International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Two-Phase Authentication Mechanism for Intelligent Transport System (TAMITS) on VANET

S. Supriya[1]*, Gopika G. S.[2] , D. Devi[3], S. Prema[4]

Submitted: 17/01/2024 **Revised**: 25/02/2024 **Accepted**: 03/03/2024

Abstract: Routing protocols in VANET are primarily determined by the vehicle's location. It is used for preventing basic collisions such as replay and position spoofing attacks. The absence of verification of the vehicle brings about harsh security collisions in VANET. Intelligent transportation systems are therefore proposed to use the Two-phase Authentication Mechanism for Intelligent Transport System (TAMITS) protocol on VANET, which uses a two-phase authentication mechanism. The vehicle's private and public keys are used to transfer data packets across the communication channel. Transmission in the VANET network is accomplished using geographic routing. This proposed solution employs two distinct rounds of location verification. The transmitted data packet is authenticated once it has been sent from the originating vehicle to its next neighboring vehicle. Finally, in the second stage, the increased distance bounding authentication approach is used to verify its location. In the VANET network, the suggested structure protects geographical routing using a location verification approach. On the basis of packet loss and delivery rates as well as throughput and end-to-end delay the TAMITS' performance is assessed. Riverbed Modeler 17.5 is used to simulate the results. By altering the number of vehicles and their speed, the proposed TAMITS protocol's performance is compared to that of the Geographical secure path routing (GSPR) protocol. Because of this, more packets can be sent to the VANET target vehicle via the TAMITS protocol.

Keywords: *Geographical secure path routing; Throughput; bounding; Packet loss ratio*

1. Introduction

Among Manufacturers have shown an interest in the relatively new technology of vehicle ad hoc networking (VANET). VANET is a promising profitable infrastructure framework used in various areas of applications. Vehicular Ad-hoc Network (VANET) deploys enhancing features such as providing safe, secure and comfortable driving to both the passenger and the driver. VANET is typically used for maintaining effective communication among the vehicles inside a network. Most of the applications in VANET have been used by automobile industries. VANET is exceptionally useful in providing real time data to vehicle clients, providing the notification identified with the post-crash, street side handle measures, and traffic identification ability. It is widely used and is a component of a healthy network request. Yet, VANETs are exposed to few dangers because of its security related difficulties like low resilience for error, high mobility, and so forth. The high rates of collisions like eavesdropping, session seizing on the vehicular system are avoided with the help of VANET applications [1]. Because of its high dynamic nature, wireless communication channel, and regularly changing topology, VANET has a very wide scope for attacks. Hence, the VANET is more prone to security threats and challenges.

VANET has faced many obstacles, due to its inherent characteristics such as random changes in system topology, unbounded system size and high mobility (Fonseca & Festag 2006). It is also subjected to several attacks like impersonation, session capturing, identity uncovering, location tracking, repudiation, eavesdropping and DoS[2]. Moreover, the location-based attacks on routing like Sybil attack and wormhole attack (Dok et al. 2010) pose major threats to VANET. To make VANET more secure and protected, it's critical to verify the network's location. This chapter proposes a new VANET TAMITS protocol in place of the current one. As previously mentioned, it's based on the GSPR protocol. It conducts Authentication checks to verify the vehicle's position before approving these data packets using a distance bounding approach.

1.1 Contribution

Rivas et al. (2011) have proposed the GSPR for protective path selection which presents a verification plan for information transmission without a location verification scheme. The SLV technique devised by Lin et al. (2008) proposed numerous schemes such as a distance bounding scheme, authentic verification, and estimation based on geographical region to validate the location of a vehicle [6]. A message does not provide the acknowledgement from the destination. Further, it cannot confirm the location of a

[1] *Assistant Professor, Department of CSE, Sathyabama Institute of Science and Technology, Chennai, Tami Nadu*
*Email: supriya.cse@sathyabama.ac.in**
[2] *Assistant Professor, Department of CSE ,Satyabhama Institute of Science and Technology, Chennai, Tami Nadu*
Email: gopikags41@gmail.com
[3] *Assistant Professor , Department of CSE ,Sathyabama Institute of Sciencse and Technology, Chennai, Tami Nadu Email: devi.cse@sathyabama.ac.in*
[4] *Assistant Professor, Department of ECE, Sri Krishna College of Technology, Coimbatore. Email:prema.s@skct.edu.in*

vehicle universally for a wider range. These issues motivate the development of a solution to verify the location of a vehicle. The proposed TAMITS combines GSPR, authentication checks and the distance bounding scheme. GSPR requires asymmetric cryptography without any secure initialization among the vehicles. Authentication checks enable the verification of the correctness of received timestamp, transmission range and speed information of the vehicle. Distance bounding scheme is used to authenticate the location of vehicles. The integration of this proposed approach is to provide a multilevel security mechanism with a low implementation complexity. Thus, the proposed TAMITS protocol's aim is

1. To develop an effective location verification system for vehicles and authentication techniques in order to ensure VANET security.

