MAvanet: Message Authentication in VANET using Social Networks

Anirudh Paranjothi
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville, USA

Mohammad.S.Khan
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville, USA

Mais Nijim
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville, USA

Rajab Challoo
Department of Electrical Engineering and Computer Science
Texas A&M University-Kingsville, USA

***Abstract*— Vehicular ad-hoc networks (VANETs) have gained a lot of attention from both academic and industry due to its immense potential in revolutionizing the vehicular communication industry. VANETs facilitate vehicles to share safety and non-safety information through messages. Safety information includes road accidents, natural hazards, road blocks etc. Non-safety information includes tolling information, traveler information etc. The main goal behind sharing this information is to reduce road accidents by alerting the driver about the unexpected hazards. In our algorithm social networks are used to create an active topology from all possible users in sender's profile, who are active at a particular point of time. Message authentication achieved by providing profile of user and Quick Response Code (QR code) technique. The novelty in our approach lies in the fact that, we assume no hand held device is used. This proposed architecture is used from the car dashboard. Simulation results are presented and compared with P2P systems.**

Keywords- VANET, Social networks, QR code, Authentication

I. INTRODUCTION

VANET was evolved from the concept of MANET with distinguished characteristics like high mobility, highly changing topology [1]. VANET is popular among automobile industries and government agencies that are responsible for public safety and transportation. It allows developers to build applications, simulation tools, and protocol. The report given by the National Highway Traffic Safety Administration (NHTSA) concluded that distracted driving is one of the main reasons for road accidents, of which 38% of distracted drivers were using cell phones [2]. Other reasons for road accidents are bad road condition, poor driving, poor vehicle design, etc. Serious accidents will cause financial loss, physical disability, and even death. Report given by Federal Highway Administration (FHWA) in 2013 specified that number of people injured in vehicular accidents in the period of 2012 to 2013 were 33908, which is less when compared with previous years. The administration also reported that accidents were rapidly decreasing due to the development of VANET communication and Intelligent Transport System (ITS) [3]. Main aim of creating high performance, highly scalable and securable VANET is to reduce road accidents, vehicle damage and to ensure road safety. To build a safety system the following properties of VANET needs to be considered: [4].

i) Nature of Communication: In vehicular communication, the users are represented as nodes where nodes should establish a connection with other nodes to share the information.

ii) Mobility: VANET is mobile in nature where all nodes except Road Side Unit (RSU) are changing their positions with different speed and directions.

iii) Continual Sharing information: Since VANET is mobile in nature; nodes will continuously share their information with other nodes.

iv) Low Volatility: VANET is low volatile in nature because nodes participating in communications are available only for short period of time.

Communication between vehicles is the key component in VANET. It uses wireless ICT (Information Communication Technologies) for vehicular communication. Vehicular communication allows vehicles to share information like traffic jams, accident information, safety information, entertainment, etc [5]. Two types of communication are possible in VANET: 1) Vehicle to Vehicle (V2V) (Short range) 2) Vehicle to Road Side Units (RSU) (Long range). Road Side Units (RSU) will be located at the critical points of the road. In this type, the vehicles will take help of RSUs to communicate with other vehicles. This type of communication is called as Vehicle to Infrastructure (V2I) communication.

Security becomes major issue while sharing such information in VANET. There is a high possibility of security attack during vehicular communication. Some of the attacks are 1) Bogus information attack 2) Unauthorized preemption attack 3) Message Replay attack 4) Message modification attack 5) Impersonation attack 6) Denial of Service (DOS) attack, etc [6]. To protect VANET from security attacks security mechanisms needs to be incorporated with it. The security mechanisms should meet the following requirement: 1) Authentication, 2) Integrity, 3) Non repudiation, 4) Access control, 5) Privacy.

Social networks are becoming popular and its users are increasing rapidly. Recent survey conducted by the pew research center states that facebook remains the most popular social media site and overall 71% of internet users are on facebook [7].

QR codes were developed in the year 1994 by the automobile industry in Japan to track the manufacturing vehicles. QR

978-1-5090-1496-5/16/$31.00 © 2016 IEEE

codes are now popularly used among developers to provide a secure login to the user. It consists of black modules arranged on a white background. QR codes can be read by devices like smart phones, camera, scanner etc. and processed using QR encryption and decryption algorithms.

In our approach, we concentrated on delivery of non-critical messages. The main motive of our approach is to provide vehicular communication through dashboard without using cellphone. This enables the users to participate in communication without taking hands off the steering wheel.

MAvanet authenticates sender and recipient using social networks. On a successful authentication, primary connection will be established between the sender and recipient and they can take part in communication. During communication, messages will be encrypted in the form of QR code at sender side and it will be decrypted at the receiver end. We used ns-2 simulator to measure our system performance and to compare the results with other systems. Our proposed system (MAvanet) supports only V2I communication.

