RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks

K. Balan[1], A. S. Khan[3], A. A. Julaihi[4], S. Tarmizi[5], K. S. Pillay[6]
Faculty of Computer Science and Information Technology
University Malaysia Sarawak
Kota Samarahan, Sarawak, Malaysia

L. F. Abdulrazak[2]
Research Management Center
Computer Science Department,
Cihan University Sulaimani, Iraq

H. Sallehudin[7]
Faculty of Information Science and Technology
University Kebangsaan Malaysia
UKM Bangi, Selangor, Malaysia

***Abstract*—Autonomous Vehicular Ad hoc Networks (A-VANET) is also known as intelligent transportation systems. A-VANET ensures timely and accurate communications between vehicle to vehicle and Vehicle to Roadside Unit (RSU) to improve road safety and enhance the efficiency of traffic flow. Due to open wireless boundary and high mobility, A-VANET is vulnerable to several security threats especially impersonation, denial of service, pollution attacks. This paper presents a novel Received Signal Strength Indicator (RSSI) based public key infrastructure (PKI) to address the above-mentioned attacks. Each incoming signal will be authenticated based on RSSI value and digital signal (obtained using PKI) is utilized for cryptography and communication within the insecure channel. The proposed solution is verified with and without the presence of attacker by evaluating the packet delivery ratio and packet overhead.**

***Keywords*—Autonomous; vehicular ad hoc networks; public key infrastructure; received signal strength indicator**

I. INTRODUCTION

Vehicular Ad Hoc Networks is also known as intelligent transportation systems. The aim is to provide inter-vehicle communication and roadside to vehicle communication to increasing road safety, improving local traffic flow and the efficiency of road traffic by providing accurate and timely information to road users [1], [2]. In VANET, vehicles are used as network nodes as seen in Figure 1. Security necessities are imperative to provide safe communication in VANET. Due to high mobility, security is more challenging because nodes constantly change network topology. Due to its open-access nature, additionally, VANET is powerless against pollution, Denial of Service (DoS), impersonation, and message fabrication attacks. Thought process of the attackers is to alter the message content, to occupy from different malicious attack, to get the information required, send false message and make network resources become unavailable to others. The various security attacks adopted by an attacker such as pollution attack, impersonation attack, DoS attack and fabrication attack do not only invade driver's confidentiality but also pose risks to the driver, which can cause serious harms/injuries or, worse, loss of lives.

Autonomous vehicles are a type of self-driving car in this current technology of world [3]. The number of autonomous vehicles being used on the road is increasing day by day. Self-driving car, driver-less car or robotic cars are capable to perform an action and navigate without human input or driver responsibility. The autonomous car will have its own GPS (Global Positioning System) as function to locate the user destinations [4]. Alongside other technology that has emerged during this time, the idea of autonomous car can be categorized as an excellent idea, however there are still draw back happened. As the autonomous car is wireless, it depends on a system for exchanging data or information between other vehicles in order to avoid collision on the road [5], [6]. The use of wireless sensor network (WSN) system creates an opportunity to the attacker such as hacker to attack the car system and function of the autonomous car.

An attacker could launch pollution attack by sending malicious or useless data to the target vehicles in order to reduce the vehicles performance. The attacker also created a great number of fake messages to interrupt the vehicle and make it malfunction. In addition, some attackers will distract those good vehicles from malicious attacks in order for other attackers to attack successfully.

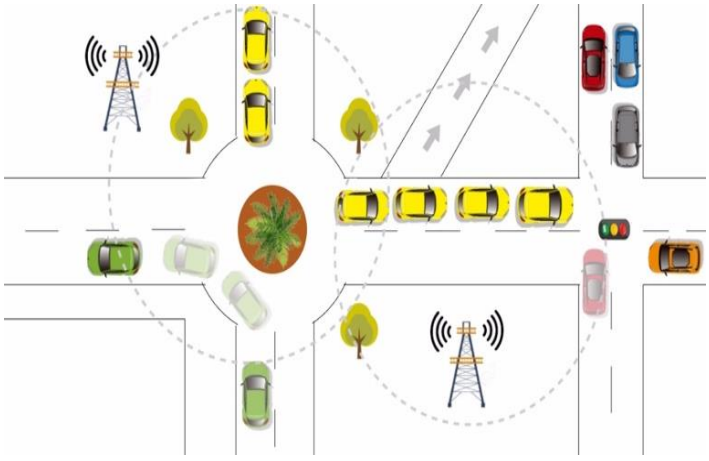

Fig. 1. Basic VANET Structure.