2. To provide enhanced security against data packet loss and position based identification using TAMITS protocol.

3. To evaluate the proposed scheme's performance in terms of packet loss rate, packet

4. delivery rate, throughput, end-to-end delay, and control overhead.

2.Related Work

Intelligent Transport Systems (ITS) have demonstrated improvements in the flow of traffic during the past few years. The ITS's purpose is to deliver better by updating data about the highways, and safer driving for all VANET vehicles that participate in the network [7]. The approaches that have been developed over the past several years by numerous researchers are covered in this part.

A. Ullah et al., suggested location-based routing (LBR) rules, that is used to deliver the taxonomy, is presented. This strategy aims to examine the parked cars that are closer to the intersection where the path will be chosen. This method is more expensive and only offers slower packet their delivery, less delays, and shorter data transmission times.

Abumansoor, O et al., offered a number of security concerns as well as fixes for the many problems and difficulties with VANETs. The numerous attack types and methods that are used to address a number of threats were also covered in this article, along with performance data.

Chaurasia, B. K et al., described the adaptive strategy, which regulates traffic depending on automobile communication. As the duration of the queue gets shorter, this technology shortens the time that vehicles have to wait. Utilizing the junction of vehicles, clustering is used to improve this system. This method uses the clustering strategy to determine the density of automobiles that are found in the cluster. The outcomes' accuracy is improved by using the DBCV method. This method, which is used to gather density information, combines cluster and strategic dissemination methodologies. Within the area, clusters are generated based on movement and orientation. The course of the cars is determined using maps and GPS.

3. System Methodology

In TAMITS protocol, authentication is provided by the LMS algorithm, the location of the vehicle is verified by the authentication check and finally the location is authenticated by the two phase authentication scheme [3,4]. The protocol is predicated on the presence of TA in the network and on the presence of GPS- equipped automobiles. Each vehicle transmits the encrypted data packet to its nearby vehicle through radio transmission. Data packet contains the geographical position of the transmitter that is encrypted using geographic hashes. The suggested TAMITS's block diagram is presented in Figure 1

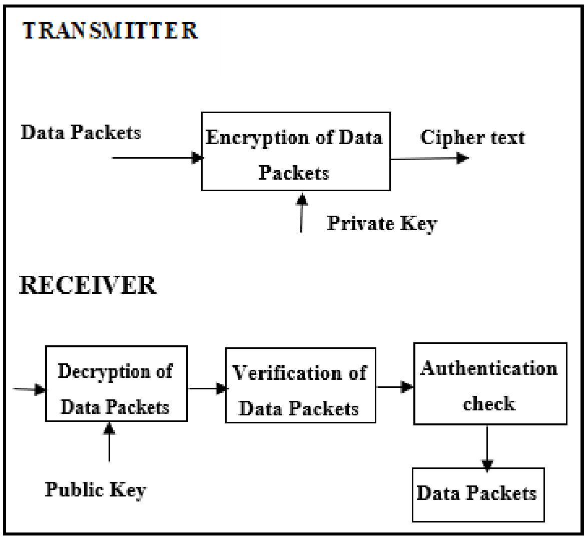

Fig. 1. Block diagram of TAMITS protocol

3.1Data Packets

In TAMITS, each vehicle broadcasts the data packet to its nearby vehicle on a periodic basis. Sharing information with its nearby vehicle assists in confirming the routes and detecting any obstacles that may exist between the group of vehicles. A data packet is constructed using the public key, the arbitrary nonce or alternatively known as Random Nonce generated by the vehicle, the geographic hashes of surrounding vehicles, and the vehicle's ID and position. Table 1 details the format of a data packet.

