REVIEW ON VARIOUS SECURITY THREATS & SOLUTIONS AND NETWORK CODING BASED SECURITY APPROACH FOR VANET

Jitendra Bhatia and Bhumit Shah
Department of Computer Engineering, Nirma University, Ahmedabad.

ABSTRACT

Intelligent Transport Systems (ITS) are advanced applications which, without embodying intelligence as such, aim to provide innovative services relating to different modes of transport and traffic management and enable various users to be better informed and make safer, more coordinated, and 'smarter' use of transport networks. Today ITS (Intelligent Transport system) has the main focus in research of Mobile Ad-hoc Network (MANET) Communications. A Mobile Ad-hoc Network (MANET) is a self-configuring network of mobile devices called mobile nodes. Vehicular Ad-hoc Network (VANET) is a prime concept of MANET where security, privacy and reliability are major issues. To support message differentiation in VANET, IEEE 802.11p standard is incorporated in vehicular communication. In this paper, we analyze various security aspects and threats in VANET and propose the novel solutions based on network coding. Network coding is a technique in which node is allowed to combine and encode one or more input packets into encoded packets instead of directly forwarding them over finite field. In this paper, we also examine the tradeoffs of the proposed solutions along with the necessary solutions to overcome them.

KEYWORDS: *VANET, Security, Privacy, Reliability, Network Coding.*

I. INTRODUCTION

Vehicular ad hoc network (VANET) has become one of the promising fields of research due to the significant progress in Intelligent Transportation Systems (ITS). VANET has numerous applications in our daily life which includes traffic awareness, accident detection, automatic toll paying, collision avoidance, internet usage on road etc. This is possible due to prominent progress in wireless communication via which we can connect the vehicles and information is passed in the form of signals. Vehicles act as a mobile node and signals propagate through air.

As VANETs are using wireless communication channel, one important issue which is need to be taken care of is its privacy, security and reliability. As wireless communication has its inherent characteristic of broadcasting capability, one must be aware that whatever the messages or the information that is being transmitted by sender will be received by all other nodes currently in its communication range. There are RSUs (Roadside Units) and OBUs (On-Board Units) which gives us the mechanism of communication with other vehicles, so there is a good amount of probability that either of them might be attacked, hacked or crashed down through various threats such as malicious nodes, wormhole attacks, accidents, password breach etc. If this will not properly be paid attention then the whole VANET system may malfunction and result in some difficulties especially in situations where life critical information is involved.

There have been several of methods suggested to secure the communication and provide reliability and privacy to the information on air.

Privacy preserving scheme: 1. Pseudonym Based & 2. Group Signature Based

In first scheme, protection is provided by set of public-private key pairs and set of pseudonyms to sign the safety messages, given by TA (Trusted Authority). Pseudonyms are periodically changed and thus a node can be prevented from attack by not disclosing their identity. But there is a major disadvantage if the new pseudonym got corrupted because there is no scheme to ensure non availability of links of consecutive pseudonyms acquired by vehicles. In second scheme, group of vehicular nodes are formed and group leader can only sign the safety messages on behalf of sender from that particular group. We can also encrypt the safety message along with this pseudonym to get more extent of privacy.

Though these both schemes are crucial for privacy protection, there are several drawbacks we have to deal with. One major issue is database. RSU has to deal with large database to identify the sender from their keys and pseudonyms and as they are changing frequently, we must have at least 50000 key pairs per year for one vehicle driven 3 hours a day. In this way delay (i.e. time to authenticate the sender and receiver) will also be introduced in signal transmission. So to overcome these difficulties, we have proposed several schemes to overcome different attacks.

This paper is organized in the following way. Threats are reviewed in section II whereas solution and comparison of various techniques are mentioned in section III. The novel approach for the consequences from reviewed schemes is discussed in section IV. Finally section V concludes the paper with future works in section VI.

II. VARIOUS THREATS

As described above, VANET system uses the wireless channels so they are always subject to get vulnerable by several threats listed below.

The major threats to the VANETs are:

- Message Forging (Bogus Information)
- Impersonation (Pretention)
- Packet Dropping
- Black Hole
- Sybil Attack
- Denial of Service (DoS)
- Worm Hole Attack
- Hidden Vehicle Problem
- On-Board Tampering etc.