The suggested solution for controlling the vulnerability of VANET system is road side unit that depends on public key infrastructure. Encrypted message can only be decrypted using the owner's private key. Meantime, the proposed solution will request the vehicles to register and road side unit will validate their personal information before accessing to the communication network. The technique used to evaluate the proposed solutions is the measurement of Packet Delivery Ratio and Packet Overhead. It clearly shows the measurement of it based on the proposed solutions with and without attacks. It shows the difference when there is and there is none of the attackers that attacks and disturb the communication network. Firstly, the message is encrypted by public key and then it will decrypt using the owner's private key to read the information or data in it. The technique has enabled the message transfer between two parties in a secure manner, indirectly mitigate the various security attacks based on public key infrastructure. With the aid of road side unit and public key infrastructure, the defense and security of the communication network will increase significantly by allowing the vehicles to register themselves as a valid vehicle in the network. Moreover, the VANET system will become robust and no longer vulnerable to various malicious attacks.

II. Related Works

Timed Efficient Asymmetric Cryptography (TEAC) uses asymmetric cryptography to protect them from attacks [7]. Asymmetric basically uses public and private key in VANET system to validate any user before granting them access to it. Timed Loss Tolerant Authentication (TESLA) is utilized as an authentication technique for broadcast network communication. Although Public Key Infrastructure (PKI) is one of the ways to authenticate different user, but in this case, TESLA can be used to authenticate user instead of using PKI. TESLA is not only systematic for signatures but also more efficient and secure. TESLA also discards used messages if the verification is the out of date.

To enhance In-Vehicle Network Security [8], authentication and encryption is one of the most effective way to provide secureness to a controller are network (CAN) frame. Before that, there is four important issues that needs to be considered. First, key management is essential to provide a good authentication and encryption as well as key update. Secondly, the more the message authentication code (MAC), the more it corrupts the transmission effectiveness. Next, by giving authentication and encryption for CAN frames, it will give the frames a serious delay that will affect the effectiveness the vehicles flexibility. Lastly, the compatibility between the CAN bus that has been improved by authentication and encryption and existing devices must be well label.

Resilient Control Strategy [9] has been presented to refine and enhance the vehicles execution. The strategy that used to control the resilient is a totally new version of Cooperative Adaptive Cruise Control (CACC) where extra estimation algorithm is added into the CACC. This estimation algorithm has three main important components and that is a model-based witness, a slower estimator for the vulnerable attack situation and a Luenberger observer. This algorithm has good functions in it as it can detect the DoS attack as soon as it disrupts the communication network. Thus, it can estimate the number of vehicles that are proceeding in the communication network.

For the transmission of messages [10] in VANET to be transmitted safely, anonymous message authentication has been used in this case. To provide efficiency in authentication, cooperative authentication protocols will be used here. Although there are still several reports of cooperative authentication protocols that fail, success report will still be chosen based on the method of cooperative authentication protocols. Moreover, there is no matching problem here when it comes to cooperative and non-cooperative modes. By using a simulation and analyze it, this protocol does not need mode synchronization while there is no message losses as well even if the density is assigned with 200/km2. Lastly, a binary tree can always decrease the transmission size when the messages are updated for a brand-new group key.

Distributed Aggregate Privacy-Preserving Authentication (DAPPA) [11] manage to obtain an improved version of privacy, good and quick message processing and key guarantee freeness without using a perfect tamper-proof devices (TPD). To solve the message broadcast problem in serious cases, a good solution is that to utilize flexible beacon frequencies for message transmission within a communication network.

An Integrated Circuit Metrics (ICMetric) based on Micro Electro-Mechanical System (MEMS) gyroscope has been proposed [12]. The ICMetrics techniques will generate the symmetric key for data communication and attack detection based on gyroscope sensor device reading. The detection system named as ICMetricIDS is a novel intelligent intrusion detection that is based on ICMetrics in VANETs which able to secure external communication system of the self-driving and able to identify the existing and previously unseen attack for instance fabrication, modification and interception. Advantageously, the experiment demonstrates the proposed security system such as Feed-Forward Neural Network (FFNS)-IDS and k-Nearest Neighbors (k-NN)-IDS will able to identify and block the malicious vehicles in VANETs of self-driving and semi-self- driving vehicles.

INTERLOC has been proposed to demonstrate the detect Sybil attack that gives false information about the vehicle location [13]. The INTERLOC will estimate the area of vehicle that has no error and required an observer to process all the data it received. The vehicles must send the exact location and estimating distance to the observer and the observer will calculate the polygon of intersection point of the vehicles. The result of polygon may be varying due to environment. In preventing any error or false information, the estimated distance between the vehicle and observer will always be updated. Advantageously, the experiment demonstrates that INTERLOC performs better in localization and accurately detect Sybil attack. The high accuracy can improve the traffic safety significantly and making INTERLOC a reliable alter- native to GPS.