Table 1 Format of data packet

Vehicle ID	Location of Vehicle	Geographic hashes of the closest nodes.	Public Key	Randomized access

3.2 Geographic Hashes

Let {Xn } be the set of vehicles in VANET. The geographic location of each vehicle {Xni} where i = 1, 2…, n €{Xn } is given by (Ga, Gb). The Ga denotes the geographical location of node in 'a' direction and Gb denotes the geographical location of node in 'b' direction. The direction is determined using a method for scaling the geographical area in conjunction with the global scaling element. Each node Xni transmits a message M successfully using a pair consisting of a public key (puKi) and a private key (prKi)[8]. These keys are generated using the RSA algorithm. The sending node encrypts the message M using the prKi. The receiving node decrypts the message M using the puKi. In geographic routing, each node is aware of its location, which is communicated to its neighbors via beacon signals. It also includes the location of its neighboring nodes that are encrypted using geographic hashes [9]. These hashes constitute an arrangement of the entire number of tokens kept by each node. Every token relates to a particular location of a geographical area which is unveiled to nodes inside the transmission range of that node.

3.3 GSPR Protocol

Geographic routing, or position-based routing, is another term for it. It relies on geographic position information. It requires the determination of location by each node determined for the routing in the network. The source has knowledge of the destination's network location. Without knowledge of the network's structure or the existence of previously discovered routes, geographic routing can route the information to the destination [17]. Geographic routing enables packets to be routed to specific places [10]. When there aren't any nodes in the one-hop vicinity of the destination, the routing protocol produces a failure message. Each of the nodes in the one-hop neighborhood of the target location is a viable destination. (Pathak et al. 2008) implement the GSPR protocol, a secure infrastructure-free geographic routing protocol. Out-of-band communication or shared secret initialization are not required with the GSPR protocol. The GSPR protocol manages security by broadcasting messages to all nodes in the network on a regular basis. The GSPR protocol uses anonymous nodes that are aware of their position to maintain privacy within the VANET. The advantages of GSPR protocol are

1. In the presence of malicious nodes, send messages to the desired destinations.

2. Possibility of detecting malicious nodes and avoiding bad geographic regions that contain

them.

3. Self-authenticated public keys and the position of nodes along the routing path. The GSPR

protocol has drawbacks that include:

4. Due to limited nodes, the GSPR protocol fails to handle scenarios such as sparse networks.

5. Because hello messages are used as control messages in the GSPR protocol, it has a greater routing overhead.

Nodes that have been found to be malicious or defective can be eliminated from the network using GSPR's protocol[11]. Using secure routing paths in the network, the routed packets are expected to arrive at their intended destinations successfully. A modified GSPR protocol is implemented as TAMITS protocol for improving the delivery of packets. This is discussed in the following section.

3.4 Modified GSPR Protocol

The modified GSPR protocol is used to find the route from the source (S) to the destination (D). Let NS be the nonce created by the node S. Let Vni , Vni+1 , Vni+2 ,…Vni+k be the intermediate nodes between S and D. The modified GSPR protocol determines the path between S and D as follows: Let the information packet be the transmitted message from S to D[19,20]. At S, the information packet contains D, source location, NS and the message. The information packet is forwarded to its next hop node. It contains the message and a new location list appended to the current node location and the previously received node location list when it is received by a next hop node. At that point, it performs reliability checks for its verification. The message is transferred to the next hop node and a positive reply is provided back to the previous hop node upon completion of reliability tests. The good response includes the next hop node's geographic hash, a node identifier, and a public key. When you receive an affirmative response, it means that the protocol is working as expected in the one-hop neighbors region. In this way, the previous hop node can make sure the public key of the next hop node is legitimate before proceeding. In this way, the next hop node's geographic hash allows the current node to check for authenticity and make appropriate corrections based on the information it receives. In the case of failure in reliability check verification, the message is discarded from the transmission. If the next hop node is not a D node, its further transmission is carried out to reach D. Finally, the information packet reaches D. On getting the information, node D confirms the integrity of the message [12]. A response is then sent to the S acknowledging the receipt of the acknowledgment, together with a list of locations visited along the way and a list of public keys used to return to the source. An acknowledgement message completes the protocol by sending a signed copy of the routing path taken by the original forward message.