The rest of the paper is organized as follows: section II, discusses about background and related works on VANET security issues and QR codes. Section III, discusses about general architecture of VANET and explains about RSU, OBU and AU. Section IV, focused on proposed architecture. In section V we proposed an algorithm (MAvanet) for message passing, QR encryption, and QR decryption. We present simulation results carried out in section VI. Finally, we present the conclusion and future work in section VII.

II. Related work and Background

Sanoop *et al.* [3] used the concept of Transient Certificate (TC) and Multi-Hashed Binary Tree (MuBT) to minimize security issues in VANET. The authors have also used public cloud to reduce storage space requirements in vehicles and RSU. N.Varshney *et al.* [4] have proposed a protocol that discussed about VANET security by providing digital certificates. X. Lin *et al.* [8] have proposed an authentication theory with privacy support. The authors used certificates. Certificate has single public key and it can be used for long period. But they have not considered about location, privacy issues. Roberta *et al.* [9], has discussed about the issue of providing routing solutions to applications in VANET. The authors also focused on directional broadcast forwarding based on Forwarding Decision Algorithm (FDA) and Topology Discovery Algorithm (TDA). W. Puech *et al.* [10], has focused on module recognition of QR codes. The authors illustrated new Weighted Mean Square Error (WMSE) method to increase the significance in central pixel and decrease significance in border pixels. A. Nath *et al.* [11], has focused on confidential encrypted data hiding using QR code and illustrates the steps involved in generating QR code. The authors also discussed about encryption, decryption process associated with QR code but they have not discussed about issues, challenges involved in QR code.

R. Hussain *et al.* [12], pseudonymous authentication protocol to improve the security and privacy in VANET. However, this protocol establishes a communication link based on honest from certification authorities. S. Biswas *et al.* [13] used identity based signature scheme to implement message authentication in VANET and also they combined their approach with ECDSA to incorporate the features of proxy signatures. Q. Kang *et al.* [14] integrates pseudonym with identity based signature to provide message authentication in VANET. The authors have also used batch verification to increase the efficiency of message dissemination. X. Liu *et al.* [15] has proposed cipher text based encryption scheme for message authentication. The authors have also discussed about hierarchical based access control to provide scalability during message transmission. They have not discussed about efficiency with it. K. Lim *et al.* [16] have discussed about fast dissemination of messages in VANET using RSU's with high computation power. They also ensure anonymity and message trace mechanism to their senders.

To the best of our knowledge no one has implemented QR code technique and social networks together for message authentication in VANET. We proposed an algorithm MAvanet which provides message authentication in VANET and thereby build high performance, securable networks suitable for vehicular communication.

III. General Vanet Architecture

Vehicular communication i.e., V2V communication and V2I communication are accomplished using wireless medium called Wireless Access in Vehicular Environments (WAVE). The popularity of VANET helps developer to build applications to enhance road safety and reduce accidents. VANET consists of three main components 1) Application Unit (AU), 2) On Board Unit (OBU), 3) Road Side Unit (RSU) represented in Figure 1 [5]. In VANET Road Side Unit (RSU) is called as provider since it hosts an application and On Board Unit (OBU) is called as user since it uses the service provided by RSU. It has sensors which are used to collect and send information. Application Unit (AU) is used to access the application provided by RSU.

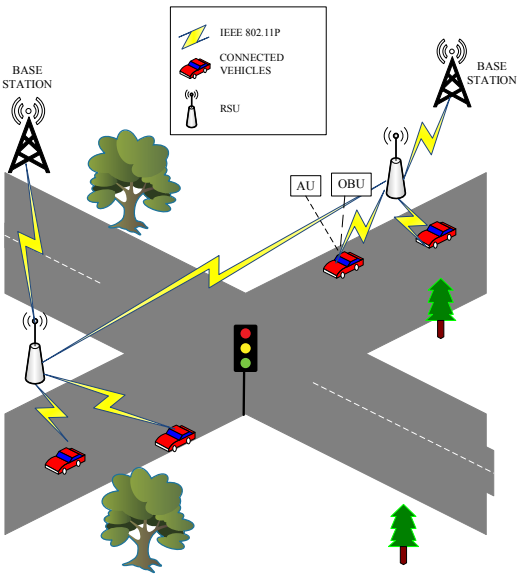

Figure 1: General architecture of VANET

A. Road Side Unit (RSU)

RSU will be located on the road side. It contains one dedicated network device used for short range communication and other network devices in RSU are used for communication within the network [5] shown in Figure 1. The main functions of RSU are:

1) Usually, ad-hoc network will have shorter communication range but RSU helps in improving communication range by sending the information to other RSU or redistributing information in OBU [5].

2) RSU will be used to provide internet connectivity to OBU.

B. On Board Unit (OBU)

OBU will be located in a vehicle. It is used to transfer the information from OBU to OBU or OBU to RSU. OBU has specialized user interface to connect one OBU with another. OBU also contains a memory to perform read and write operation. IEEE 802.11p (radio frequency channel) is responsible for connecting one OBU with another OBU or RSU as shown in Figure 1. The main functions of OBU are data security, IP mobility, wireless radio access, network congestion control, ad hoc and geographical routing, etc. [5]

C. Application Unit (AU)

AU obtains communication services from OBU. Generally, AU will be a device connected to OBU using wired or wireless link. AU in VANET uses the application provided by the provider using communication services given by OBU [5] as shown in Figure 1.