2.1 Message Forging: This is one of the most known attacks which are primarily concerned with the ongoing information. Malicious nodes forge the message coming from the sender and transmit to the other vehicles in the range so that all the other nodes get the wrong information and VANET system will collapse.

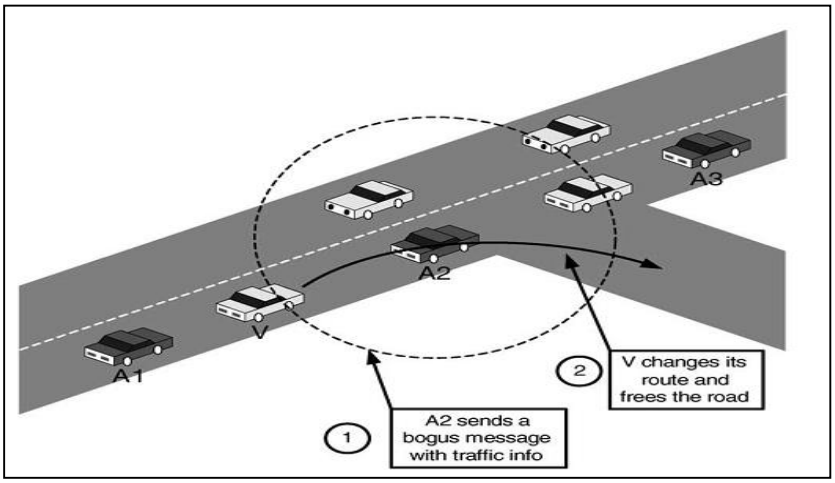

Fig-1. Bogus information [1]

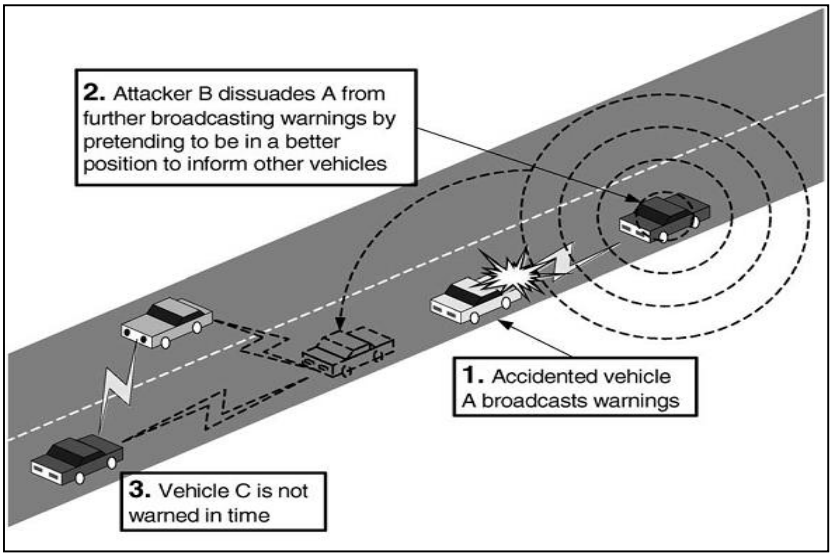

Fig-2. Hidden vehicle problem. [1]

As shown in above image, this type of attacks are hazardous to human life as one may get wrong traffic information and meet with accidents.

2.2 Wormhole Attacks: In this attack, at least two malicious nodes in a network transfer packets from a private tunnel which they have built by cooperation with each other and if message passes through this tunnel then security breach occurs. Whenever any node is affected by Wormhole, it can do faulty behaviours, get unauthorized access and even prepare a DoS (Denial of Service) attack which is very dangerous for ad hoc networks particularly in VANET. In short Wormholes creates a scenario of incorrect understanding of network topology.

2.3 Denial of Service: This is a type of attack which cause jamming or congestion in the network. As its name describes, service required by particular sender is denied (i.e. message passing is stopped) at particular node affected by malicious node. This may cause an accident by sending dummy messages.

