and the proposed security scheme. The dynamic network scenario is simulated, and the performance of the proposed scheme is compared with the other two protocols using the specified parameters. The objective is to comprehensively assess and contrast the efficacy of the proposed security scheme in mitigating the impact of Sybil attacks within the dynamic network environment. By systematically measuring and analysing the performance parameters, this study aims to provide valuable insights into the effectiveness of the proposed security solution and its comparative performance against conventional AODV routing and routing scenarios in the presence of Sybil attackers.

Table 1. Simulation Parameter for Deployment of VANET

Parameters	Configuration Value
Simulation Tool	NS-2.31
Simulation Area	1650m*1650m
Routing Protocol	AODV
Network Type	VANET
Attack Type	Sybil
Security Technique	SAPNB
Number of Vehicles	50
Number of RSU	9
Physical Medium	Wireless
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Packet Size	256 Byte
Simulation Time (Sec)	300 Sec

5.1 Results Analysis

This section compares the simulation results of the attack without Sybil and SAPNB. The proposed security scheme gives better results than the previous VANET approach.

5.2 Throughput Analysis [Kbps]

The evaluation of network throughput performance involves calculating the number of packets or bits received at the destination per unit of time. The throughput performance in four distinct scenarios has been graphically represented, focusing on assessing the effectiveness of the proposed Sybil Attacker Prevention using Network Behavior (SAPNB) detection and prevention scheme in Vehicular Ad-hoc Networks (VANET). Notably, the graph illustrates that the proposed SAPNB scheme outperforms in the presence of attackers within the VANET environment. In scenarios involving the presence of attackers, the throughput is nearly negligible. However, introducing the proposed SAPNB scheme demonstrates significantly enhanced throughput performance, reaching a maximum level. This outcome signifies the superior routing performance offered by the SAPNB scheme within the dynamic network setting. The higher throughput achieved by the proposed scheme underlines its

efficacy in mitigating the impact of Sybil attacks and ensuring the efficient and secure transmission of data in VANET.

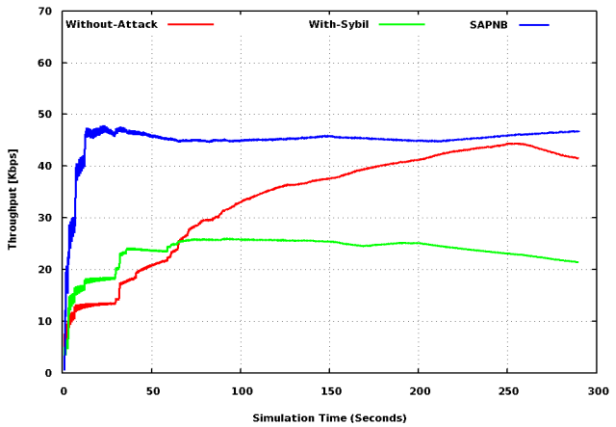

Figure 1. Throughput Analysis

5.3 Normal Routing Load

The packet transmission process involves the sender disseminating packets throughout the network to determine the destination. Each node within the network forwards these routing packets until the destination is successfully located. The graph presented here scrutinises the routing overhead in three scenarios: normal operation, the presence of an attacker, and the utilisation of the proposed security scheme. The routing overhead is notably lower in scenarios without and with an ongoing attack, particularly in the initial 100 seconds. The reduced routing overhead during this period can be attributed to the sender's search for the receiver. However, if, during this search, a nearby Sybil attacker is present, misidentification of the receiver may occur.

Consequently, the route reply message sent to the sender by the misidentified receiver leads to the inability of the actual sender to identify any valid paths. In such cases, the attacker intercepts and drops the data packets, initially contributing to lower routing overhead. Comparing the normal and proposed security scheme scenarios, it is evident that both exhibit higher routing packet numbers. However, this increased routing packet count is accompanied by a corresponding increase in data reception, ensuring a more efficient network operation with minimal overhead. This emphasises the efficacy of the proposed security scheme in maintaining robust data transmission capabilities even in the presence of potential attacks, highlighting its effectiveness in enhancing network performance.