IV. Proposed Architecture

In our approach, we defined connectivity between vehicles based on social network connectivity. Assume, vehicle V1 (Sender) wants to send a message to vehicle V2 (Recipient). First, connection will be established between V1 and V2 using social networks. This ensures secure message delivery from sender to intended recipient. Through Figure 2, it can be observed that only the intended recipient (V2) can read the message.

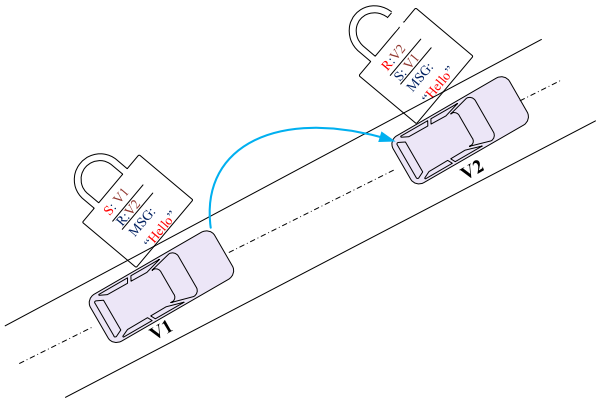

Figure 2: Communication and Authentication between vehicles

The proposed architecture is represented in Figure 3. In our approach, we assumed that users who are involved in vehicular communications are directly connected to each other using social networks at a particular time. Communication between users is carried out through dash board without using cell phones. Here, Vehicles are connected using social networks and communicating with other vehicles with the help of RSUs. These vehicles are termed as connected vehicles and represented as "C", other vehicles are termed as unconnected vehicles and represented as "UC". Connected vehicles are represented as nodes and the network established by them is termed as active topology. RSUs are connected to base station or Wi-max tower that authenticates sender and recipient. On sender side, user authenticates the recipient and their location. On a successful authentication, primary connection will be established between sender and recipient. Figure 3 represents the extracted topology of active users in social networks. The topology extracted using social networks specifies that how the users are connected to each other in social networks. By establishing a primary connection between the active users, we can ensure that message gets delivered to the intended recipient. Once the primary connection is established, messages will be encrypted in the form of QR Code and it will be transmitted from Sender to Recipient. On receiver side, user authenticates sender through social networks. On a successful authentication, QR code will be decrypted and the message will be displayed to the user at receiver end.

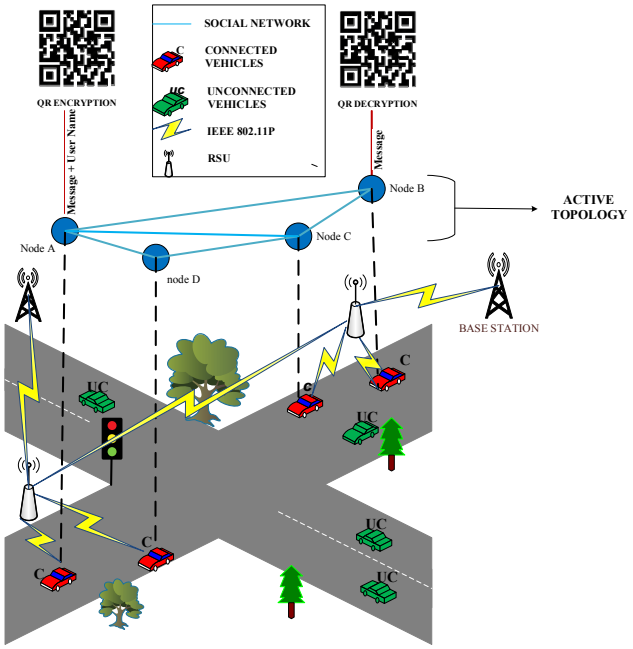

Figure 3: Secure message passing in VANET

A. Active Topology

In our approach, we implemented social networks to extract an active topology in VANET. We considered each user in a social network as a separate node and they are distinguished from each other by their identities like user id, user name, email, etc. One main advantage of using social network is, it is easy to track social interaction of the users through their social tie ups.