3.5 Reliability Check Mechanism

The time stamp, transmission range, and speed of the node specified in the information packet received by a node are used to perform a reliability check. An old packet will be rejected if it has a timestamp difference between when it was sent and when it is received (Tst) larger than the threshold time (Tth)[18]. If this is not the case, the node will unicast the data packet to the next hop node in the chain. Replay attempts by hostile nodes in the network are successfully thwarted by the reliability check on the timestamp of the received packet. Let Rmax be the maximum distance a node may transmit data over a given time period. The distance between the source and receiver nodes can be estimated using the received signal strength[13]. The data packet is lost if the distance is greater than Rmax. The transmission range reliability check is able to locate the sender vehicle inside Rmax thanks to the reliability check. A vehicle's top speed in any given geographical location is called Vmax. Speeds that deviate from Vmax show that the vehicle is disobedient to local speed laws, according to the manufacturer. As a result, nodes' information packets are deleted from transmission. Once all of the reliability check criteria have been successfully verified, the packet will go through the distance bounding method to verify the vehicle's location. Any other condition results in the packet being rejected.

3.6 Distance Bounding Scheme

To authenticate users and drivers, the VANET uses their geolocation information. Successful authentication provides easy access to the network. Distance bounding scheme is used by assuming two nodes such as verifier node (Vni) and prover node (Vni+1) for authenticating the message in the network. The minimal distance between two nodes in the network is constrained by this function. It is also used for preventing position spoofing attacks by which Vni verifies whether Vni+1 is located in the claimed region. Let us assume that the Vni broadcasts the query message to its next hop node[15-16]. The following is a description of how a distance- bounding scheme works. The nodes Vni and Vni+1 share a secret key using Diffie- Hellman key exchange protocol before its transmission. The first step is for Vni to generate a random nonce and then send a query message to Vni+1 for processing. MAC of nonce generated by the Vni with secret key is an inquiry message. Upon receiving the message from Vni, Vni+1 will respond with its current location, speed, and direction. Subsequently, the message is linked with random nonce produced by the Vni. For the Vni+1, it generates a MAC address and responds to the Vni with that address. Finally, the Vni verifies the response's legitimacy. In this case, the distance between the Vni and Vni+1 is given by d = (((t) -)/2) * c where the query message of the Vni and the response message of the Vni+1 have travelled for the same amount of time ((t)). ¥ is the fixed minimum processing delay that takes place by the Vni+1 and The speed of light is given by the constant c. The minimum distance is used to authorize the location information of the Vni+1.

4. Performance Analysis

This section examines the TAMITS protocol's throughput, latency, and control overhead, as well as packet loss and delivery ratios. Riverbed Modeler 17.5 was used to implement the TAMITS. TAMITS's performance is compared to that of the GSPR protocol in a variety of driving conditions, including varying vehicle counts and changing vehicle speeds. Figure 2 depicts the TAMITS protocol's network topology.

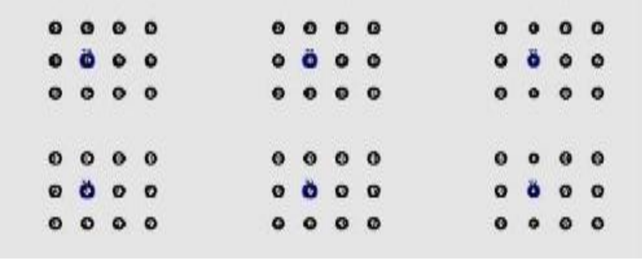

Fig. 2. Simulation Topology of TAMITS protocol using Riverbed Modeler 17.5

Table 2 simulation parameters used to implement TAMITS protocol

Parameters	**Attributes**
Number of vehicles	100
Area	3000m x 1500m
Media Access Control	802.11.n
Simulation Time	20 m/s
Traffic (activity) Source	Constant bit rate (CBR)
Mobility model	Randomized access model
Transmission Rate	1250 kbps
Packet size	1024 bytes
Vehicle speed	20,40,60,80 and 100m/s

4.1 Performance Parameters

The following are the measures used to evaluate the TAMITS protocol's efficiency.

Packet loss ratio: Basically, it's how many packets were lost in comparison to how many were sent, divided by how many were transmitted.

Packet delivery ratio: It's the amount of data delivered to and received from a particular location in relation to the amount of time it takes.

Throughput: It measures how much data can be successfully transported in a specific time period from one location to another in bits/sec. It's sometimes used to check how much of a channel's bandwidth is being consumed. End-to-End delay: The number of seconds it takes for a packet to get from its source to its destination across a network. Control

Overhead: It measures how many control packets are sent out compared to how many data packets arrive at their destination. The following section contains the simulation results.