An Efficient Anonymous Authentication with Conditional Privacy Preserving scheme (EAAP) has been proposed to

prevent harmful vehicles or RSU to enter the VANET as well as securing the vehicular communication [14]. The purpose of this scheme is to identify and track any vehicles and RSU which had assault the VANET. Besides, EAAP will provide anonymous authentication via five parts which are registration and key generation, Anonymous Certificate Generation, Signature generation, message verification, and conditional tracking. Based on the proposed scheme, they had proved that it give an authentication with low signature verification cost and certificate. Moreover, it able to provide an efficient conditional privacy tracking system to determine the original identity of the harmful vehicles and provide rapid verification for certificates and signature compared to the other previous reported scheme.

An anonymous and lightweight authentication based on Smart Card protocol (ASC) to enhance the performance of authentication in VANET has been proposed [15]. To secure the VANET, ASC has implemented a low-cost cryptographic for validation of messages data and verification of the real identity of vehicles. Besides, they also had proved that ASC can reduce the cost of computational and communication by 50% compared to the other technique. In this scheme, dynamic change of login identity and password change phase without rely on TA (trusted authority) has been provided by ASC to avoid harmful attack while formal security model is used to prove ASC is secure from computational Diffie-Hellman problem.

III. Security Challenges

In any autonomous VANET, the motive of the attackers is to send fake information to other vehicles and get useful information or data for personal benefit. They can flood the memory of the vehicle full of useless data and also send invalid information to other vehicles in the communication network. To confuse the vehicles on the road, the attacker may also distract the vehicles to allow other malicious attack to attack the vehicles in the communication network. The attacker convinces the neighboring vehicles that there is considerable congestion ahead, then enforced them clear path for the attacker. In addition, the attacker impersonates any priority vehicle (ambulance, public servant protocol etc.) so that they can move more affluent and faster in the right side road.

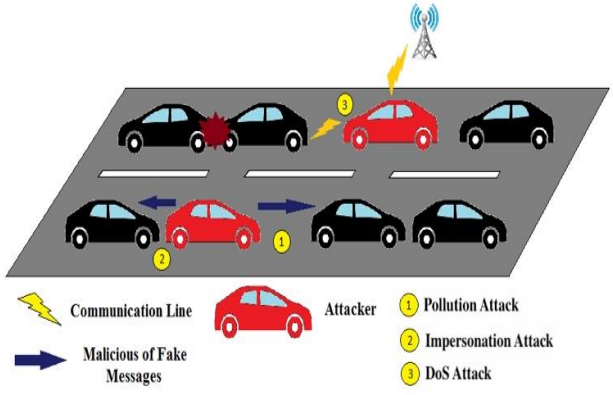

Fig. 2. Scenario on Types of Attack in VANET.

Thus, the attackers may generate Pollution attack, where the attack will only happen if the attacker sends a malicious or useless data to the vehicles until it floods the vehicles memory with bad packet that reduces the vehicles performance (Figure 2). Whereas impersonation attack happens when the attacker steals the identity of the any high priority vehicles on road and try to get benefit of the stolen identity [16]. Next, DoS Attack is an attack that allows the attacker to create large number of fake messages or identities to disturb the data transfer happening between two vehicles that causes jamming and flooding in that particular area. The detailed illustrations of the attacks can be seen in figure 2.

IV. Security Requirements

Based on the above security challenges, it is mandatory to ensure that the communication links are secure enough to perform cryptanalysis. The key three requirements are the confidentiality, integrity and availability to counter the pollution attack, impersonation attack and the denial of service attacks [17].

V. Proposed Solution

This paper proposed detailed architecture for secure communication amongst autonomous vehicles, specifically between the vehicles and vehicles and vehicles to road side units. The idea is to utilize the lightweight and distributed concepts of RSSI localization technique. In this signal strength-based position verification technique, autonomous vehicles will verify the location of other participating vehicles and verifies that at particular time, each physical location is occupied by only one identity. Second, public key infrastructure is utilized during registration process of autonomous vehicles with road side unit. To ensure the freshness of the messages, timestamps are utilized which is first generated by the RSU, and later utilized by all other participating autonomous vehicles lies under the coverage of that particular road side units. The inclusion of timestamp is to ensure that the message is fresh, which consequently minimize the changes of replay or denial of service attacks.