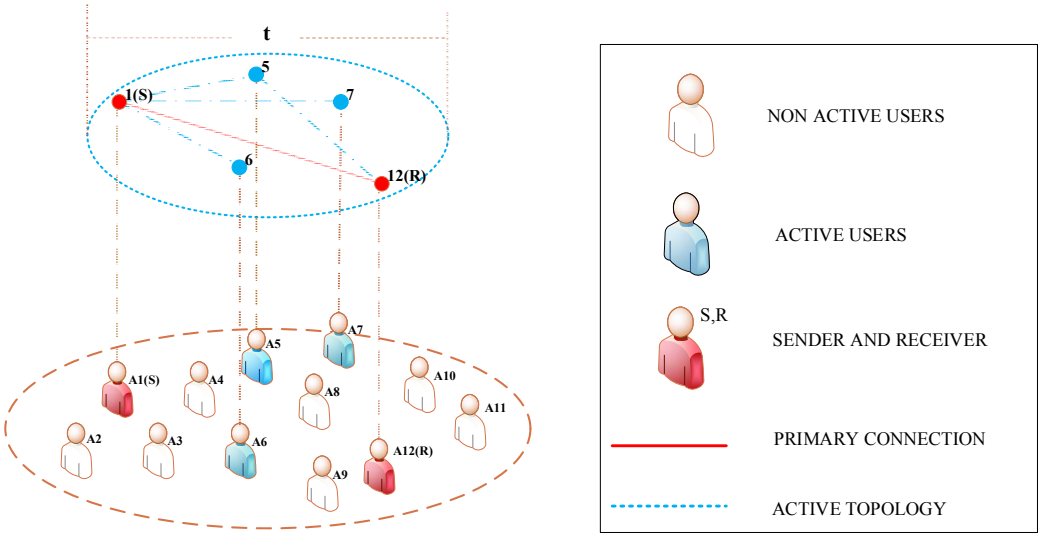

Figure 4: Extraction of active topology using social networks

Active users: The users who are active to take part in communication at a particular point of time (t) are called as active users.
Non-active users: The users who are not taking part in any communication at a particular point of time (t) are called as non-active users.
Active topology: Network established by using active users is called as active topology.

Extraction of active topology is represented in Figure 4. We considered A1, A2, A3 ,…., A12 as users who are having social networking profile and connected using social networks. For instance, A1 needs to send a message to A12 at a time period (t). First A1 needs to extract an active topology with active users. Here A1, A5, A6, A7, A12. are the active users and A2, A3, A4, A8, A9, A10 are the non-active users. Active topology is extracted with active users, which are represented as nodes. Node 1 and node 12 are the sender and receiver nodes respectively, nodes 5, 6, and 7 are active user nodes. From active topology it is clear that primary connection exists between the sender (A1) and recipient (A12). It ensures that message can be transmitted from A1 to A12.

B. QR code (Quick Response Code)

QR code is a 2D matrix barcode used to store information in the form of square dots. The main advantage of using QR code is high-speed encoding, decoding process and large storage space. Since QR code provides larger storage capacity 40 versions of QR code are available with different storage capacity. Among all smallest version of QR code is version 1 (V1) and it has 21 X 21 module size. The largest version of QR code is version 40 (V40) and it has 177 X 177 module size represented in Figure 5 [10]. Each version of QR code uses four error correction levels to store the information. The four error correction levels are 1) low level, it restores 7% of code words, 2) medium level, it restores 15% of code words, 3)-quartile level, it restores 25% of code words, 4) high level, it restores 30% of code words [10]. QR codes can be read by devices like camera, scanner etc. and it will be processed using QR encryption and decryption algorithms. QR code contains following patterns: 1) position pattern, 2) alignment pattern, 3) timing pattern, 4) format pattern, 5) version pattern.

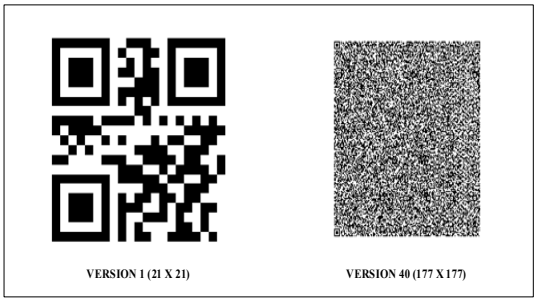

Figure 5: Different versions of QR code

C. Data Encoding

We implemented QR code technique for data encoding. In data encoding process, first sender will verify recipient's id and location. On a successful verification, the input data will be encoded using Reed – Solomon algorithm with error setting correction level. Data encoding process is represented in Figure 6. Encoding process of QR code consists of four stages: 1) numeric, 2) alpha numeric, 3) binary, 4) kanji [10]. In QR encoding technique input data will be converted to binary form. First input data will be divided into codewords. Codewords are 8 bit long and it forms blocks in which error corrections are added. Masking pattern in QR code is used to mask the codeword and it is called as codeword masking. Then, the code words will be placed in a square from bottom left corner to top right corner in a zigzag pattern [10]. Finally, function patterns like position,

alignment, timing, version and format patterns will be placed into the QR code. Once message gets encrypted, it will be transmitted from sender to intended recipient with sender's id.

