Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 5, pp. 1539–1554
DOI : 10.47974/JDMSC-1936

Secure and efficient intelligent transport system based on cryptographic authentication mechanism for vehicular ad hoc networks

Hayder Sabeeh Hadi *
Department of Basic Medical Sciences
College of Nursing
University of Kufa
Najaf
Iraq

Ahmed J. Obaid †
Department of Computer Science
Faculty of Computer Science and Mathematics
Kufa University
Najaf
Iraq

Mohammed Ayad Alkhafaji §
Department of Computer Science
College of Technical Engineering
National University of Science and Technology
Dhi Qar
Iraq

Abstract

Vehicular Adhoc Networks (VANETs) are two of the future's most commonly used communication systems. VANETs are designed to protect vehicle drivers by establishing autonomous contacts with nearby vehicles. Vehicles operate as intelligent mobile nodes in ad-hoc networks characterized by mobility and complexity. Cybersecurity in VANET is affected by malicious attacks, which must be detected and prevented. The overall performance of the proposed GPCR-MA with blackhole and Sybil attack is average latency, packet transmission ratio, energy consumption and throughput. It is predicted because the Blackhole attack vehicle sends answers instantly without checking its routing table. These changes in the

* *E-mail:* **hayders.jabar@uokufa.edu.iq (Corresponding Author)**
† *E-mail:* **ahmedj.aljanaby@uokufa.edu.iq**
§ *E-mail:* **mohammed.alkhafaji@nust.edu.iq**

metrics used contribute to the network efficiency deteriorating primarily in the face of an attack. Compared with other related schemes, our proposal provides privacy and security guarantees for VANETs while improving efficiency.

Subject Classification: *68M10, 92B20.*

Keywords: *Ad Hoc networks, Authentication, AI, Intelligent systems, Secure transport.*

1. Introduction

As mobile devices become more widespread and widespread in various fields of our lives, they are needed to function in more unrestrained and changing settings. One specific example is vehicular ad-hoc networks (VANETs), where the application must be used under the disordered and constantly evolving road traffic circumstances. In particular, the focus is on spreading VANET system applications in which information is developed and utilized in the network. The application's outputs are time-critical and must be kept accurate, even when input data changes rapidly and unpredictably [1].

In Mobile Ad Hoc Networks (MANET) [2], Inter Vehicle Communications (IVC) and Road Vehicle Communications (RVC) have recently prepared for the rapid growth of wireless communication networks. The MANET is known as the VANET, emerged from IVC and RVC. It aims to make road safety, well-organized infotainment and driving possible. Today's world is living in warfare, and the battlefield is on the highways. The estimated death toll is around 1.2 million individuals globally annually, and injures about thirty-five times that number, without forgetting that traffic congestion causes an enormous waste of time and fuel [3], [4].

Network components interact with each other via wireless channels in a wireless network. Wireless networking has become increasingly common. Wireless communication networks are divided into two categories based on the form of the communication network infrastructure, as shown in Figure 1.

VANET attacks aim to destroy the attackers' power and adversely affect the network. The attackers launch various attacks in order to cause many problems for network users. All potential attacks are primarily classified into five types with two levels of danger assigned to each. All possible assaults were included in the described classification. The only aim is to help identify these attacks and to manage them in each class [5], [6]. The attack groups of malicious vehicles, brute force attacks,

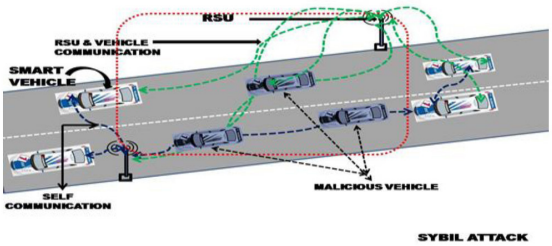

Figure 1

Sybil Attack

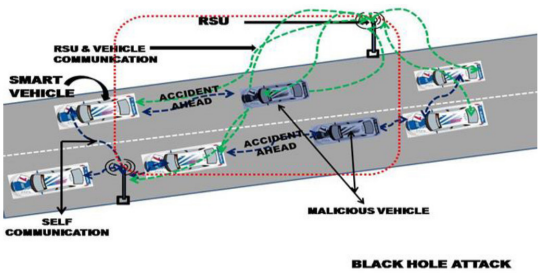

Figure 2

Blackhole Attack

misbehaviour and faulty vehicles, malicious customers, and malicious vehicles are identified and described.