For the proposed solution, road side unit (RSU) will be used to contribute in providing the information of exact location within the database of the system such as bus station, ATM, train station and more. Moreover, vehicle that is in the communication network can communicate with the RSU through vehicle-to-Road Side Unit (V2R) communication. So, in order to discover RSU nearby, vehicle will first send out solicitation packet for discovery. If RSU is successfully discovered, then the RSU will reply by sending a replay in the form of advertisement packet format. Vehicles in the communication network would need to validate their own personal access instead of depending on other communication system. This means that if there are users who want access to the communication network, they would need a proper authorization with an identification for their own following permission. By this, a secure and safe access process will have a positive result in it and this allows the system to get the information or data of the vehicles that enters and exits in the communication network. If there is any abnormality in the information or data of the vehicles that is trying to enter and exit the communication network, this means that there is a

fraud within the vehicles or users. The information of data can also be used to characterize and enhance the access for the vehicles that needs to communicate using the communication network.

There are a few phases and operations that the vehicles need to follow in order to prevent the attacker from altering the message or send fake messages to other vehicles. The first phase is the registration phase [18] where the vehicle must complete the registration by providing a complete an accurate personal data and checked by RSU. The vehicle has to submit important vehicular details such as the car registered number plate, model, etc. and the system would need to verify the information given by the vehicle to see if the vehicle is a genuine node. Once the vehicle registration is complete, the system will send a certificate signed by the certificate authority for communication purpose [19]. This will enable the vehicle to have access to the VANET communication network. During the registration phase for the vehicle to enter the communication network, RSU will check if any of the vehicle in the network is blacklisted. In addition, if there is any unregistered vehicle in the network, that particular vehicles information will be pass to the police to track unregistered vehicles. After that, RSU will be ready to serve any vehicles in the network with all the information RSU had after the registration phase.

In order to overcome the attacks before it takes over the system, RSSI (Received Signal Strength Indication) based localization will be implemented into the system. RSSI is a mechanism to secure the communication channels of vehicles by detecting the attack and provide the location to vehicle when the GPS of the vehicles is not working properly. When a vehicle sends signal to another vehicle for location request, RSSI will authenticate by checking each signal in order to detect any sign of attacks before proceeding by enabling sharing locations. Advantageously, the use of RSSI can help in detecting the attacks and remove it from the system in the earlier stage. The RSSI is based on the localization algorithm using the ratio to overcome the attack [20]. Based on theorem 5 in [20], at least 4 sensors that will monitor the radio signals can prevent user from hiding their location. Suppose that node *i* had obtained a radio signal from node 0, the RSSI will be defined as in equation 1.

$$R_i = \frac{P_0.K}{d_i^{\alpha}} \tag{1}$$

where P_0 is the transmitter power, R_i is RSSI, K is a constant, d_i is the Euclidean distance and □□is the distance-power gradient.

The proposed algorithm is possible to be used to detect attacks such as impersonation. During the receiving of the message, four receiving nodes calculate the physical location of the sender with the sender's ID using equation 2. At any time, if any message from the same physical location with different ID is received, which means that an impersonation attack on VANET. Unfortunately, it is troublesome to calculate the location using equation 2 for each of the participating vehicles to detect the attacks. Considering the fact that all x, y and x_i, y_i locations are the exact same point, attack can be detected by only through continuous recording of the signal strength in any table and later analyzing the ratio of RSSI by comparison to receive the message.

Figure 3 shows the topology for RSSI in an autonomous vehicular communication scenario. Therefore, we let each of the 4 monitoring nodes having an ID as B1, B2, B3, B4 and the impersonation attack node as S1 and S2 in time.

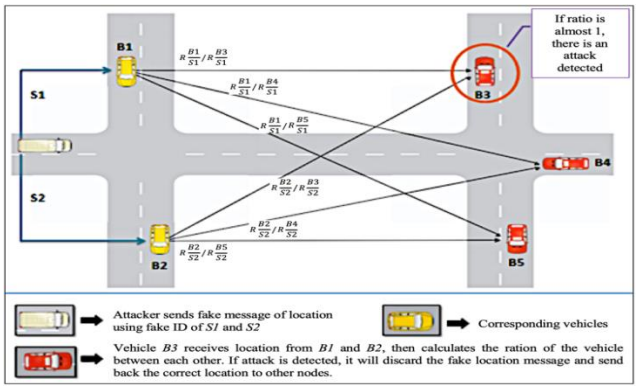

Fig. 3. VANET Scenario with RSSI Localization Implementation.