2.4 Hidden Vehicle: This is one of the most serious threats related to VANET safety. In this, attacker deceives the sender vehicle that it is in better position to send the safety messages so sender vehicle stops its signal transmission to curb the congestion in the network but the attacker mislead other nodes by passing wrong information or even not transmitting any warning messages at all. In other term, sender vehicles become hidden to others or its location being forged.

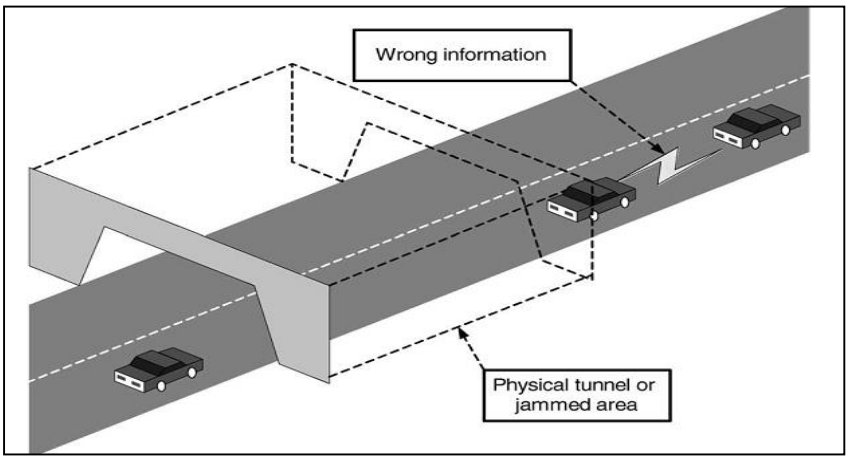

Fig-3 Tunnel jamming. [1]

Sometimes attacker may be also hidden to others by keeping itself in tunnel and cheating with safety messages which is equivalent to disabling the system.

2.5 On-Board Tampering: This issue is basically related to the reliability and privacy of the safety messages. OBUs (On-Board Units) are equipped with hardware specifications as well they have

software features implemented over there. Each of the OBU has its own key pairs (public-private keys) called pseudonyms for their identity and if it is tampered, the OBU behaves abnormally and it may cause harm to whole system.

III. PROPOSED SCHEMES FOR VARIOUS THREATS AND THEIR COMPARISON

3.1 Secure VANET Communication through Packet Leashes (SVCPL):

This scheme mainly deals with Wormhole Attacks. Earlier proposed scheme dealt with security but one major drawback of that scheme was its failure in scenario even packet was not affected by wormholes. We have tried to analyze this problem and proposed the modified scheme which has been proved efficient and secured (described in later section).

Packet Leashes: It is additive information that can be added to the transmitted packet for the restriction of its allowed transmission distance or time. Taxonomy has been described below.

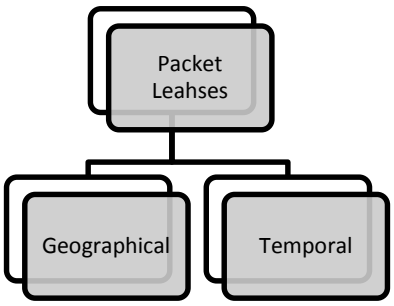

Fig-4 Types of Packet Leashes

***Geographical leashes*:** These are location based leashes which is added to the packets during transmission which includes the sender location L_s and the transmission start time T_s. When receiving the packet, receiver compares these values with location L_r and time T_r. If the clocks of the sender and receiver are synchronized to within $\pm\Delta$, and v is an upper bound on the velocity of any node, then the receiver can compute an upper bound on the distance between the sender and itself, D_{sr}. The condition that must be followed is,

$$D_{sr} \leq ||L_s - L_r|| + 2v\,(T_r - T_s + \Delta) + \mu$$

Where, μ is an error in location of sender or receiver.

By preserving this condition, geographical leashes can detect malicious nodes and thus, wormholes can be caught.

***Temporal leashes*:** The main necessity of this method is to have the tightly synchronized clocks between sender and receiver. There must be some upper on the travelled time of a packet and that can be calculated from T_s and T_r and the difference between two clocks should be as low as possible. So the condition that is to be satisfied is,

$$T_{total} \leq T_s + T_r + \Delta$$

Where, Δ is in terms of few microseconds or nanoseconds.