5. Simulation Results and Discussion

The TAMITS protocol's performance is evaluated by altering the number of vehicles in the network. The simulation was run with the simulation time set to 20 and 100 milliseconds and five connections. GSPR-20 and GSPR-100 are used to denote GSPRs with vehicle simulation times of 20 and 100 m/s, respectively. TAMITS with the number of vehicle simulation time between 20 m/s and 100 m/s are denoted as TMITS-20 and TAMITS-100 respectively. Figure 3 illustrates the packet loss ratios for the TAMITS and GSPR protocols when a variable number of vehicles is used and a simulation time of 20 ms and 100 ms is used.

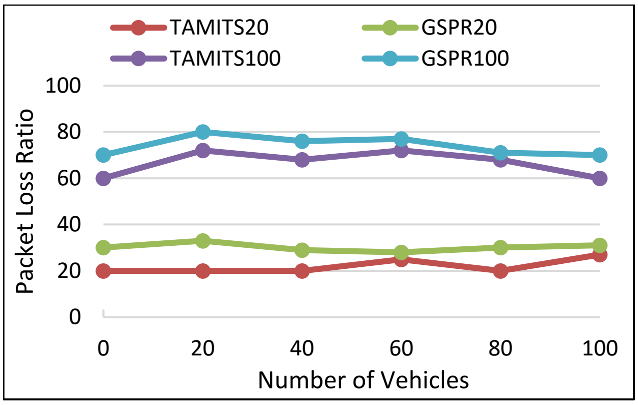

Fig. 3. Packet loss ratio of TAMITS and GSPR protocols under varying number of vehicles

The location-based vehicles in the network can be accurately identified using the TAMITS protocol. This means that the TAMITS-20 protocol's packet loss ratio is 40% lower than the GSPR-20 protocol, while the TAMITS-100 protocol's packet loss ratio is 42% lower than the GSPR-100 protocol. If the vehicles ' speed is increased, the packet loss ratio will go down. TAMITS's authentication check is to blame. As a result, packet loss is effectively prevented by the TAMITS protocol. The TAMITS protocol has a lower packet loss ratio than the GSPR protocol as a result.

Figure 4 depicts the TAMITS and GSPR protocols' packet delivery ratios at simulation times of 20 m/s and 100 m/s with varied numbers of vehicles. According to Figure 4, the TAMITS-20 protocol has a delivery ratio that is 22% greater than the GSPR-20 protocol. TAMITS avoids location-related collisions by utilizing authentication checks in addition to safe routing. Hence, the packet delivery ratio of TAMITS-100 is 26 percent higher than GSPR-100 under the 100 m/s of the simulation time. Due to its authentication approach and lower packet loss ratio, the TAMITS protocol has a greater packet delivery ratio than the GSPR protocol.

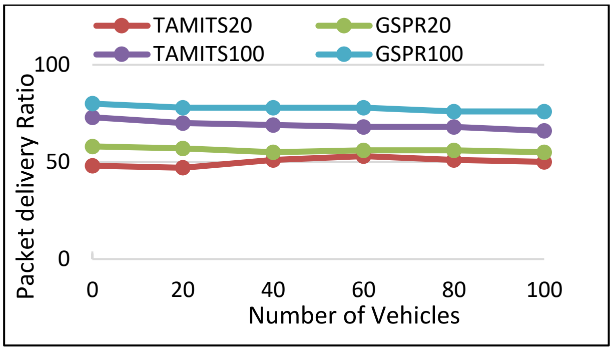

Fig. 4. Packet delivery ratio of TAMITS and GSPR protocols under varying number of vehicles

Figures 5 and 6 demonstrate the throughput and end-to- end latency of the TAMITS and GSPR protocols for varied numbers of vehicles and simulation times of 20 m/s and 100 m/s, respectively.