Let's suppose, there exist an impersonation attacker at any time t_1, it will broadcast a malicious message with its impersonated ID as S1. The monitoring node will record the signal strength value and the impersonated ID. For each of the monitoring node, it will send a message to B1 that consisting the received signal strength from S1. Then, we allow R_i^k to represent the value of signal strength when at *i*, it received the message from sender *k*. After that, the messages are collected from the monitors where B1 computes every ratio as

$$\frac{R_{B_1}^{S_1}}{R_{B_2}^{S_1}}, \frac{R_{B_1}^{S_1}}{R_{B_3}^{S_1}} and \frac{R_{B_1}^{S_1}}{R_{B_4}^{S_1}} \tag{2}$$

and locally stores the values. While at time t_2, the malicious node once again broadcasts the message using an alternate ID which is S2. The nodes that monitor the network will then record the signal strength value from S2 and send it to B1. Then, B1 calculates the equivalent ratio (3) which is

$$\frac{R_{B_1}^{S_2}}{R_{B_2}^{S_2}}, \frac{R_{B_1}^{S_2}}{R_{B_3}^{S_2}} and \frac{R_{B_1}^{S_2}}{R_{B_4}^{S_2}} \tag{3}$$

Therefore, B1 now can identify the attack by analyzing the ratio by comparison at time t_1 and t_2. When the value of the difference in the ratio of the two is close to zero, B1 then determines that an impersonation attack has happened in the area. If the ratios of the signal strength are the same, it indicates that the point of attack to fake the multiple IDs is also the in the same place. Due to that, B1 concludes that there is no attack node. If

$$\frac{R_{B_1}^{S_1}}{R_{B_2}^{S_1}} = \frac{R_{B_1}^{S_2}}{R_{B_2}^{S_2}}, \frac{R_{B_1}^{S_1}}{R_{B_3}^{S_1}} = \frac{R_{B_1}^{S_2}}{R_{B_3}^{S_2}}, \frac{R_{B_1}^{S_1}}{R_{B_4}^{S_1}} = \frac{R_{B_1}^{S_2}}{R_{B_4}^{S_2}} \tag{4}$$

is true, as in equation 4, B1 had detects an impersonation attack. The most important is when the attacker tries to attack the GPS, which is the critical function for the autonomous car, RSSI can detect it and cut the attacks and send back the location to the vehicle so that the vehicle can arrive at the destination safely.

Secondly, PKI with public key technology is utilized to securely transmit the message from vehicle to vehicle or vehicle to road side unit [21]. The information or data of the vehicle is encrypted in a secure form so that nobody can decrypt the data or the information of the vehicle without knowing their own private key. This helps to improves vehicles satisfaction by enabling communications from all around the network. PKI basically generate a digital certificate. By signing the certificate means that the certificate authority (CA) has verified the private key that corresponds to the public key in the certificate and this will be in the hand of the subject that is named in the certificate.

CA is usually a third-party company that provides a completely trusted vehicle a certificate that contains a public key that used to encrypt the data. The certificate can be distributed freely to anyone and it can only be decrypt using the correlated vehicles private key [22]. The private key must be kept securely to avoid anyone else having access to it. For instance, if vehicle A in the communication network wants to send message that contain some important information or data to vehicle B, then vehicle A can use the public key from a trusted association to encrypt the message. The encrypted message can only be decrypted using the vehicles B private key.

To be precise, PKI manage information and data in a way that it will identifies and authenticate the vehicle simultaneously to prevent attackers from hacking into the communication network because it makes it difficult for the attackers to intercept identities. In this proposed scheme, the value of signal strength encrypted with digital certificate of that autonomous vehicle is transmitted through insecure to ensure that the message came from the legitimate sender as shown below.

$$\text{Authentication Message} = [\text{RSSI}_{\text{value}}]_{\text{digital signature}} \quad (5)$$

Once the authentication message is digitally signed by the sender digital certificate, which means that the message belongs to the legitimate sender, thus, chances of impersonate is negligible. In conclusion, with the proposed solution suggested above, it will be able to solve all the three attacks stated above and the vehicles that are communicating between each other in the network would be more secure.

VI. Results and Discussion

This study proposed the RSSI localization algorithm to identify the attack autonomous vehicular networks and provide location to the vehicle when the GPS is not working properly. By using the ratio of RSSI localization from multiples receivers, it is possible to overcome the attack from the attacker by detecting the attack through recording and comparing the ratio of RSSI to receive the messages even though RSSI is time-varying, unreliable in general and non-isotopic radio transmission. The RSSI which is based on the localization algorithm which using the ratio to overcome the attack in this project is presented.

