QoS Provisioning Using Secure VANET Application for Different Network Environments

B. Usha Rani[1*], Suraiya Tarannum[2]
[1]Research Scholar, VTU RRC, Bengaluru, Karnataka, India. Email: usharanib2016@gmail.com
[2]Professor, Dept. of ECE, HKBK College of Engineering, Bengaluru, Karnataka, India.
Email: ssuraiya@gmail.com
*Corresponding Author

Abstract: Vehicular Ad-hoc Network (VANET) is an infrastructure less network. It provides enhancement in safety related techniques and comfort while driving. It enables vehicles to share information regarding safety and traffic analysis. Security of these messages is essential in VANET application due to message creation which harms the system. This makes it more difficult in traffic scenario, which can play havoc with human lives. Hence, the authors approach is to design a fraudulent secure VANET in Vehicle-to-Vehicle (V2V) communication. A Control Body (CB) is trusted by everyone, which can generate Public and Private Key for each vehicle. Authentication of the requested vehicle and message integrity is also checked in this approach. Simulation results are analyzed based on Network Throughput, Collision and Successful Packet Transmission. Our proposed algorithm is compared with NCCMA and found to perform better under most Network Environments.

Keywords: DSRC, IEEE 802.11p, RAISE, VANET, V2V.

I. Introduction

In recent times, demand and growth rate of wireless technology is very high. Now-a-days, people have another choice of wireless network, namely the Vehicular Ad Hoc Network (VANET), which is popular for its application as safety application as well as entertainment applications. Purpose of VANET development is to provide safe and reliable environment for the drivers and passengers. For the communication environment in V2V, each vehicle has an On Board Unit (OBU), which is a device driver of vehicles to easily communicate with each other and share their information. Information can be of many types, such as general information or some security related information. Generally OBU broadcast the general information (Time, Direction, Position, and Traffic events) periodically to the nearby RSU (Road Side Unite) or vehicle [1]. Periodically broadcasting of the safety related information and traffic information is standardized by the Dedicated Short Range Communication (DSRC) as beacon [2]. Beacon contains the detail information about the speed of vehicle, direction, location and other safety related information. Through these data, drivers are able to form a contextual view of the traffic conditions and situations like accidents or congested routes, hence can be avoided.

Security of these data is required because they reveal the location of the passengers and drivers. Message exchange in VANET can cause problem for the travelers, some fraud message can creates the bad environment for the users [3]. Let us suppose, some wrong information about traffic creates unamenable situation for the traffic control system, which plays with the patients in ambulance by giving wrong traffic information. Always a risk lives is attached with the attacker false information; it can also cause a death of person. A genuine user or vehicle must be authenticated before transmitting their data in the network. Providing security in the VANET system avoids traffic congestion, collision and safe driving with entertainment. V2V communication in VANET network architecture is shown in Fig. 1. Each vehicle has an OBU (On Board Unit), by which the vehicles can communicate with each, once they are in the range of communication. Each vehicle is also connected through the server/control body for the communication update. CB is trusted by the users and make V2V system secure.

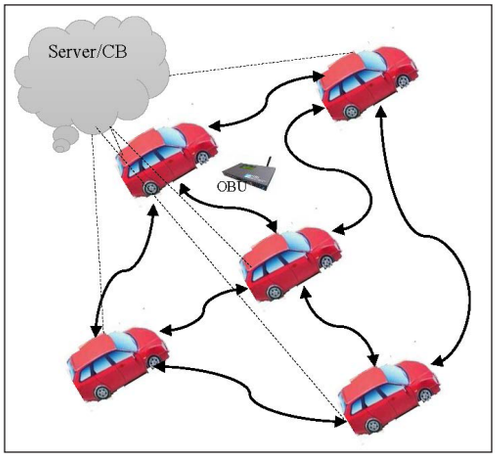

Fig. 1: VANET V2V Network Architecture

There are certain parameters which must be considered at the time of VANET system design.

- *Authentication:* User authentication is required for the VANET application; it is assured that the generated message is generated by the genuine user.
- *Reliability:* The data received data by the user must be checked to ensure that it is altered genuine and factual.
- *Integrity:* The Received message must not be alter by the third party, so message authentication is also required. Alteration of message can harm the system.
- *Anonymity:* Privacy of user must be preserved.
- *Availability:* Data must be easily available for the authenticated user.
- *Delay Handling:* It must be ensured that minimum delay is required for time sensitive or safety related information.
- *Confidentiality:* Private data must not be accessible by the Third Party unauthorized user.