Sybil attack: A vehicle sends many emails to other vehicles in the attack, each email containing an alternate source character, which the originator does not know. The important objectives of the attacker were misunderstood by sending incorrect email messages to other vehicles and permitting separate or (smart) vehicles to exit the highway for the advantages shown to the attacker, as shown in Figure 1.

Blackhole Attack: Vehicles refuse to take an interest or drop a configuration vehicle into the network. All network traffic is moved to a specific vehicle that does not exist, which allows the information to be lost. There are two ways to attack the blackhole of VANET. New customers contact other apps, and consumers refuse to communicate with the wrong messages. Then, with fresh attempts by the user, the situation remains the same: when the communication starts with other users, the neighbouring vehicle communication connection suddenly drops, and the disruption occurs. Because the routing assignment was carried out by this car, as the router client, many vehicles were connected through as shown in Figure 2.

2. Literature Review

VANET supports numerous other vehicle connectivity applications [7]. VANET has many distinct characteristics [8]. Many consider the distinguishing features of a VANET atmosphere. Thus, VANET's characteristics present problems for network design and opportunities to achieve security goals [4]. These are the self-motivated wireless networks for dynamically interchangeable vehicles [9], [10]. Vehicles can join and exit the network dynamically. The vehicle network is used for communication and transmission media without safety. It complicates it and makes it more attack-prone. Increasing network traffic over the VANET means that packet loss and even congestion are increased after contact and transmission. Congestion management and failure of the packet occurs in VANET [11]. The black hole attack one of the safety risks where the car gathered all packets wrongly claiming another path to the destination vehicle without moving them on to the destination [12]. This attack triggered a certain loss of packets over the network during the contact.

A general approach to analyzing car information on an ad hoc network where malicious vehicles can be present while looking for vehicles [13]. A safety-related presentation and accurate quantification of the efficacy of a Sybil attack by the different assumptions [14]. A congestion avoidance of vehicle safety traffic scheme for vehicle ad hoc team signature network. For collecting information from an enemy, the surveillance data collection and monitoring system design. The dynamics of the network and the estimated time of a vehicle capture depending on an opponent's power are also proposed [15].

Traffic and incident warning reports were suggested by a model to defend the vehicle's ad hoc network against service denials and address the solution of attacks [16].

In this section, security at VANET discussed a mechanism to promote confidentiality through geographical information, encryption/decryption and access control [17]. Application of traffic safety cooperative awareness and framework for conducting analysis of other nearby vehicles by combining the output of multiple modules for conducting analysis [18]. Researchers indicated that the VANET framework for security and privacy would include many additional vehicles in malicious vehicles and that data collected by a Sybil attacker should come from several different vehicles, knowing what has already been described, suggesting a slight weight and scalable mechanism for detecting attacks on Sybil [19]. The

suggested and demonstrated application of the method of attack decomposition for deriving attack matrices and the potential use of a decomposition technique in vehicle capture attack security of the enemy model relates to the difficult problem of NP optimization by demonstrating the purpose of the vehicle capture attacks that can be decomposed by the logical heuristic algorithm [20]. In an active safety case, VANET information has been activated and cooperated, and the degrees of freedom available for position forge have been demonstrated in two attacks that require a single position forging low energy compared to sophisticated movement and forging fast, potentially having a large impact on road safety [21].

3. Methodology

In this section, we study the simulated blackhole and Sybil attacks in vehicular ad-hoc networks and evaluate their effects on proposed protocol performance. Here, two different types of attacks are also considered: 1) Packet drop attack is a blackhole attack. 2) The network security breaker and forging identities creator is Sybil's attack. This paper uses the GPCR-MA protocol for performance evaluation [22]. In the GPCR-MA vehicle network, the blackhole attacker vehicle claims to have a fresh sufficient route to all the vehicle's requested destinations and absorbs network traffic. If a source vehicle transmits an RREQ message to any destination, an RREP message that contains the highest sequence is transmitted by a blackhole attacker vehicle and perceives this message as coming from the target vehicle or the vehicle with a fresh enough route to the destination. The source believes the target is behind the blackhole attacker and excludes the other RREP packets from another vehicle. The source then starts to send its data packets to the black hole with the assurance that such packets hit the destination.