A. Evaluation Parameters

In this paper, Packet Delivery Ratio (PDR) and Packet Overhead (PO) are used as the observed parameters for the proposed solution. Both of these parameters are obtained against the different number of nodes in the network.

PDR is the amount of ratio in packets that are successfully transmitted or send to a goal target that sent by the sender [23]. Moreover, packet delivery ratio is also important to identify problems that might cause a poor throughput. PDR will be used to measure the performance of the vehicles using the proposed solution with attacks and using the proposed solution without attacks in the communication network.

PO is the additional cost incurred by the network due to maintaining latest information in the data packet. While additional information may affect the throughput of the network, in reality, the overhead offers actual information of the network availability.

B. Conceptual Results and Analysis

When there is no attack during the exchange of packet between vehicles, the receiver will receive the same amount of packet send by the sender. As shown in Figure 4, Car A successfully delivered the 10 packets to Car B without any loss of packets.

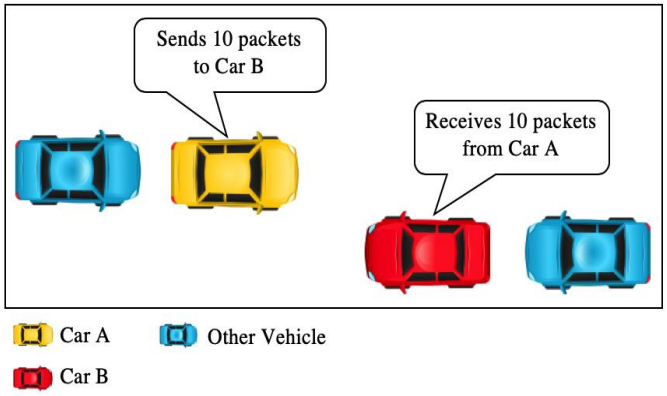

Fig. 4. Packet Transmission without an Attack.

When there is an attack during transmission of the packet between vehicles, the receiving node will receive either a reduced amount or more packet than actual packet transmitted by the sender node. As shown in Figure 5, Car A send the 10 packets to Car B, but when there is an attack, Car B only received 5 packets from Car A.

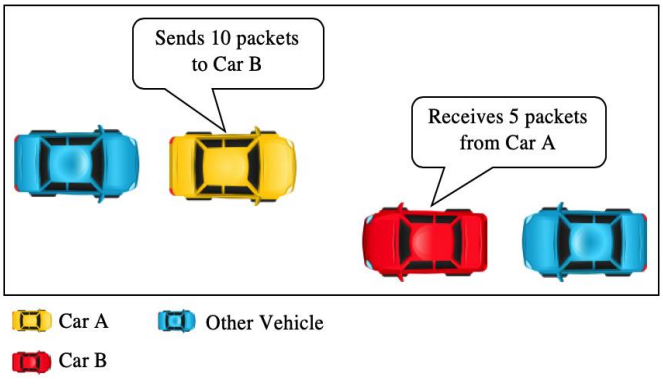

Fig. 5. Car a Sends 10 Packets to Car B but Car B Only Receives 5 Packets.

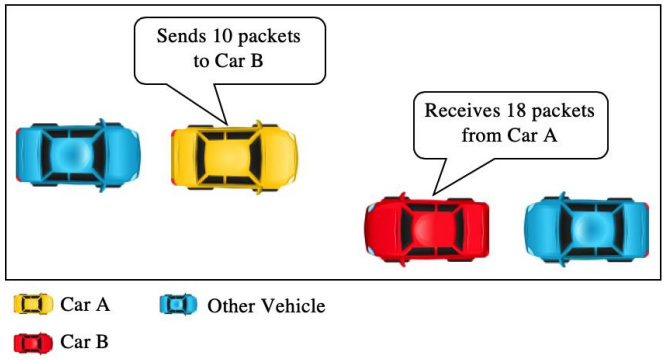

Fig. 6. Car a Sends 10 Packets to Car B but Car B Receives Additional Packets.

Figure 6 depicts another scenario when there is additional packet transmitted during the exchange of information between vehicles the delivery ratio seem to be more than one, clearly indicating that there is a malicious packet inserted by an attacker and the network is compromised.

The graph in Figure 7 indicates where Car A, C, D, F and H sends the specific number of packets to B, D, E, G and I respectively, the receiver will receive the same amount of packet delivered by the sender.

In Figure 7, the graph shows the percentage of packet delivery ratio against the number of nodes during no attack. The proposed solution used RSSI localization where it compares the ratio of RSSI during time, t_1 and t_2 to receive the packet. If

$$Ri - Rj = 0 \quad (5)$$

then there is an attack at the area and the location of the fake attack is at the same place. When the proposed solution is used, it will compare the ratio of RSSI at time, t_1 and t_2 to receive the packet. If

$$Ri - Rj > 0 \quad (6)$$

Then there is no attack and the network is secure for communication with other nodes.