Modern research lays emphasis on related work in terms of Security. In the Symmetric Key Scheme, between the vehicle and RSU a Key is generated called as Shared Symmetric Key (SSK), then the RSU sends the authentication message to the sender for verification of message. Authentication scheme is proposed in the RSU-algorithm. The Symmetric Key Authentication scheme is RAISE. For the authentication of message RSUs assist the vehicles in RAISE (). Vehicles generate a code that is attached with the message, called Hash-Message Authentication Code (HMAC) in the RSU range. Authentication message is added to each vehicle by the RSU. Verification of the authenticated message happens fast when the short HMAC is attached to the message. Due to this, less Computations and Communications happen. The performance of this technique is better than other techniques that depend on attaching certificates to the message. This technique is not scalable. The communications cannot take place if the two vehicles are in the range of the same RSU.

In this paper, a Five Layer Hierarchical security system from top to bottom is proposed which is an improvement, law, norm, management and technology. In VANETs, to determine the attached nodes, Corroborate Intrusion Detection system is proposed.

In the real mode, the message is grouped for its safety [8] and the V2V message is distributed with light weight solution, decentralized via the efficient group leader. In this approach, the information and identity of vehicle is not secured. The work proposed in [9] concentrates on secure vehicle communication in VANET and provides a framework for the security. This framework is a combination of RAS and AES to from the hybrid cryptography. So, this frame work is used for secure communication in vehicles. For RSA and AES, hybrid approaches required high computations.

Another security model, considers three type of network environment, as City, where Speed of vehicles is moderate and sometime low due to high traffic density and transmission can also get disturbed through physical condition like tall buildings which are very dense. The second is Express way where vehicle speed is very high and traffic is also very less. The third is village environment has less number of vehicles and traffic is also less [14].

The rest of the paper is organized as follows: Section Two is about our proposed Secure V2V Communication approach, based on Public and Private Key. In Section Three we discuss about the simulation results and analyze our system performance. This is followed by a section in conclusion.

II. Proposed System Model

A. System Model

For security based VANET application shown in Fig. 2, the system model has a Control Body (CB) is maintained, that is trusted by everyone. Each vehicle has an On Board Unit (OBU) installed in the vehicle. CB communicates with the vehicle through a secure channel in the network known as Transport Layer Security (TLS) protocol. Communications among the vehicle in the network follow Dedicate Short Range Communication protocol (DSRC). CB issues a pair of Private and Public Key for each vehicle. At the time of message broadcasting, vehicle signs the message with its own Private Key for Integrity and the Receiving vehicle checks the integrity with the sender's Public Key.

In a secure architecture of the VANET, identity of sender and his location cannot be accessible by any common person or who only has accessing authority of publicly known parameters. But existing approaches do not have such a scheme and make a hole in secure system. Fake identity of the vehicle must be stopped and also malicious nature of a vehicle which can broadcast a message on behalf of other genuine vehicle. For this we are model a secure and identified system for VANET application. In the first phase, a Control Body (CB) generates all the system related parameters for the vehicle at the time of system configuration phase. It also generates the identity for each vehicle in the Identity Generation Phase. In the final phase, Message Authentication is checked by the receiver vehicle.

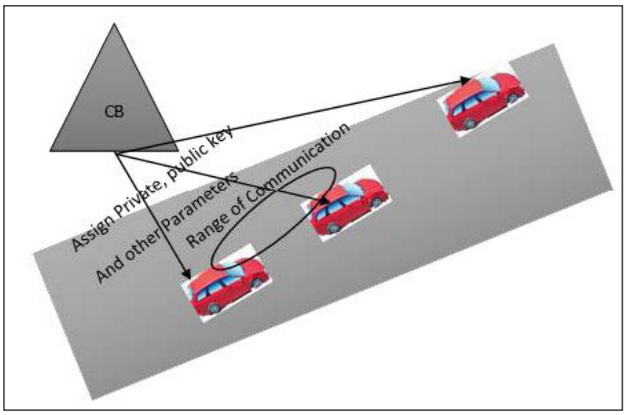

Fig. 2: VANET Secure Architecture

B. Phase

Assignment of the system parameters starts and finishes in this phase by the CB. Some of the parameters known publically are presented in Table I.