V2V scenario: Consider two vehicles V_i and V_j that need to establish a common session key sk_{ij}. The source vehicle V_i select a random number $r_i \in Z_q^*$ and gets the neighbor vehicle key $R_i = r_i P$, chooses one of the vacant private key s_i and neighbor vehicle public key S_i in $pkList_i$, gets the current timestamp t_i, computes $\sigma_i = r_i + s_i.h_2\,(S_i, R_i, t_i) \bmod q$, and sends the message $M_i = \{R_i, t_i, S_i, \sigma_i\}$ to V_j. Upon receiving M_i, V_j checks whether $|t_j - t_{cur}| \le \Delta t$, where T_{cur} is the current timestamp, and Δt is the maximum valid transmission interval. The vehicle V_j selects M_i expired the session. For the validity check of S_i, V_j calls the function *validateVehiclePK* using the parameter $pkList_i = \{S_i\}$. If the vehicle V_j will consider M_i as an unacceptable message. Otherwise, V_j checks whether the equation $\sigma_i * P$

$= R_i + h_2(S_i, R_i, t_i).S_i$. Si holds or not. If not, V_j rejects M_i. Otherwise, V_j achieves operations the same as V_i does and sends $M_j = \{R_j, t_j, S_j, \sigma_j\} =$ to V_j. The session key is designed by $sk_{ij} = h_3(R_i, R_j, S_i, S_j, t_i, t_j, S_i.S_j)$ for V_i or $sk_{ji} = h_3(R_i, R_j, S_i, S_j, t_i, t_j, S_j.S_i)$ for V_j. It is evident that $sk_{ij} = sk_{ji}$ since $s_i.S_j = s_j.S_i = s_i s_j P$.

V2MV scenario: A group of vehicles denoted $V_1, V_2, \ldots, V_n$ would also like to establish a common session key sk_n. To achieve that, every V_i $(1 \le i \le n)$ broadcasts $M_i = \{R_i, t_i, S_i, \sigma_i\}$ to all vehicles. After receiving $n-1$ messages m_x $(1 \le x \le n, x \ne i)$, V_i, Vi checks the freshness of all messages. If the freshness is satisfied, V_i calls the function *validateVehiclePK* using the parameter $pkList_i = \{S_x(1 \le x \le n, x \ne i)\}$. If the function returns false, V_i terminates the process. Otherwise, V_i checks whether the batch verification equation $(\sum_{x=1,x\ne i}^{n} \sigma_x) . P == \sum_{x=1,x\ne i}^{n}(R_x + h(S_x, R_x, t_x).S_x)$ holds or not. If not, V_i terminates the process. Otherwise, V_i calculates the common session key as $sk_n = h(\{R_x, S_x, t_x(1 \le x \le n, x \ne i)\}, s_i.S_1 \ldots S_{i-1} S_i \ldots S_n)$.

3.1 *Integration of Blackhole Attack with GPCR-MA*

In the first step, we modified the GPCR-MA and added the Blackhole Attack function for the network. We need to define any vehicle as a blackhole. In the second step, apply the blackhole attack on the vehicle. The blackhole attack can be applied in one or more vehicles. In the third step, modify the recvRequest of the GPCR-MA. If the vehicle is in a blackhole attack, then the vehicle forwards the fake reply message to the source vehicle as a normal vehicle. It pretends that I am not the destination but have a fresh and shorted path to reach it. In step fourth, modify the GPCR-MA routing table; if a vehicle is a blackhole attacker, then drop the packet information without specifying any reason for dropping the information. The source vehicle was unable to connect to the real destination vehicle; the Blackhole vehicle received all packets from the source vehicle and dropped packet information. The blackhole vehicle always sends the reply message with a higher sequence number see Figure 3.