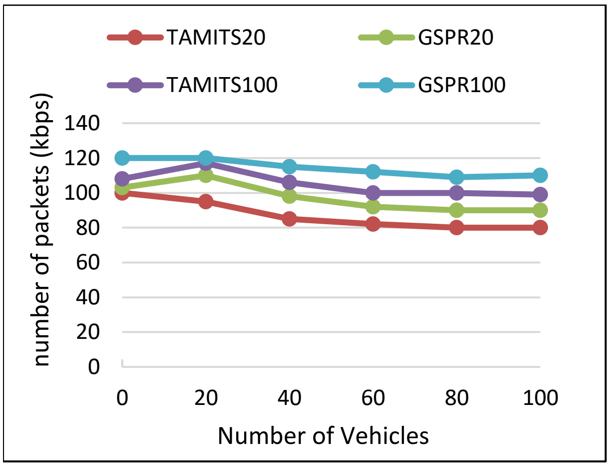

Fig. 5. Throughput of TAMITS and GSPR protocols under varying number of vehicles

As shown in Figure 5, the TAMITS-20 protocol achieves an 18% higher throughput than the GSPR-20 protocol. The TAMITS protocol minimizes transmission call loss and collision rates when the vehicle's simulation speed is increased to 100 m/s. This means that the TAMITS-100 protocol offers a 10% boost in performance over the previous GSPR-100 protocol

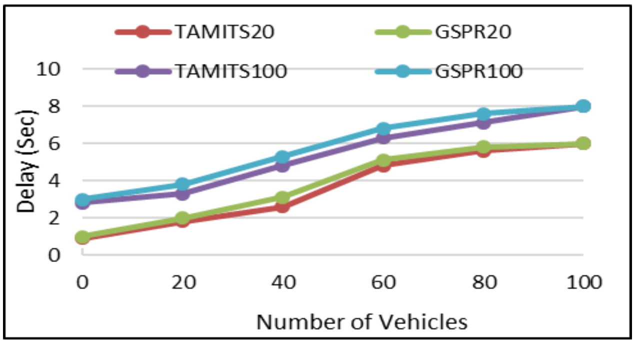

Fig. 6. End to End delay of TAMITS and GSPR protocols under varying number of vehicles

As seen in Figure 6, the TAMITS-20 protocol has an 18% longer delay than the GSPR-20

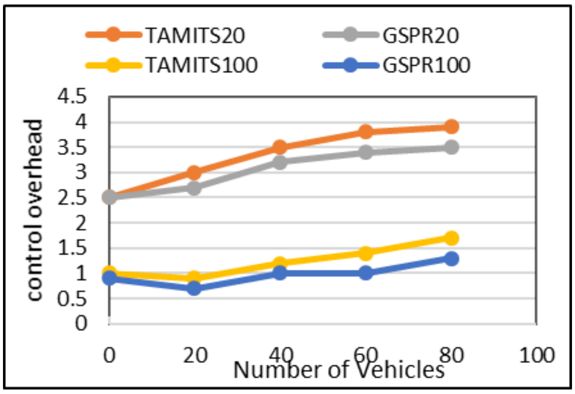

Fig. 7. Control Overhead of TAMITS and GSPR protocols under varying number of vehicles

TAMITS-20 protocol has a 15% reduced overhead than GSPR-20 protocol, as shown in Figure 7. There is an increase in simulation time, as well as more frequent route alterations and the activation of TAMITS protocol's route finding mechanism. Thereby, GSPR -100 protocols overhead is 17 percent more than TAMITS -100 protocols. Due to the use of GPS-based location services, which do not require reestablishing the path when disrupted by fast-moving vehicles, the TAMITS protocol has minimal overhead.

The TAMITS protocol's performance was examined by altering the network's vehicle speed, as depicted in Figure 8. In the network, vehicle speeds were adjusted at 20 m/s and 100 m/s to study the simulation. GSPR with 20 and 100 simulation times are denoted as GSPR-20 and GSPR-100 respectively. TAMITS with 20 and 100 simulation times are denoted as TAMITS-20 and TAMITS-100 respectively. Figure 9 shows the packet loss ratios for the TAMITS and GSPR protocols at 20 m/s and 100 m/s vehicle speeds, respectively.