TABLE I: PARAMETERS AVAILABLE PUBLICALLY

Notation	Definition
CB	Control body
B	additive group
B_G	multiplicative group
(bm)	bilinear Map
$t \in Y_p$ i	A random number
K_{pub}	Public key.
H(·) and h(·)	SHA-224 or SHA-256 [9]

1. Two Sub Groups are created by the CB namely, B and B_G of order p. Where B represent the Additive Group and B_G represents the Multiplicative Group of same Prime order P. Bilinear Map (bm) [5] of this can be represented as,
$$(\text{bm}) = B \times B_G.$$
Let M and N be two generators in the group B.
2. A Random Number $t \in Y_p$ is selected by the CB and generate $M_{pub} = t\text{M}$ and x as a Private Key and M_{pub} as a Public Key.
3. CB selects the two, as function H(·) and h(·).
4. When a vehicle registers for the first time CB assign an identity ID to the vehicle as $ID \in B$ with a Secure Password (SP). These values are added inside the OBU as ID, SP, t.
5. Rest of the other public details are available for the all other vehicles, these parameters are $\{B, B_G, p$, bm, M and N, H(·) and h(·)$\}$.

C. Phase 2

In this phase, anonymous identity is generated by the vehicle V_a for passing the authentication request by the other vehicles.

1. Vehicle input their ID and SK into the OBU security system and pass the Security Verification. If ID and SP combination are not matched or any one of them is incorrect, it refuses and stops the authentication and further communications. If these ID and SP combinations are correct, it starts further module of communications. An adversary not knowing the secure password, will be stopped which increases the security of the system.
2. A Random Number is chosen at the time of secure Identity Generation Phase, which selects a random value $q_a \in Y_p$ and generates a Secure Identity as SID_a. There are two parts of the SID_a as $SID_{a,1}$ and $SID_{a,2}$. To reduce the delay, this generation can be done offline. Whereas,
$SID_{a,1} = q_a\,\text{M}$ and
$SID_{a,2} = ID \oplus \text{H}(q_a\,M_{pub})$
3. Message msg_a generated by V_a and input in device for the transmission. Device selects as random pair of SID_a, q_a and a current time T_a. Further for message signing steps, it calculates the signature sig_a of msg_a.
$sig_a = (q_a + t\,\text{ln})\,(msg_a \,||\, SID_a \,||\, T_a)\text{N})$.
4. Once this process is complete, the device generates the secure message $\{SID_a, msg_a, sig_a, T_a\}$ and V_a transmits it to its neighboring vehicle which is in the range of communications.

D. Phase 3

In this phase, the verification of message is done by the neighboring vehicle, once it receives the message. Vehicles verify the message signature to alleviate the false message possibility. Verification of message is sent by V_a.

In above phase 2, the step 4 shows final deliver message as, $\{SID_a, msg_a, sig_a, T_a\}$ by the vehicle V_a to the neighbor vehicle V_n. For authentication of message, V_n uses the publically assign parameters by the CB and performs the operation given below:

1. Time based verification is started by V_n for checking the originality of the message. Let us suppose that the message receiving time of V_n is T_n. The Vehicle computes the time as $\Delta T \geq T_n - T_a$. If $\Delta T \geq T_n - T_a$ is true, then V_n continues the communication process, otherwise it discards the final message.
2. V_n can also authenticate the signature, whether
$$\text{bm}(sig_a, \text{M}) = \text{bm}(SID_{a,1} + \text{h}(msg_a \,||\, SID_a \,||\, T_a)\,M_{pub}\text{N})$$

If this holds, V_n accept the message and start communication with V_a. Through this approach, we design a safe and secure communication environment for the VANET.

III. RESULTS AND ANALYSIS

To evaluate the performance of a secure VANET application, windows 10 operating system with Dot Net framework 4.0 and C# 6.0 programming language for development of VANET environment was used. We considered a secure network environment and used the standardized DSRC/WAVE protocol for transmission in VANET. Further a secure approach was implemented as proposed in [13] as one Control Channel and CEV-AMAC and named as S-AMAC. In [13] author designed an adaptive medium access scheduler (AMAC) for V2V communication and it is dedicated to the short range communication. In [13] the author have simulated their work for network collision, throughput and packet transmission in different network environments. QAM-64 was employed for modulation and a 27 Mbps transfer rate and coding rate of 0.75. There are three models considered for analysis as City (C), Expressway (E) and Village (V) [14]. The obtained result for the SAMAC is analysed and compared with the SNCCMA.