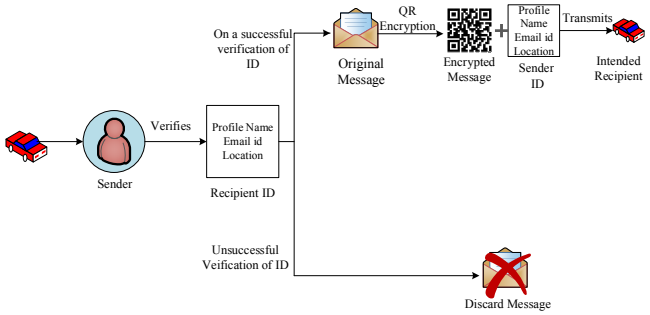

Figure 6: Data encoding process

D. Data Decoding

We implemented QR code technique for data decoding. DES (Data Encryption Standard) algorithm involves in decryption process of QR code. QR code decoding algorithm will be applied to QR code image in binary form to retrieve the input data. One major disadvantage of using QR code is that, input data encrypted using QR is not safe as anyone can access encrypted information using QR reader/decoder.

In our approach, we provided solution to this issue by authenticating the sender's id at the recipient end. On a successful verification of sender's id, the encrypted message will be decrypted using QR code decoding algorithm and original message will be displayed to the intended recipient. If the sender's does not exist in recipient friend list, the received message will be discarded. Data decoding process is represented in Figure 7.

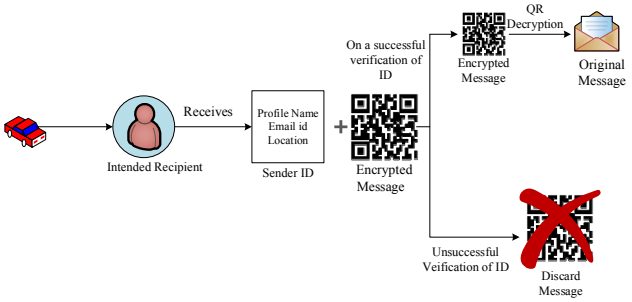

Figure 7: Data decoding process

V. MAVANET (MESSAGE AUTHENTICATION IN VANET)

The proposed algorithm MAvanet is divided into two major parts, 1) MAvanet sender side algorithm, 2) MAvanet receiver side algorithm. MAvanet sender side algorithm consists of two main sections, 1) topology extraction, 2) QR encryption. MAvanet receiver side algorithm has one major section, 1) QR decryption. The secure message delivery is based on these sections. MAvanet provides the facility of accessing the friend list of sender and receiver. *FRIEND_LIST (i)* contains the list of friends who are connected to sender and receiver through social network. MAvanet sender side algorithm takes the input of text message (msg), location (loc), and recipient name (rec_name) from the sender. MAvanet receiver side algorithm takes the input encrypted message (msg_encoding) from the sender side algorithm.

MAvanet sender side algorithm: In sender side algorithm, first section discusses about extracting a topology. Our topology is extracted based on active users. *Extract_Topology ()* is used to extract a topology based on active users. Once topology is extracted, two constraints are involved in establishing connection between sender and recipient.

1) The recipient name should exist in sender's friend list. *validation (j)* is used to validate the friend's list of sender and *recipient_exists* contains the recipient name.
2) The recipient should be accessible from sender's location. The function *location (loc)* is used verify recipient location.

The connection will be established, if the above constraints are satisfied. Primary connection ensures that sender authenticated the recipient and the communication link will be established between them. But, the message needs to be encrypted before it being transferred. The second section of MAvanet sender side algorithm discuss about message encryption (Line 10).

Algorithm $\text{MAvanet}_{\text{sender}}$(msg,loc,rec_name,FRIEND_LIST(i)

```
1.  Extract_Topology()
2.  for all j ∈ FRIEND_LIST (i) do
3.          recipient_exists = validation (j)
4.  end for
5.  current_location = location (loc)
6.  if (recipient_exists AND current_location == 1) then
7.      call QR_encryption (msg)
8.          encryption = QR_Encryption (msg)
9.          con_msg = Code_Word (encryption)
10.         mat_pat = Gen_Mat_Pat (con_msg)
11.         qr_input = Gen_QR_Format (mat_pat)
12.         msg_encoding = QR_encoding (qr_input)
13.     print QR code is generated
14. end if
15. Send (msg_encoding, rec_name)
```

Function *QR_Encryption (msg)* is used to encrypt the message from sender to recipient. The following steps are involved in converting text message to QR code. *Code_Word (encryption)* is used convert input message into 8bit code words. The Reed-Solomon error correction will be added to code words and it will be stored in *con_msg*. The function *Gen_Mat_Pat (con_msg)* is used to convert code words into matrix pattern (i.e.,) it forms the square. The code words will be placed from bottom left corner to top right corner and it

will be stored in *qr_input*. The function *Gen_QR_Format (mat_pat)* is used to form 15bit information, which is used to create QR code and it will be stored in *msg_encoding*. Finally *QR_encoding (qr_input)* is used to generate QR code. After successful generation of QR code, the message will be transmitted from sender to intended recipient.