Authentication: Information within the packets such as time stamp and location must be preserved from alteration by malicious nodes with a technique. In another word, whatever comes to receiver, it must be able to confirm values that it is legal and authenticated. There are various ways for message authorization such as TIK, TESLA, LHAP. Digital Signature scheme is also proposed which is very efficient but it induces the overhead in the system. We can also used novel scheme called HEAP which uses HMAC based protocol for authentication which gives better performance as well as low overhead.

3.2 Short Messaging Service for VANET (SMSV):

As VANET communication is a new concept in research, the implementation is also costly as compared to normal communication. The cost of TPD (Temper proof Device), EDR (Electric Data Recorder), GPS (Global Positioning System), OBU and RSU Deployment, Infrastructures are very much high for

any developing or NON-VANET county. So there should be some way so that VANET can be used at low cost and efficient performance.
Till now there has been very little research on low cost VANET so we are proposing one scheme for the same which has quite better performance and efficient mechanism.
Mobile Communication is developed field in each country and SMS (Short Messaging Service) is very important feature of it. It can be used for vehicular communication also by sending safety or non-safety messages through SMSs from senders to the receiver.

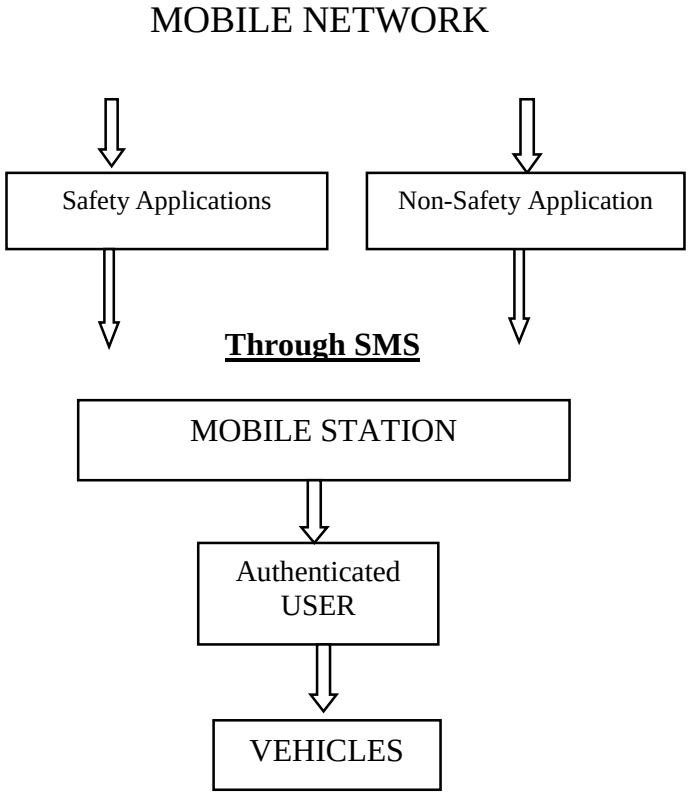

Fig-5 Basic Concept behind SMSV

Working: Prime Idea behind the mobile network usage is Mobile Switching Center (MSC) and Short Messaging Service Center (SMSC). MSC performs all switching task from within and outside the network. MSC has two registers called Home location Register (HLR) and Visitor Location Register (VLR). HLR is a permanent storage database used for management of users and service profiles. These both are used to find the user location. If accident happens in any region, then HLR gives information about where the users reside in that region. HLR directly communicates with Short Messaging Service Center (SMSC) and provides the possible rerouting routing information for the specified users through sending SMSs.
Information Collection is the major task in this scheme where ICD (Information Capture Device) is used. It consists of various sensors, transmitters and electronic equipment's which are used to capture the data of any accident or traffic jam. ICD sends this information to BTS (Base Transceiver Station) which in turn sends to MSC and SMSC. SMSC broadcast this SMS to all users in the range and hence the communication is achieved. For ICD, we need to develop some efficient and robust algorithms which stand in adverse conditions as well.
This solution can provide service to safety as well as non-safety applications. Through SMS services people can find the empty parking lot near the shopping malls, restaurants and sport complexes (Non-Safety) and users can take appropriate decision to use alternative route A or route B upon knowing the accident location through SMS (Safety). But we need to take care of trust and privacy issues in the implementation phase.