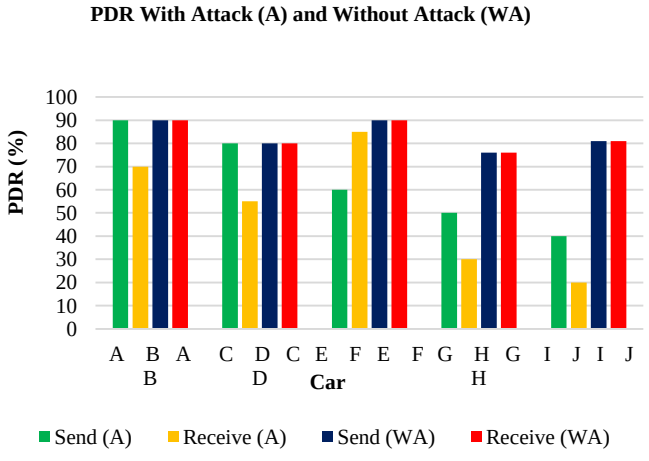

Fig. 7. PDR of Proposed Solution with RSSI Localization During Attack.

Based on Figure 8, the graph shows the percentage of packet overheads against the number of nodes with and without RSSI localization during and attack. It is essential to understand how the increasing number of nodes and speed can affect the packet delivery ratio. The conceptual result that is expected to have a slight difference in the packet overhead in an unsecured VANET network is compared to the one with the implementation of the RSSI. As the number of nodes increase, the gap between the secured and unsecured network increases and we would be able to see a much significant difference in the packet overhead. This increase in the packet overhead could possibly due to the understanding that the attack has widespread among the nodes in a much-congested environment, causing the packet overhead to increase. However, with the implementation of the RSSI localization in the network, the packet overhead seems to be much steadier and kept at a manageable level even at greater traffic congestion. Therefore, we can conclude that there is a significant difference of packet overhead with and without the implementation of RSSI Localization during an attack in the VANET network.

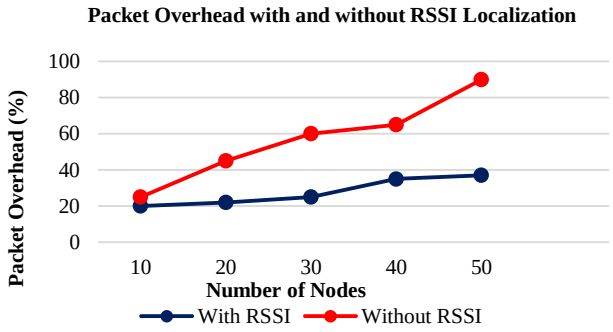

Fig. 8. Packet Overhead with and without RSSI Localization.

VII. Conclusion

In conclusion, a conceptual framework is proposed for autonomous VANET system to overcome denial of service (DoS), pollution and impersonation using signal strength and digital certificate. When vehicle sending the signal to other vehicle for the location request, signal strength will authenticate by checking each signal in order to detect any sign of attacks before proceeding by enabling sharing locations. With the road side unit, user's information security can be enhanced. The efficiency of the proposed solution is conceptually measured using Packet Delivery Ratio and Packet Overhead. With these conceptual measurements, the security of the vehicle and user information is expected to be more secure. The proposed solution is hoped to encounter the various attacks presented above effectively. Lastly, road side unit provides more secure and reliable communication from one vehicle to another vehicle. With road side unit and public key infrastructure, security of the message will increase significantly. For future work, this proposed solution will be implemented and simulated for its performance in terms of packet delivery ratio and packet overhead. In addition to that, the performance of the proposed solution will also be evaluated against other current existing solutions to determine its efficiency.

ACKNOWLEDGMENT

This research is the outcome of collaborative research between University Malaysia Sarawak (UNIMAS) and Cihan University, Sulaimaniya Campus and is fully funded by Research and Innovation Management Centre (RIMC-UNIMAS) and Research Management Center, Cihan University, Sulaimaniya Campus.

REFERENCES

[1] A. Abbasi and A. S. Khan, "A Review of Vehicle To Vehicle Communication Protocols for VANETs In The Urban Environment", Future Internet, 10(2), art. no. 14.

[2] A. Mehmood, A. Khanan, A. H. H. M. Mohamed, S. Mahfooz, H. Song, and S. Abdullah, "ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET," IEEE Access, vol.6, pp. 4452-4461, 2017.