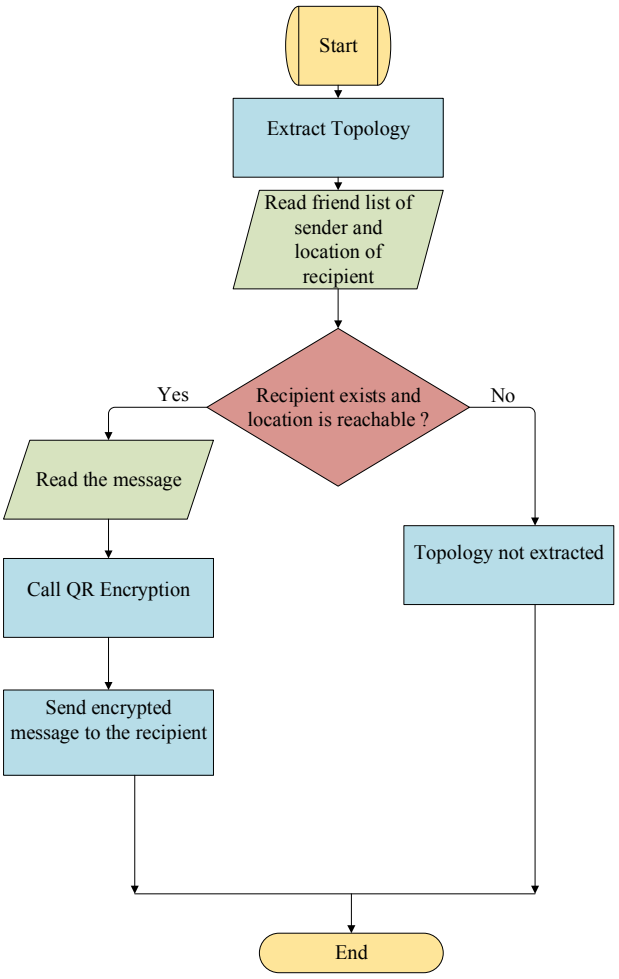

Figure 8: Flowchart for MAvanet sender side algorithm

MAvanet receiver side algorithm: In receiver side QR decoding algorithm will be used to decode the encrypted message. Receiver side algorithm of MAvanet discuss about message decryption (Line 5). Here, the sender name should exist in recipient's friend list. *validation (j)* is used to validate the friend's list of sender and *sender_exists* contains the sender name.

Function *QR_Decryption (msg_encoding)* is used to decrypt the message at receiver end. The message needs to be decrypted will be stored in *decryp_msg*. The function *QR_Reader (decryp_msg)* is used for decryption. The decrypted message will be stored in *inp_message* and it will be displayed to the recipient.

Algorithm MAvanet$_{receiver}$(msg_encoding,FRIEND_LIST(i))

```
1.  for all j ∈ FRIEND_LIST (i) do
2.      sender_exists = validation (j)
3.  end for
4.  if (sender_exists == 1) then
5.     Call QR_Decryption (msg_encoding)
6.        decryp_msg = QR_Decryption (msg_encoding)
7.        inp_message = QR_Reader (decryp_msg)
8.  end if
9.        display the message to recipient
```

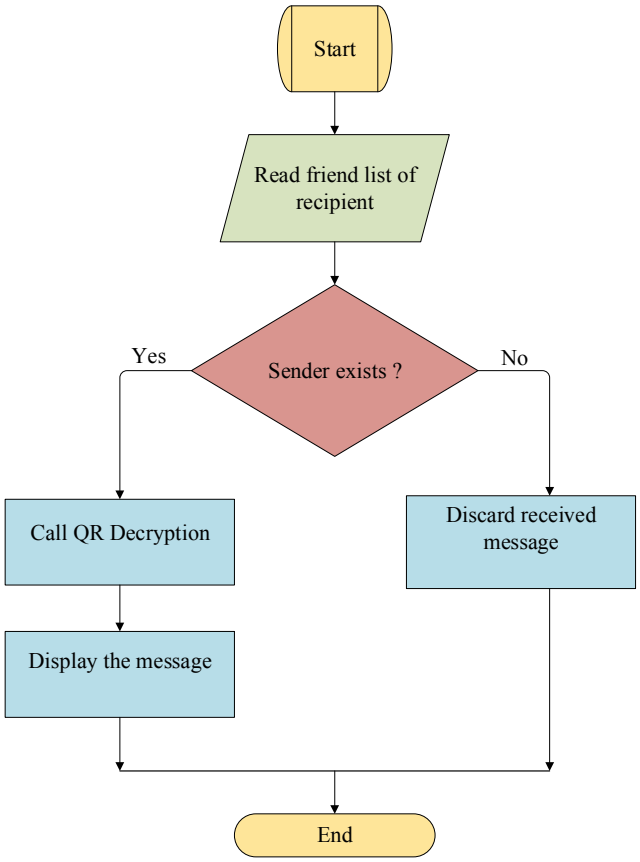

Figure 9: Flowchart for MAvanet receiver side algorithm

VI. Performance Evaluation

The simulation of our algorithm is done using ns-2 simulator [17]. We considered the following parameters to measure the performance:

- Message dropping probability: The probability of message dropped before it reaches the receiver.
- Latency: The delay of delivering packets from sender to receiver.
- Efficiency of QR algorithm: Time taken by the QR algorithm for encryption and decryption of message.