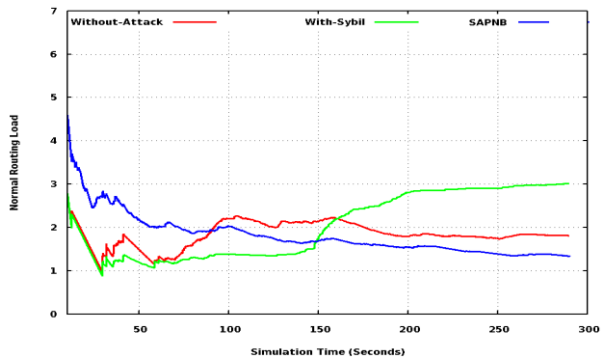

Figure 2. Routing Load Analysis

5.4 True Positive & False Positive Analysis

The graph under consideration provides insights into true detection analysis, offering a glimpse into the misbehaviour of nodes within the VANET. True detection, which reflects the accurate identification of malicious nodes in the network, is crucial for minimising data drops and ensuring the network's overall integrity. The detection of attackers is determined by analysing both the False Detection Ratio and True Detection Ratio. A high True Detection Ratio, as depicted in the graph, indicates that the presence of attackers in the network is either negligible or nonexistent. This outcome reflects a superior performance of the network, signifying its resilience against potential threats.

Additionally, the drop percentage in the network is negligible, further reinforcing the robustness of the network in effectively identifying and neutralising malicious nodes. The graph illustrates a scenario where attackers are positively detected, and the True Detection Ratio exceeds 98%. This outcome underscores the network's capability to accurately identify and mitigate the presence of attackers, thereby contributing to a secure and reliable VANET environment. The high True Detection Ratio is a key indicator of the effectiveness of the security mechanisms deployed, showcasing the network's ability to distinguish between normal and malicious behaviour and respond accordingly. False detection refers to instances where the network

security system incorrectly identifies normal behaviour as suspicious or malicious. A lower false detection rate is generally preferred, indicating a higher accuracy in distinguishing between normal and malicious activities. The detection of Sybil identities in the network is crucial, and an effective system should aim to minimise false detections while accurately identifying and blocking Sybil attacks.

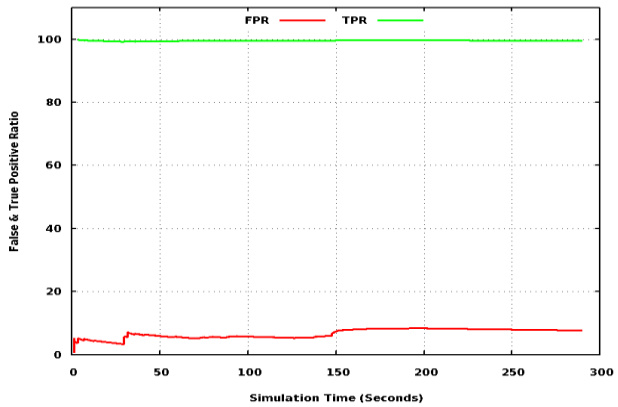

Figure 3. True Positive and False Positive Analysis

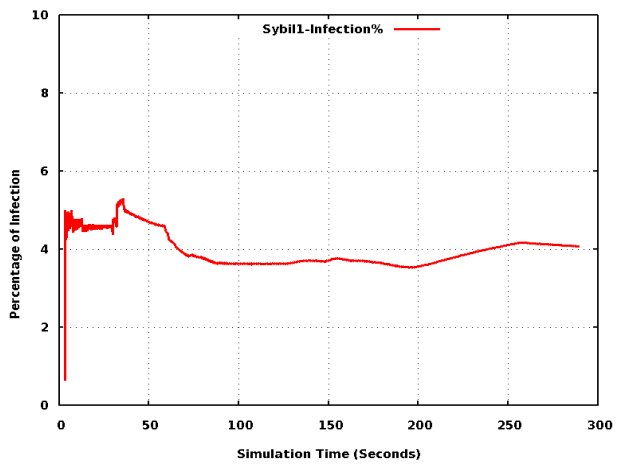

Figure 4. Sybil Attacker Infection Analysis

5.5 Percentage of Sybil Attack Infection

In the graph of Figure 4, two modules of the Sybil attacker are considered, each associated with different Sybil identities. The infection percentage ratio measures the evaluation of the attacker's impact on the network. Initially, in the presence of the attacker, the drop percentage in network performance is determined, reaching a minimum of 40% by the end of the simulation time of 300 seconds. Upon implementing the proposed SAPNB security scheme, the infection count in the network is significantly reduced, practically approaching zero. This indicates that the security scheme effectively mitigates the Sybil attacker's malicious activities and enhances overall network performance.