A. Average Throughput Performance Analysis:

Average Throughput achieved for City, Expressway and Village environment considering 20, 40 and 80 user as presented in Fig. 3 is 19.87 Mbps for S-AMAC and 18.35 Mbps for NCCMA. In case of Expressway environment, the achieved Average Throughput is 18.77 Mbps for S-AMAC and 16.74 Mbps for NCCMA. In case of Village environment, the achieved Average Throughput is 16.09 Mbps for S-AMAC and 14.87 Mbps for NCCMA.

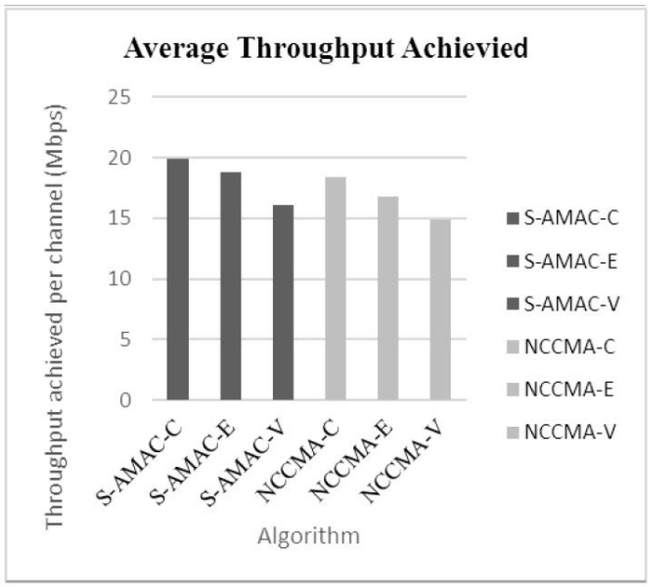

Fig. 3: Achieved Average Throughput in Secure V2V VANET Environment

B. Average Successful Packet Transmission Analysis:

Average Successful Transmission for City, Expressway and Village environment in considering 20, 40 and 80 user is presented in Fig. 4. The Average Successful Packet Transmission is 147.33 packets for S-AMAC and 144.77 packets for NCCMA. In case of Expressway environment, the achieved Average Successful Packet Transmission is 139 packets for S-AMAC and 127 packets for NCCMA. In case of Village Environment, the achieved Average Successful Transmission is 113 packets for S-AMAC and 108 packets for NCCMA.

C. Average Packet Collision Performance Analysis:

As security parameters are added the size of the data packet is increased due to Signature, Identity and Time Stamp. The Time Slots remain the same, which increases the collisions in the network to a little extent for our proposed secure SAMAC and to a more extent for SNCCMA. Average collision packets for City, Expressway and Village environment by considering 20, 40 and 80 user is presented in Fig. 5. The average numbers of collision packets are 232 for S-AMAC and 238 packets for NCCMA. In case of Expressway environment scenario, the average collision packets are 246 packets for S-AMAC and 259 packets for NCCMA. In case of Village environment, Average Collision Packets are 265 packets for S-AMAC and 273 packets for NCCMA.

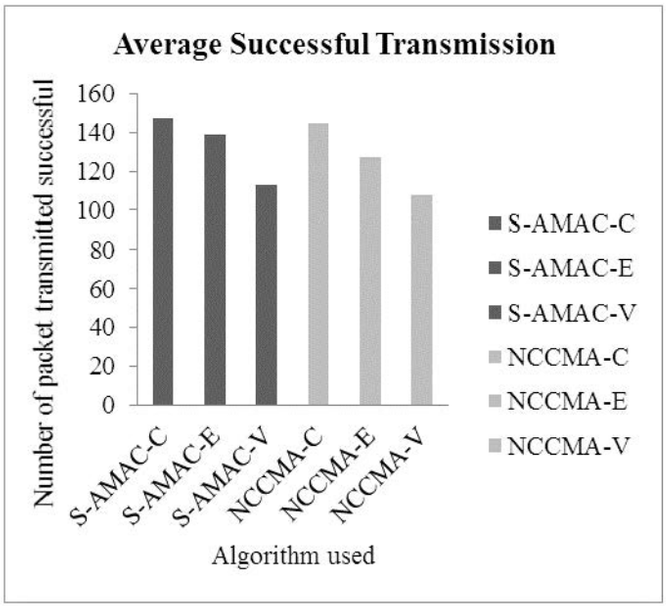

Fig. 4: Average Successful Packet Transmission in Secure V2V Communication for Various Algorithms