The vehicular network with blackhole attacks is presented as shown in Figure 4. Here, GPCR-MA with blackhole attack routing is used for the communication. In this scenario, there are two sources: a receiver, a blackhole attacker and another intermediate vehicle in the network. We know that the GPCR-MA with blackhole routing works differently from the original GPCR-MA vehicular routing. The complete working of the

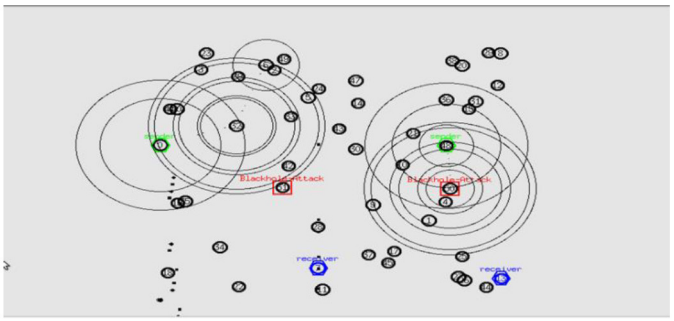

Figure 3

The Blackhole Attack network for 50 vehicles using GPCR-MA routing protocol for VANET

GPCR-MA with blackhole is mentioned in the above section. According to the working blackhole pretend that I am not the destination, but I have a fresh route to reach my destination. As blackhole vehicle receives information from the source or intermediate vehicles, it's directly dropped. The above images fully fill the work of the GPCR-MA blackhole routing. Without connection from the source or destination vehicle, blackhole received the information and dropped it. In Figure 4, a small rectangle box representing the dropped information and a black dotted line (…) is set up route with the blackhole vehicle.

3.2 *Integration of Sybil Attack with GPCR-MA*

In the first step, we modified the GPCR-MA and added the Sybil Attack function for the network, which we need to define any vehicle as the Sybil attack. In the second step, apply the Sybil attack on the vehicle. The Sybil assault can be used on one or more vehicles. The Sybil attack can occur in a vehicle as it operates without a central authority that can verify each communicating entity's identity. In the third step, modify the recvRequest of the GPCR-MA; if the vehicle is the Sybil attack, then the vehicle forward the reply message to the source vehicle as the normal vehicle but with the same vehicle ID at a a different location and sequence number. A Sybil attacker compromises one or more legitimate vehicles that provide the source vehicle with incorrect routing information to draw data traffic towards them. In step four, modify the GPCR-MA routing table entry; if the vehicle is the Sybil attacker, then it sends data information by identity at multiple locations and changes the sequence number. While data information is passed through the Sybil vehicle, it consumes it. In

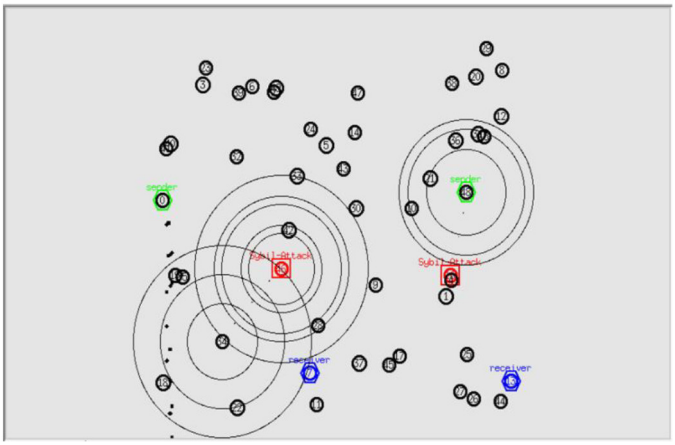

Figure 4

The Sybil Attack network for 50 vehicles using GPCR-MA routing protocol for VANET

step fifth, Sybil Attack tries to stop the simulation before the actual time of the end simulation. Here, Attack moves from one location to a different location with the same identity and shows the network communication completed before the end of the simulation time.

In Figure 5 below, according to the Sybil attack model, vehicles 0 and 48 are the source vehicles that started the communication first. Vehicles 7 and 13 are the destinations that received the information initiated by the source vehicle. In this network, 50 vehicles are considered at random speeds. Vehicles 46 and 16 behave like the Sybil attack. Vehicle 46 is made by Sybil, which compromises vehicle 34.

This presumption allows certain vehicles in the network to be comparable to the source and destination. The simulation is conducted over 100 seconds. The Sybil attack takes place in 70 seconds to 150 seconds. Sybil disrupts the network by supplying inaccurate routing information and falling data packets. Therefore, contact stops earlier than expected. It results in more residual vehicle energy in the network. In comparison, one vehicle with multiple IDs and varying transmission capacity absorbs more capacity than an attacker and a compromiser vehicle.