VI. CONCLUSION AND FUTURE WORK

Vehicular Ad hoc Networks (VANETs) exhibit the remarkable capability to establish networks in diverse settings, providing communication in environments where conventional infrastructure networks are impractical. The varying speeds and destinations of vehicles, all following the same route for timely arrivals, contribute to the dynamic nature of VANETs. Despite their potential, the research on security issues in VANETs faces numerous technical challenges. Bandwidth, processing capacity improvements, enhanced spectral reuse, and frequency allocation are crucial for addressing VANET's technical challenges. The mobility and open media characteristics make VANETs more susceptible to security threats than wired and wireless cellular networks. Hence, developing robust security mechanisms becomes imperative for ensuring secure communication in VANETs. The current research highlights the ongoing need for advancements in security measures, particularly in countering Sybil attacks. Sybil attackers, capable of altering their behaviour and identity, can significantly impact the performance of intermediate nodes in dynamic networks. The proposed security scheme proves highly effective in safeguarding network communication by neutralising the malicious activities of Sybil attackers. The scheme minimises packet dropping, reduces network overhead, and maintains throughput performance comparable to normal network operations. Sybil attackers are adept at dropping packets and assuming multiple identities, so their detection remains challenging. In the dynamic context of VANETs, where vehicles continuously transition between zones, detecting attackers becomes a complex task. Our future work proposes a location-based security scheme leveraging GPS technology to address this. We aim to facilitate more accurate and efficient detection in the dynamic VANET environment by correlating the number of packets dropped by attackers with their GPS-derived

location. This location-based approach holds promise for enhancing the security posture of VANETs in the face of evolving threats.

Reference

[1]. A. G. Hameed and M. S. Mahmoud, "Vehicular Ad-hoc Network (VANET) – A Review," 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), pp. 367-372, 2022.

[2]. S. Parashar and R. Tiwari, "Traffic Control and QoS improvement Analysis in V-to-V and V-to-RSU Communication in VANET," 2023 World Conference on Communication & Computing (WCONF), pp. 1-5, 2023.

[3]. Bassem Mokhtar, Mohamed Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks", Alexandria Engineering Journal, Elsevier, pp. 1-11, accepted 22 July 2015.

[4]. Arun Singh Kaurav and Sushama Rani Dutta, "Detection and prevention from different attacks in VANET: A Survey", International Conference on Physics and Energy 2021 (ICPAE 2021), vol. 2040, 2021.

[5]. Xin-She Yang, Mehmet Karamanoglu, "Swarm Intelligence and Bio-Inspired Computation," 2013.

[6]. Nirbhay Kumar Chaubey, Dhananjay Yadav, "Detection of Sybil attack in Vehicular Ad hoc Networks by Analysing Network Performance," International Journal of Electrical and Computer Engineering (IJECE), Vol. 12, No. 2, pp. 1703-1710, April 2022.

[7]. G. Soni, K. Chandravanshi, "A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack," Sustainable Communication Networks and Application, Lecture Notes on Data Engineering and Communications Technologies, vol 93, pp. 649-663, 2022.

[8]. Vasiliy Krundyshev, Maxim Kalinin, Peter Zegzhda "Artificial Swarm Algorithm for VANET protection against routing attacks", IEEE Industrial Cyber-Physical Systems (ICPS), 2018.

[9]. Thanmayee Karimireddy, Ahmad Ghulam A Bakshi, "A Hybrid Security Framework for the Vehicular Communications in VANET", IEEE WiSPNET Conference, 2016.

[10]. Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International Conference on Communication and Signal Processing, pp. 1175-1179, 2013.

[11]. Sourav Kumar Bhoi, Pabitra Mohan Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International Conference on Communication and Signal Processing, pp. 1170-1174, April 3-5, 2013.

[12]. Yinghui Guo, Sebastian Schildt and Lars Wolf, "Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks", Fifth International Conference on Communication Systems and Networks (COMSNETS), pp. 1-7,2013.

[13]. Karan Verma, Ashok Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", IEEE 3rd International Conference on International Advance Computing Conference (IACC), pp. 550-555, 2012.

[14]. Tulika, Deepak Garg. Manoj Madhav Gore, "A Publish/Subscribe Communication Infrastructure for VANET Applications", IEEE Workshops of International Conference on Advanced Information Networking and Applications, pp. 442-446, 2011.

[15]. Roshan Jahan Preetam Suman, "Detection of Malicious Node and Development of Routing Strategy in VANET," 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016.

[16]. Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and

Routing in VANET," IEEE Symposium on Colossal Data Analysis and Networking (CDAN), 2016.

[17]. TrupilLimbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication," IEEE, 2016.