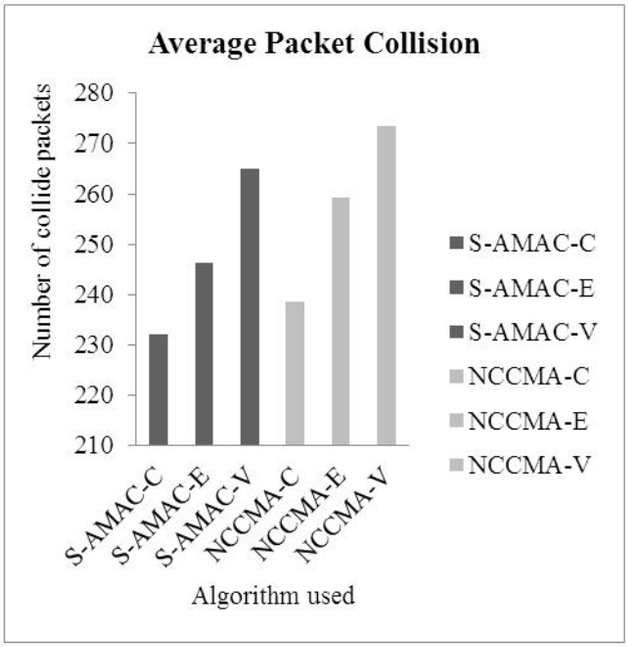

Fig. 5: Average Packet Collision Comparisons between SAMAC and NCCMA for Varied Environments

IV. Conclusion

In this work, we propose a secure VANET application for V2V communication. Security is needed for the VANET application.

To reduce the possibility of alter of the message by Third Party; we propose to verify the Authentication of user as well as to check the Integrity of message. Time Stamp based message originality verification is done. Result is analyzed based on Average Throughput achieved for different network environments as City, Expressway and Village. Through simulation, we analyze that the proposed scheme of S-AMAC performed better than the existing NCCMA approach. Communication with security parameter increased the number of Packet Transmissions while still performs better than the existing approach. The number of successful transmission is more for S-AMAC than the NCCMA. Collisions are also reduced in S-AMAC than NCCMA. We conclude that the overall system performance is good and applicable for secure VANET communications.

References

[1] T. Leinmüller, C. Maihöfer, E. Schoch, and F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification," In *Proceedings of the 3rd International Workshop on Vehicular Ad-hoc Networks (VANET'06),* pp. 57-66, 2006.

[2] DSRC Technology, Intelligent Transportation Systems, [Online]. Available: http://www.its.dot.gov/dsrc/

[3] D. Dolev, and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198-208, 1983.

[4] C. C. Lee, and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441-1449, 2013.

[5] A. Menezes, "An introduction to pairing-based cryptography," Mathematics Subject Classification, Primary 94A60, 1991.

[6] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks," In *IEEE International Conference on Communications, 2008, ICC'08*, Beijing, China, pp. 1451-1457, 19-23 May 2008.

[7] H.-T. Wu, and W.-S. Hsieh, "Rsu-based message authentication for vehicular ad-hoc networks," *Multimedia Tools & Applications*, vol. 66, no. 2, pp. 215-227, 2013.

[8] H. Jin, and P. Papadimitratos, "Scaling VANET security through cooperative message verification," In *2015 IEEE Vehicular Networking Conference (VNC)*, 16-18 Dec. 2015.

[9] National Institute of Standards and Technology (NIST), Secure Hash Standard, FIPS PUB 180-2, 2002.

[10] Q. Liu, Q. Wu, and L. Yong, "A hierarchical security architecture of VANET," In *International Conference on Cyberspace Technology (CCT 2013)*, 23-23 Nov. 2013.

[11] R. Coussement, B. A. Bensaber, and Ismail Biskri, "Decision support protocol for intrusion detection in VANETs," In *Proceedings of the 3rd ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, ACM, 03-08 Nov. 2013.

[12] A. A. Wagan, and L. T. Jung, "Security framework for low latency VANET applications," In *2014 International Conference on Computer and Information Sciences (ICCOINS)*, IEEE, 03-05 Jun. 2014.

[13] B. U. Rani, and S. Tarannum, "AMAC scheduling: To optimize QOS for DSRC," In *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT),* Bangalore, pp. 1543-1549, 20-21 May 2016.

[14] B. U. Rani, and S. Tarannum, "A mobility aware environmental channel modelling for DSRC based STS for V2V," *International Journal of Enhanced Research in Science, Technology and Engineering*, vol. 5, Issue 4, pp. 73-82, Apr. 2016.