3.3 *Secured GPCR-MA Protocol for attack prevention*

To secure the network from the attacker, we modified our proposed GPCR-MA vehicular protocol to prevent the attacker in the VANET Network, as shown in Figure 6. The proposed model enhances the

GPCR-MA protocol to fulfil security secure network features. To protect the vehicular network from the blackhole and Sybil attacker. The proposed model uses two Mechanisms: (1). Digital signatures authenticate the RREQ and RREP messages, and (2). The Hash Function can authenticate RREQ and RREP hop account fields. The protocol mainly works by adding a message extension to each GPCR-MA message. Extension messages contain a GPCR-MA packet digital signature with an original sender's private key and a hop count hash function tag.

GPCR-MA uses asymmetric encryption to authenticate all routing messages and hash chain areas, which cannot be modified to authenticate the hop count field. In the proposed model, all fields except the hop count are non-modifiable. The main point is that the two vehicles did not have the same digital signatures. It protects the data transfer information that cannot be changed during transmission in RREQ/RREP messages. The method is authenticated by using the public key of the message's source. If a vehicle receives a routing request, the vehicle checks the signature of the received packet. The vehicle calculates the hop count hash value when the signature is verified. If the RREQ or RREP routing message is equal to or equal to the proposed model value, then the routing message is valid for the hop count and the hash value increment. The proposed model

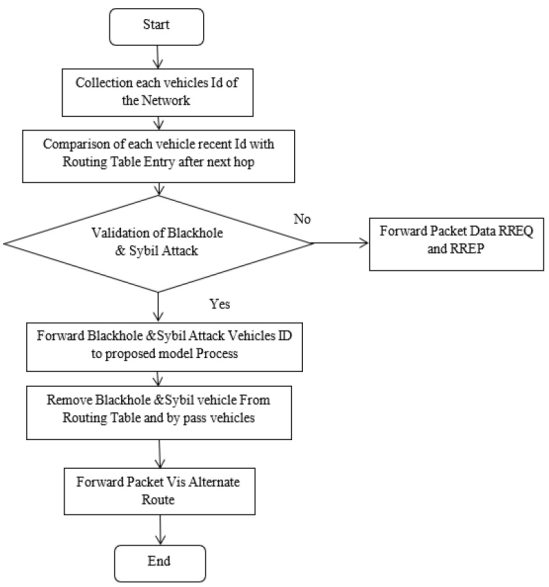

Figure 5

The working process of the proposed model

indicates that any vehicle uses a digital signature to sign all fields for information generation or transmission.

The first step modified the packet structure of the GPCR-MA to the RREQ and RREP messages. Which added the digital signature, hash value and maximum hop count for every vehicle. In the second step, design the session key by sender or receiver. These sender and receiver session keys are designed for the digital signature. In the third step, the random seed value values for the random function are set. In the fourth step, change the sendRequest function of the GPCR-MA by adding the digital signature. Which changes the index value by adding MSG_HASH in the sendRequest

$$Digital - Signature = index + MSG\_HASH;$$

A RREQ packet is generated using the hash value algorithm after computing the digital signature in the sendRequest function. In the sixth step, make the change of recvRequest function in the GPCR-MA, the established message is reserved, and the digital signature, as well as hash value, is also designed. Now verifying both the session key designed by the sender and received in every hop. If the session key is validated, then the same GPCR-MA process will continue; if not validated, then drop the packet because of the signature mismatch. Its process is also applied to the intermediate vehicle. Add the digital signature, hop count and hash value to the RREP packet in the seventh step. The eighth step consists of verifying the digital signature and hash value received by the sendReply function against those received by recvReply. In the ninth step, need to verify the digital signature as well as hash values of the vehicles, then the source vehicle sends the information to the destination vehicle; otherwise, it drops the information. The proposed model is used to secure, attack resilient and efficient the network. This protocol is used against the blackhole or Sybil attack to identify and remove from the network.