[3] Y. R. B. Al-Mayouf, M. Ismail, N. F. Abdullah, S. M. Al-Qaraawi, and O. A. Mahdi, "Survey on VANET technologies and simulation models," ARPN Journal of Engineering and Applied Sciences, vol. 11, no. 15, pp. 9414-9427, 2016.

[4] A. Idris, M. Ismail, M.H Hamdan, M. R. Baharon, N. L. Abdullah, M. H. A. Hamid, A. S. H. Basari, "A Comparative Study between Bluetooth and GPS Tracking System," Journal of Advanced Research in Dynamical & Control Systems, vol. 10, no. 02-Special Issue, pp. 1327-1335, 2018.

[5] Y. R. B. Al-Mayouf, N. F. Abdullah, O. A. Mahdi, S. Khan, M. Ismail, M. Guizani, S. H. Ahmed, "Real-Time Intersection-Based Segment Aware Routing Algorithm for Urban Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2125–2141, 2018.

[6] Y. R. B. Al-Mayouf, O. A. Mahdi, N. A. Taha, N. F. Abdullah, S. Khan, and M. Alam, "Accident Management System Based on Vehicular Network for an Intelligent Transportation System in Urban Environments," Journal of Advanced Transportation, vol. 2018, Article ID 6168981, 11 pages, 2018.

[7] S. V. Mahagaonkar and N. Dongre, "TEAC: Timed efficient asymmetric cryptography for enhancing security in VANET," in 2017 International Conference on Nascent Technologies in Engineering (ICNTE), New Mumbai, India, 2017.

[8] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," IEEE Network, vol. 31, no. 5, pp. 50-58, 2017.

[9] Z. A. Biron, S. Dey and P. Pisu, "Resilient Control Strategy under Denial of Service in Connected Vehicles," American Control Conference (ACC), 2017.

[10] H.J. Jo, I.S.Kim, and D.H. Lee, "ReliableCooperativeAuthentication for Vehicular Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 4, pp. 1065–1079, 2017.

[11] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin and C. Hu, "Distributed Aggregate Privacy-Preserving Authentication in VANETs," IEEE Trans- actions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516– 526, 2017.

[12] K. M. A. Alheeti, R. Al-Zaidi, J. Woods and K. McDonald-Maier, " An intrusion detection scheme for driverless vehicles based gyroscope sensor profiling," in 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2017.

[13] M. T. Garip, P. H. Kim, P. Reiher and M. Gerla, "INTERLOC: An interference-aware RSSI-based localization and sybil attack detection mechanism for vehicular ad hoc networks," in 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2017.

[14] M. Azees, P. Vijayakumar and L. J. Deboarh, " EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," IEEE Transactions on Intelligent Trans-portation Systems, vol. 18, no. 9, pp. 2467–2476, 2017.

[15] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 12, pp. 10626–10636, 2017.

[16] Irshad Abbasi, A. S. Khan, Shahzad Ali, "A Reliable Path Selection Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks", Eurasip Journal On Wireless Communication and Networking, 2018(1), 236.

[17] A. S. Khan, H. Halikul, M.N.Jambli, R. Thangaveloo, Mitigation of Non-Transparent Rouge Relay Stations in Mobile Multi hop Relay Networks, Advanced Science Letters, 2017 , 23 (6), pp. 5246-5250,

[18] Y. Park, C. Sur, S. W. Noh, and K. H. Rhee, "Secure vehicle location-sharing for trajectory-based message delivery on VANETs," in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, UK, 2017.

[19] A. H. A. Halim, M. Elshaikh, M. N. M. Warip, and R. B. Ahmad, "Validation of performance analysis for optimized vehicular ad hoc network using Taguchi method," Jurnal Teknologi, vol. 77, no. 32, pp. 133–140, 2015.

[20] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang, "Privacy-Preserving Location Based Services For Mobile Users In Wireless Networks", Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2004.

[21] A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, "The case for dynamic key distribution for PKI-based VANETs," International Journal of Computer Networks & Communications (IJCNC), vol. 6, no. 1, pp. 61–78, 2014.

[22] Irshad Abbasi, A. S. Khan, Shahzad Ali, "A Reliable Path Selection Packet Forwarding Routing Protocol for Vehicular Ad hoc Networks", Eurasip Journal On Wireless Communication and Networking, 2018(1), 236.

[23] Irshad Abbasi, A. S. Khan, Shahzad Ali, "Dynamic Multiple Junction Selection based Routing Protocol for VANETs in City Environment", Applied Sciences, 8(5), 687.