The results are obtained at a constant interval of 3%.

A. System Analysis

In system analysis, we calculated the probability of system failure. Failure of system will occur in following scenarios: 1) device damage, 2) malicious attack, 3) device offline, etc. The probability of system failure $P_{sysfail}$ is given by:

$$P_{sysfail} = \sum_{i=0}^{n-m} \binom{n}{i} \lambda^i (1-\lambda)^{n-i} \quad (1)$$

Where, λ is the probability of device failure, n is the no of users connected in a system and m is to recover the original data. The system failure will occur when there are more than $n-m$ failures at a time

From equation (1), it is clear that when m increases, the reliability of system decreases since the system can tolerate minimum number of failures. Like the quality of message, the probability of system failure also contributes in performance of the system. Minimum number of failures leads to maximum performance in the system.

B. Message success rate analysis

In this section, we are calculating the message success rate. Here, message success rate is directly proportional to performance of our proposed system. Increase in message success rate will increase the performance of the system. The message success rate M_{SR} is given by:

$$M_{SR} = \frac{P_{msg} + \varepsilon_{delay}}{N_{users}} \quad (2)$$

$$P_{msg} = \begin{cases} 0, no\ communication\ link\ established \\ 1, communication\ link\ established \end{cases}$$

Where, P_{msg} is the probability of message delivery. It can be either 0 or 1. If P_{msg} is 0, it indicates there is no communication link established between sender and receiver or If P_{msg} is 1, it indicates there is a communication link established between sender and receiver. ε_{delay} is the delay of delivering packets and N_{users} is the number of users in a system. From equation (2), it is clear that the quality of system depends on the number of users. The message success rate is increased when the number of users N_{users} is less and decreased when the number of users N_{users} is more.

C. Experimental Setup

1) Delay analysis of MAvanet: In this analysis delay is calculated in seconds with respect to the number of users. From Figure 10, we can observe that, the delay increases as the number of users increases in the system for a given input text message. As the number of user's increase, more data should be processed simultaneously, hence we can observe the delay.

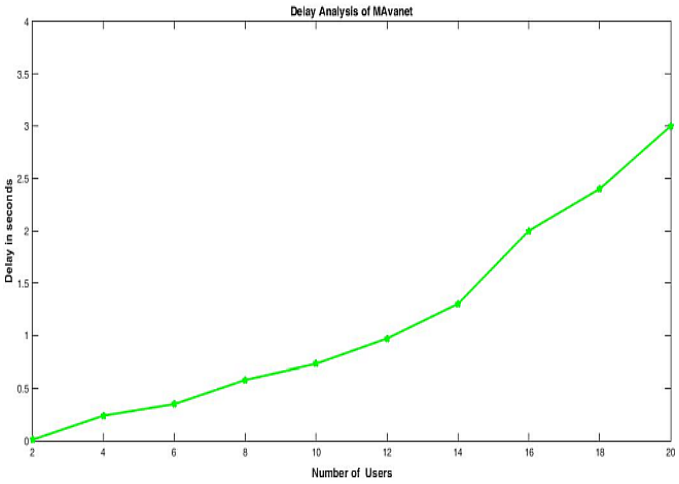

Figure 10: Delay analysis of MAvanet

2) Message delivery quality of MAvanet: Figure 11 represents message delivery quality in MAvanet for a given input text message. For this analysis message delivery quality is calculated with respect to number of users. As shown in Figure 11, message delivery quality decreases as the number of users increases in the system. This is due to the increase in load of a system when the number of users increases. However, the number of users connected to this network is constrained as the active users in a social network is limited at a particular time (t). It increases the message delivery quality of our system.

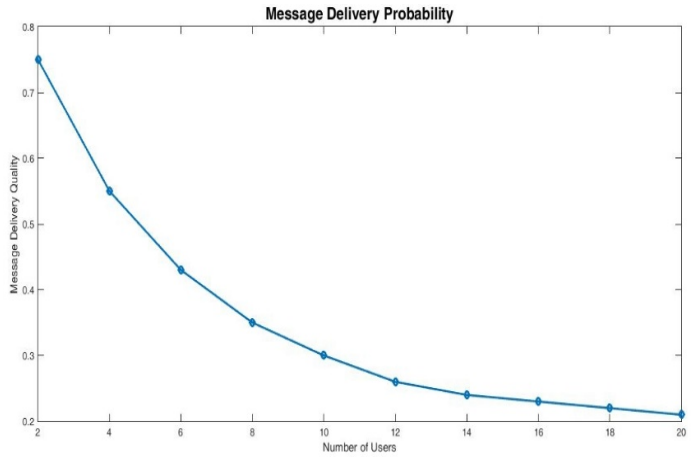

Figure 11: Message delivery probabiility of MAvanet

3) Message authentication probability: Figure 12 represents message authentication probability of MAvanet and P2P systems. In this simulation, we consider probability of message delivery failure with respect to number of users. We assume that for each user the probability of message delivery failure is distributed in the range of (0-1).