The vehicular network with attack prevention is presented in Figure 7. Here, the proposed model routing is used for the communication. In this scenario, there are two sources: the receiver, the blackhole attacker and another intermediate vehicle in the network. The proposed model protects the vehicular network from the blackhole and Sybil attack. The proposed model works based on every vehicle's digital signature and hash value. Every vehicle has its session key. The digital signatures are utilized to sustain the identity of every vehicle. i.e., no two vehicles have the same digital signatures. As a vehicle send RREQ messages to the other vehicle, first, it has to digital signature the RREQ message with the hash value. On sending the RREQ message, an intermediate vehicle that

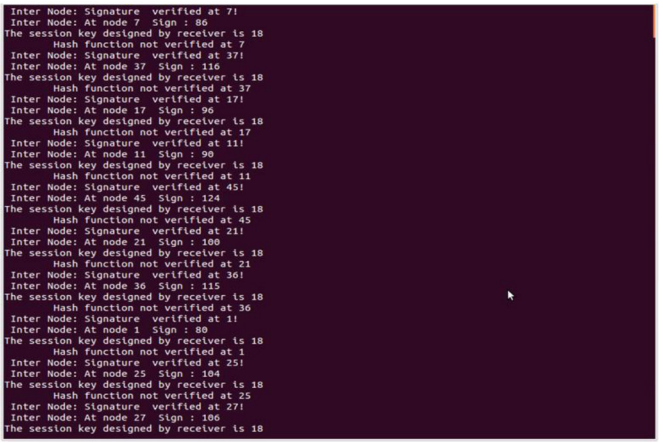

Figure 6

The session key, hash function and verification process of the vehicle

receives this RREQ now has to verify the digital signatures and hash function. By this authentication mechanism, all the attacks or attacker vehicles are excluded from the vehicular network. No attacker vehicle will receive the information from the vehicular network in this way. This proposed model solution is secure and fulfils the standard security requirements.

4. Result Analysis and Discussion

VANETs face specific threats to securities, i.e. attacks to interrupt normal network performance. Blackhole attacks are the type of attack occurring in VANET. Security is VANET's most important function, as misbehaving causes life and time. Various security threats and attacks occur on VANET and disrupt the services provided due to the open wireless nature of communications. The VANET network attacks in the different layers are identified and focused primarily on network layer attacks. During a Sybil attack, a vehicle sends different messages to other vehicles, and every information carry an alternative source ID unknown to the originator. The basic goals of the attacker (malicious vehicle) are confused by transmitting incorrect signals to other vehicles and by allowing specific or intelligent vehicles to exit the road for the assailant's (malicious vehicle) advantage. Several messages comprising various sources of manufactured identity were sent by attackers to another car. The attackers generate many on-road vehicles with the same identity and traffic jam location illusions using false messages.

The effect of the VANET model of mobility was analyzed through a graphic representation in GPCR-MA with Blackhole. Figure 8 shows the average delay for GPCR-MA with Blackhole based on simulation time and traffic density presented correspondingly. The traffic density-based GPCR-MA with blackhole has the lowest value as the simulation time is less. The dropped blackhole packet ratio is very high, which makes the packet delivery ratio in GPCR-MA very low. Figure 7 shows the performance analysis of the proposed model with blackhole attacks regarding packet delivery.

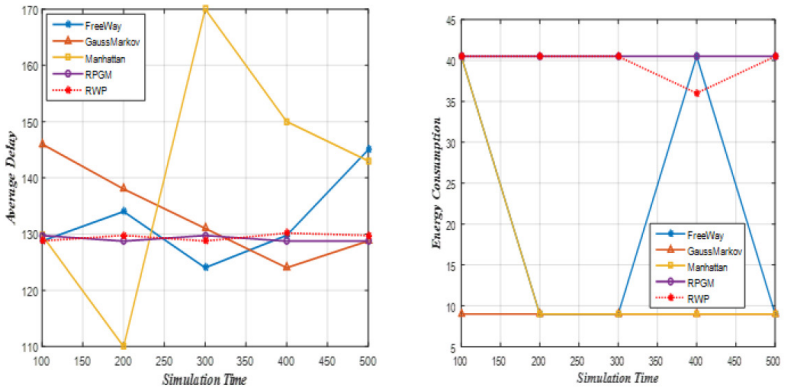

Figure 7

Graphical representation of average delay and energy consumption for blackhole Attack