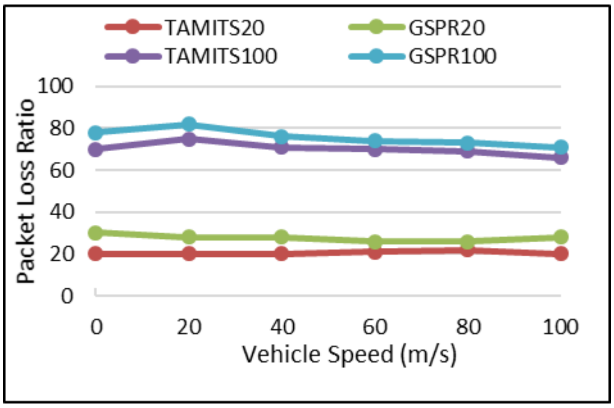

Fig. 8. Packet loss ratio of TAMITS and GSPR protocols under varying speed

The vehicle's speed was varied from 20 m/s to 100 m/s, and figure 8 demonstrates that the TAMITS protocol's packet loss ratio is 48% lower than the GSPR protocol. Since TAMITS uses authentication checks in addition to secure routing, the location related collisions are avoided, thus TAMITS protocol produces lower packet loss ratio compared to GSPR protocol. Figures 9 and 10 demonstrate the TAMITS and GSPR protocols' packet delivery ratios and throughput at speeds of 20 m/s and 100 m/s, respectively.

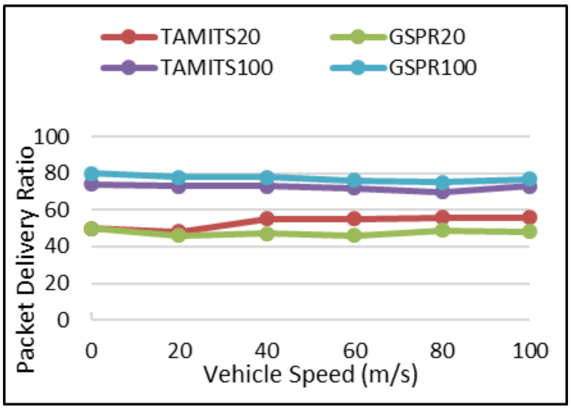

Fig 9. Confusion Matrix on Decision Tree

Figure 9, shows results of the packet delivery ratio of TAMITS-20 as 30 percent higher than GSPR-20. Since TAMITS uses reliability of links in addition to secure routing between vehicles, the location related collisions are avoided in the transmission of data packets between vehicles. According to the simulation results, employing the TAMITS protocol allows them to send more data packets per second.

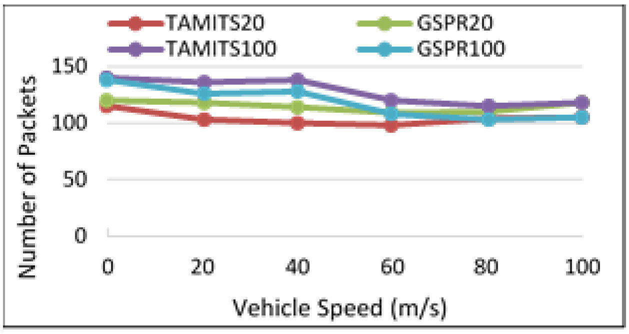

Fig. 10. Throughput of TAMITS and GSPR protocols under varying speed

Figure 10, brings to light the throughput of TAMITS-20 as 20 percent higher than GSPR-20. Simulations show that using the TAMITS protocol increases data transmission rates. The simulation results show the ability to deliver higher throughput compared to GSPR protocol by implementing TAMITS protocol.

6. Conclusion

This chapter proposes the TAMITS protocol, which employs authentication check, connection dependability, and a distance bounding authenticated scheme to validate a vehicle's location in the network. TAMITS protocol provides security against position based vehicle collision. In order to provide secure geographical routing in VANET, it also uses a layered secure technique to protect location-based routing and its services. Using Riverbed Modeler 17.5 simulator tool, the comparative analyses of TAMITS simulation results are carried out. This results in lower packet loss ratios and higher packet delivery ratios as well as increased throughput as well as increased delay and decreased overall overhead. The planned TAMITS, on the other hand, does not address the major invasion of privacy that drivers and VANET users experience. It also is not able to handle privacy attacks such as identity revealing and truthfulness to the forwarded packet.

Reference

[1] K. Abboud and W. Zhuang, "Stochastic modeling of single-hop cluster stability in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 226-240, 2016. doi:10.1109/TVT.2015.2396298.

[2] M. Abu Talib et al., "Systematic literature review on Internet-ofVehicles communication security," *Int. J. Distrib. Sens. Netw.*, ISSN: 1550147718815054 14, vol. 14, no. 12, 2018. doi:10.1177/1550147718815054.

[3] O. Abumansoor and A. Boukerche, "A secure cooperative approach for Non line-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 275-285, 2012. doi:10.1109/TVT.2011.2174465.