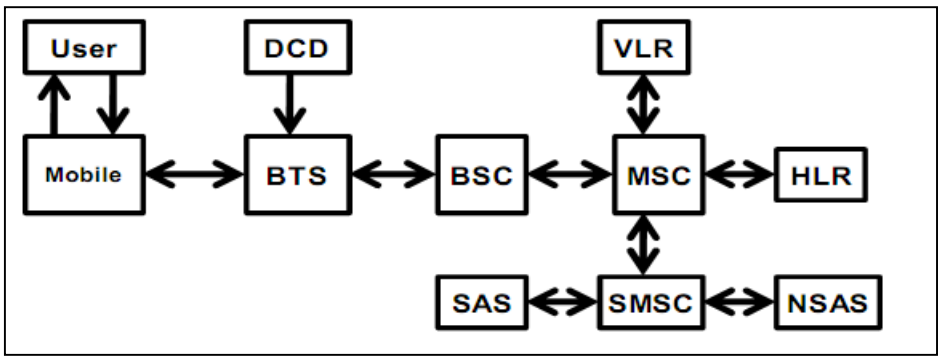

Fig-6. Working Principle of SMSV [10]

3.3 Sybil Attack Detection and Solution:

Sybil attack is a spoofing attack which is created by stealing the identity of any current working node, forging or pretending to be another node. It also penetrates wrong topological information in the network through non-existing nodes (called Sybil identities). It highly threatens the VANET system because system may crash or disable due to wrong information about any particular identity or malicious node.

Working: in this scheme, RSU is the main component. Periodically beacons are sent to the RSUs by the nodes coming under their range which contains the information about the ID and the location of the particular node.

VEHICLE ID	TIMESTAMP	POSITION

Fig-7 Beacon Packet Structure

Authorized RSUs periodically calculate the distance based on (i) Received Signal Strength (RSS) and (ii) angle of vehicle sending the beacon with reference to the RSU. Each RSU compares and analyzes the difference of the neighboring vehicles' motion trajectories. Sybil nodes are detected based on the difference value and classified in various categories as per the intense level of attack by the Sybil identities and given a special number called 'rank' which depicts its intensity. Each RSU calculates and stores the record of all the vehicles passing across them in the format as shown below.

RSU-ID	Vehicle-ID	Time stamp	Angle	Distance	RSS	#Rank

Fig-8 Format of the frame created by RSU in this scheme

The Basic assumption is to be made here that RSU must be honest and robust to be affected by any other threats. Attacker broadcasting fake accident warning will be detected in fairly short period.

3.4 Witness and Trust based Neighbor Table Scheme (WTNTS):

The malicious nodes have abnormal behavior than the normal node which can be easily detected through witnessing them along with regular time intervals. In this proposed scheme, *reputation* of specific nodes plays an important role in determining the plausibility of it through the witness based table of neighboring tables.

This can be done through following steps:

- *Reputation Checking*: This is the first and the main stage of this scheme where the reputation and the plausibility are to be checked by RSU and give the prior confirmation about its validity. This is done directly or indirectly. Directly means the reputation level is determined by experiences of other nodes and the node's behavior whereas in indirect method, the reputation of a node is gained from nodes whose reputations are already known and depending upon the relative position and geographical circumstances, decision has to be made.

- *Neighbor Table Formation and Message Handling*: On arrival of an event message every forwarding node generates an opinion on the trustworthiness of this message and according to the reputation level (r) of a node; an entry has to be done in the Neighbor Table. Along with this, the position, timestamp, velocities are added by the OBU. This is shown below.

No.	*name*	*position*	*velocity*	*time*	*r*
1	A	P_1	v1	t_1	0.3
2	RSU_1	P_2	0	T	1
…	…	…	…	…	…

Fig-9. Trust Neighbor Table (TNT) [6]

- *Selection and Rejection*: According to the information in the table, a node is marked as Selected (S) or Rejected (R) by seeing upon the value of 'r' as well as its relative position calculations.