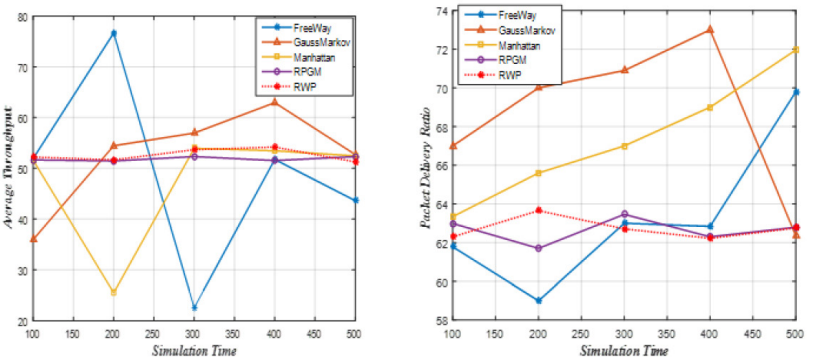

Figure 8

Graphical representation of Average Throughput and PDR for blackhole Attack

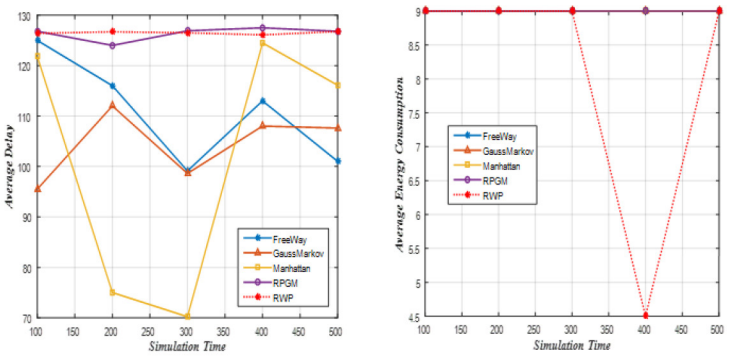

Figure 9

Graphical representation of average delay and energy consumption for Sybil Attack

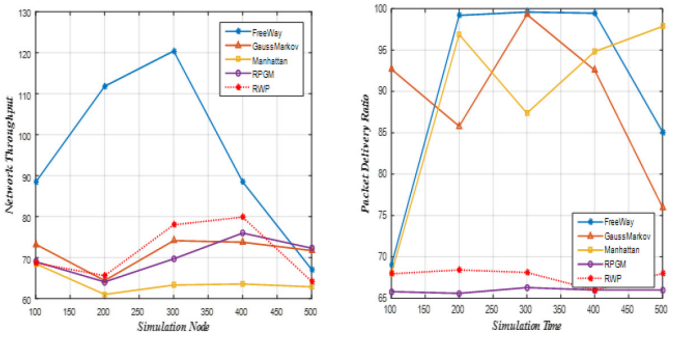

Figure 10

Graphical representation of Average Throughput and PDR for Sybil Attack

The energy consumption based on rapidly changing network traffic and state, i.e. Gauss Markov, RWP, Manhattan model and RPGM, are performed similarly and as network traffic increases, energy consumption decreases in Figure 10. The analysis of the proposed simulation results shows that delay and energy consumption increased during the simulation time. GPCR-Attack detection is used to detect Sybil's attack and block communication.

The performance of throughput and PDR for Sybil-Attack are almost the same for Manhattan, RPGM and RWP for all simulation times, but when we compare these mobility models with freeway and Gauss Markov model of mobility, they performed better than the other three models of mobility as shown in Figure 9. The second scenario simulation time versus

network throughput performance also showed that the freeway is better than Gauss-Markov, Manhattan, RPGM, and RWP in Figure 10.

5. Conclusion

A Blackhole and Sybil attack is one of the main security problems in any VANET network. A summary of various current techniques for recognizing VANET dark opening attacks with their defects is provided. The attacks have two scenarios for the average delay and delivery ratio efficiency parameters. Within a network, the protocol must be redundant and stable. The vulnerability of the proposed GPCR-MA with a Blackhole and Sybil Attack has been examined here to have a more severe impact if there are more vehicles and more route requests. The rate of delay severance during blackhole attacks is 2 to 5 % higher than GPCR-MA. The output of the proposed GPCR-MA is affected by the attack. Based on current research and analysis, we infer that GPCR-MA is more vulnerable to a Blackhole and sybil attack.

References

[1] P. Rani, N. Hussain, R. A. H. Khan, Y. Sharma, and P. K. Shukla, "Vehicular Intelligence System: Time-Based Vehicle Next Location Prediction in Software-Defined Internet of Vehicles (SDN-IOV) for the Smart Cities," in *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations*, F. Al-Turjman, A. Nayyar, A. Devi, and P. K. Shukla, Eds., Cham: Springer International Publishing, pp. 35–54 (2021). doi: 10.1007/978-3-030-82800-4_2.