[4] D. Ameneh and G. R. Akbar, "An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks," *Comput. Electr. Eng.*, vol. 40, no. 2, pp. 517-529, 2013.

[5] M. R. Asaar et al., "A secure and efficient authentication technique for vehicular ad-hoc networks",< 'https://eprint.iacr. org/2016/822.pdf' >, *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5409-5423, 2016. doi:10.1109/TVT.2018.2822768.

[6] M. Ayaida et al., "Joint routing and location-based service in VANETs," *J. Parallel Distrib. Comput.*, vol. 74, no. 2, pp. 2077-2087, 2014. doi:10.1016/j.jpdc.2013.10.004.

[7] S. K. Bhoi and P. M. Khilar, "SIR- A secure and intelligent routing protocol for vehicular ad-hoc networks," *IET Netw.*, vol. 4, no. 3, pp. 185-194, 2015. doi:10.1049/iet-net.2014.0053.

[8] G. S. Bickel, 2006, 'Inter/Intra-Vehicle Wireless Communication'.

[9] S. Biswas and J. Misic, "Deploying proxy signature in VANETs.", Global telecommunication conference: 1-6, 2010. doi:10.1109/GLOCOM.2010.5683526.

[10] Bohlooli and K. Jamshidi, "A GPS-free method for vehicle future movement directions prediction using SOM for VANET," Appl. Intell., vol. 36, no. 3, pp. 685-697, 2012. doi:10.1007/s10489-011-0289-9.

[11] Caballero-Gil et al., "Mutual authentication in self-organized VANETs," Comput. Stand. Interfaces, vol. 36, no. 4, pp. 704-710, 2014. doi:10.1016/j.csi.2013.12.005.

[12] J. Chang et al., "Performance analysis with traffic accident for cooperative active safety driving in VANET/ITS," Wirel. Personal Commun., vol. 74, no. 2, pp. 731-755, 2014. doi:10.1007/s11277-013-1318-2.

[13] Chaudhuri et al., "Identity based secure algorithm for VANET," *Procedia Eng.*, vol. 38, pp. 165-171, 2012. doi:10.1016/j.proeng.2012.06.023.

[14] [14] B. K. Chaurasia and S. Verma, "Infrastructure based authentication in VANETs," *Int. J. Multimedia Ubiquitous Eng.*, vol. 6, no. 2, pp. 41-54, 2011.

[15] L. Chen et al., "A secure ambulance communication protocol for VANET," *Wirel. Personal Commun.*, vol. 73, no. 3, pp. 1187-1213, 2013. doi:10.1007/s11277-013-1273-y.

[16] T. Chen et al., "Trusted routing for VANET", 9th International Conference on Intelligent Transport Systems Telecommunications (ITST), 2009, pp. 647-652. doi:10.1109/ITST.2009.5399276.

[17] T. W. Chim et al., "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189-203, 2011. doi:10.1016/j.adhoc.2010.05.005.

[18] J. Cui et al., "An Efficient Messageauthentication Scheme Based on Edge Computing for Vehicular ad hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 5, pp. 1621-1632, 2019. doi:10.1109/TITS.2018.2827460.

[19] S. Iqbal et al., "Simulating malicious attacks on VANETs for connected and autonomous vehicle cybersecurity: A machine learning dataset," *CSNDSP*, pp. 332-337, 2022. doi:10.1109/CSNDSP54353.2022.9908023.

[20] Lastovetsky, "Heterogeneity in parallel and distributed computing," J. Parallel Distrib. Comput., vol. 73, no. 12, pp. 1523-1524, 2013. doi:10.1016/j.jpdc.2013.08.010.

[21] X. Liu et al., “A Q-learning based adaptive congestion control for V2V communication in VANET,” *Int. Wirel. Commun. Mob. Comput. (IWCMC)*, vol. 2022, pp. 847-852, 2022. doi:10.1109/IWCMC55113.2022.9824995.

[22] S. J. Mohammed and S. T. Hasson, “Modeling and simulation of data dissemination in VANET based on a clustering approach.” International Conference on Computer Science and Software Engineering (CSASE) vol., vol. 2022, 2022, pp. 54-59. doi:10.1109/CSASE51777.2022.9759671.

[23] S. Shaleesh et al., *Vehicle Location Privacy Protection Mechanism Based on Location and Velocity*. DASA, 2022, pp. 800-803. doi:10.1109/DASA54658.2022.9765290.