The P2P system does the message authentication randomly [18] but our proposed system MAvanet provides message authentication based on social tie ups. As shown in Figure 12 our MAvanet system outperforms the P2P system, especially when the number of users is increasing. We further observe that when the number of users increases very high, the probability of failure for both the systems is large. This is due to the load on a system increases as the number of user's increase.

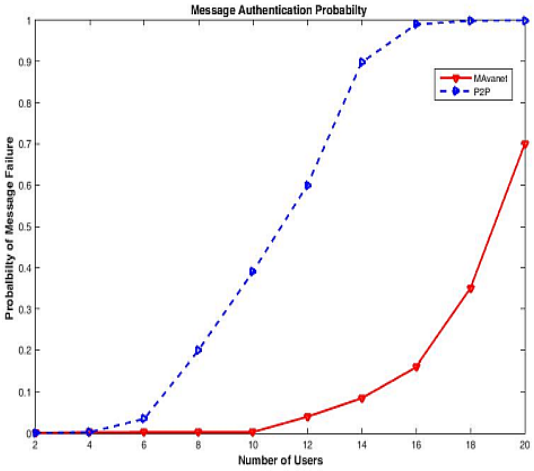

Figure 12: Message authentication probability of MAvanet

VII. Conclusion and Futurework

In this paper, we proposed a system which addresses the message authentication in VANET. The use of QR code in message encryption and decryption increases the performance of the system since it provides the facility of high speed encoding and decoding process. We used social networks to build an active topology in the system. The topology created ensures that input text message gets authenticated and it reaches the relevant user associated in a primary connection. We have proposed an algorithm (MAvanet) which is secure, and gives better performance when compared with others.

In this paper we have concentrated on extracting topology using primary connection and we will extend this approach to extract topology based on secondary connections and other lower level of connections using multi hop technique. This will improve the scalability of our current architecture.

References

[1] X. Lin and R. Lu, *Vehicular Ad Hoc Network Security and Privacy*: John Wiley & Sons, 2015.

[2] Official US government website for distracted driving:*http://www.distraction.gov/stats-research-laws/facts-and-statistics.html*

[3] S. Mallissery, M. Manohara Pai, R. M. Pai, and A. Smitha, "Cloud enabled secure communication in Vehicular Ad-hoc Networks," in *Connected Vehicles and Expo (ICCVE), 2014 International Conference on*, 2014, pp. 596-601.

[4] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth," in *Communications and Signal Processing (ICCSP), 2014 International Conference on*, 2014, pp. 768-772

[5] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of network and computer applications,* vol. 37, pp. 380-392, 2014.

[6] H. La Vinh and A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," *International journal on AdHoc networking systems (IJANS),* vol. 4, pp. 1-20, 2014.

[7] Pew Research Center website: *http://www.pewinternet.org/2015/01/09/social-media-update-2014/*

[8] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *vehicular Technology, IEEE Transactions on,* vol. 59, pp. 3589-3603, 2010.

[9] L. Campelli, M. Cesana, and R. Fracchia, "Directional broadcast forwarding of alarm messages in VANETs," in *Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on*, 2007, pp. 72-79.

[10] I. Tkachenko, W. Puech, O. Strauss, J.-M. Gaudin, C. Destruel, and C. Guichard, "Centrality bias measure for high density QR code module recognition," *Signal Processing: Image Communication,* vol. 41, pp. 46-60, 2016.

[11] S. Dey, A. Nath, and S. Agarwal, "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 512-517.

[12] U. Rajput, F. Abbas, H. Eun, R. Hussain, and H. Oh, "A two level privacy preserving pseudonymous authentication protocol for VANET," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2015 IEEE 11th International Conference on*, 2015, pp. 643-650.

[13] S. Biswas, J. Mišić, and V. Mišić, "ID-based safety message authentication for security and trust in vehicular networks," in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference On*, 2011, pp. 323-331.

[14] Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li, "Efficient authentication and access control of message dissemination over vehicular ad hoc network," *Neurocomputing,* 2015.

[15] X. Liu, Z. Shan, L. Zhang, W. Ye, and R. Yan, "An efficient message access quality model in vehicular communication networks," *Signal Processing,* vol. 120, pp. 682-690, 2016.

[16] K. Lim and D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," *Vehicular Communications,* vol. 4, pp. 30-37, 2016.

[17] ns 2 website: *http : //www.isi.edu/nsnam/ns/.*

[18] H. Weatherspoon and J. D. Kubiatowicz, "Erasure coding vs. replication: A quantitative comparison," in *Peer-to-Peer Systems*, ed: Springer, 2002, pp. 328-337.