[2] S. Aluvala, K. Sekhar, and D. Vodnala, "Analysis of Security Threats and Issues in MANETs," *International Journal On Advanced Computer Theory And Engineering (IJACTE)*, vol. 4, no. 5, Art. no. 5 (2015).

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13 (2014).

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20 (2017).

[5] P. Rani and R. Sharma, "IMFOCA-IOV: Intelligent Moth Flame Optimization based Clustering Algorithm for Internet of Vehicle," in 2023 14th International Conference on Computing Communication and

Networking Technologies (ICCCNT), Delhi, India: IEEE, pp. 1–6, Jul. (2023). doi: 10.1109/ICCCNT56998.2023.10307646.

[6] P. Rani *et al.*, "Federated Learning-Based Misbehaviour Detection for the 5G-Enabled Internet of Vehicles," *IEEE Trans. Consumer Electron.*, pp. 1–1 (2023), doi: 10.1109/TCE.2023.3328020.

[7] N. Hussain, P. Rani, N. Kumar, and M. G. Chaudhary, "A deep comprehensive research architecture, characteristics, challenges, issues, and benefits of routing protocol for vehicular ad-hoc networks," *International Journal of Distributed Systems and Technologies (IJDST)*, vol. 13, no. 8, pp. 1–23 (2022).

[8] F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103 (2016).

[9] M. K. Hasan and O. Sarker, "Routing protocol selection for intelligent transport system (ITS) of VANET in high mobility areas of Bangladesh," in Proceedings of International Joint Conference on Computational Intelligence: IJCCI 2018, Springer, pp. 123–135 (2020).

[10] P. Rani and R. Sharma, "An Experimental Study of IEEE 802.11n Devices for Vehicular Networks with Various Propagation Loss Models," in *Advanced IoT Sensors, Networks and Systems*, vol. 1027, A. K. Dubey, V. Sugumaran, and P. H. J. Chong, Eds., in Lecture Notes in Electrical Engineering, vol. 1027. , Singapore: Springer Nature Singapore, pp. 125–135 (2023). doi: 10.1007/978-981-99-1312-1_11.

[11] P. Rani and R. Sharma, "Intelligent transportation system performance analysis of indoor and outdoor internet of vehicle (iov) applications towards 5g," *Tsinghua Science and Technology* (2023).

[12] N. Hussain, P. Rani, H. Chouhan, and U. S. Gaur, "Cyber Security and Privacy of Connected and Automated Vehicles (CAVs)-Based Federated Learning: Challenges, Opportunities, and Open Issues," in *Federated Learning for IoT Applications*, S. P. Yadav, B. S. Bhati, D. P. Mahato, and S. Kumar, Eds., in EAI/Springer Innovations in Communication and Computing. , Cham: Springer International Publishing, pp. 169–183 (2022). doi: 10.1007/978-3-030-85559-8_11.

[13] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 29–37 (2004).

[14] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET," in 2007 IEEE international conference on Mobile Adhoc and sensor systems, IEEE, pp. 1–6 (2007).

[15] A. K. Mishra and A. K. Turuk, "Adversary information gathering model for node capture attack in wireless sensor networks," in 2011 international conference on devices and communications (ICDeCom), IEEE, pp. 1–5 (2011).

[16] H. Hasbullah and I. A. Soomro, "Denial of service (DOS) attack and its possible solutions in VANET," *International Journal of Electronics and Communication Engineering*, vol. 4, no. 5, pp. 813–817 (2010).

[17] G. Y. Yan, G. Choudhary, M. C. Weigle, and S. Olariu, "Providing VANET security through active position detection," in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 73–74 (2007).

[18] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008), Citeseer (2008).

[19] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594 (2011).

[20] P. Tague and R. Poovendran, "Modeling node capture attacks in wireless sensor networks," in 2008 46th annual allerton conference on communication, control, and computing, IEEE, pp. 1221–1224 (2008).

[21] T. Leinmuller, R. K. Schmidt, E. Schoch, A. Held, and G. Schafer, "Modeling roadside attacker behavior in vanets," in 2008 IEEE Globecom Workshops, IEEE, pp. 1–10 (2008).

[22] N. Hussain, P. Shukla, and A. Singh, "Detection of Sybil attack in vehicular network based on GPCR-MA routing protocol," *J. Curr. Sci*, vol. 20, no. 1 (2019).

Received November, 2023