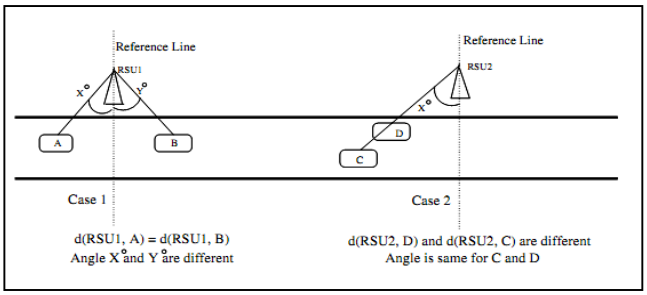

Fig-10. Identification of Sybil attacks.[6]

Now, if any message comes, through the table lookup method a message is accepted if the vehicle is *'trusted'* and discarded if the vehicle is *'rejected'*.
The main advantage of this scheme is it is highly dynamic in nature because as the time passes, the trust values are updated upon its quality of service and regarding plausibility so the malicious node can be easily detected in short span of time.

Comparison of above existing schemes based on privacy, security and reliability:

In VANET, the main goal is to achieve privacy, security and reliability. If all of them are satisfied then that scheme has to be the best but in real does not exist. Each of them has several advantages and disadvantages which continues the cycle of research.

Table 1. Comparison between reviewed schemes on privacy, security and reliability

	Scheme	**Privacy**	**Security**	**Reliability**
1.	For avoiding Wormholes	X	√	X
2.	SMS	√	X	X
3.	Sybil Attack	√	√	X
4.	TNT	X	√	X

Here, in both the figures we have shown the pros and cons of the reviewed schemes for the threats regarding different parameters.

Table 2. Comparison between reviewed schemes on delay, overhead and cost efficiency

	Scheme	**Delay- Problem**	**Overhead-Induced**	**Cost-efficiency**
1.	Wormholes	X	√	X
2.	SMS	√	X	√
3.	Sybil Attack	X	√	X
4.	TNT	√	√	√

In Packet Leashes scheme (1), we get the security against the wormholes but it is not the only essential thing. The privacy of sender and receiver, reliability of message, cost etc. has to be taken care for better and optimized solution, for which this scheme fails because the packet leashes only checks the location and timestamp without paying attention to the ID of the nodes and the scheme does not have any mechanism to verify whether the packet has been received by the receiver or not (Acknowledgements).

In SMS transmission message scheme (2), we get our data transmitted very easily through cheaper way and less delay but the main things-privacy and security is overlooked. There is no way to check whether the messages are from reliable and authenticated node or not.

In Sybil attack solution scheme (3), the scheme has less overhead due to the extra fields in the packet header for the location and the angle of sender. Though it takes care of security and privacy very well, reliability is yet to be implemented in that because the message must reach at desired destination.

In TNT solution (4), there is a high overhead of neighbor table so it also introduce delay in forwarding information. It provides security mechanism from threats but we can optimize it with providing privacy and reliability a well via private key infrastructure mechanism assembling to this scheme and this scheme is efficient and economical for the developing countries.

Observing these tables, it is clear that all solutions are lacking at some aspects of data communication, particularly reliability which is one of the neediest parameters for it. So here we have tried to find the solution which gives essential privacy and security as well as fair reliability along with cost efficiency.

IV. PROPOSED SCHEME

In linear network coding encoded packets are linear combination of various original packets. So, meaningful coefficients should be used for encoding and decoding of packets. Linear network coding requires central authority to control generation of this meaningful coefficient. Algorithms employed for this should be centralized. But in wireless networks due to node's mobility and heterogeneity of network distributed approaches are suitable. So RLNC suggests the random generation of the encoding coefficient [7].

In RLNC packets are encoded and decoded as follows:

Encoding

- Original packets $M_1, ..., M_n$
- Encode packet $X_i = \sum_i g_i M_i$, where i=0 to n
- Coefficients vector $g = (g_1, .., g_n)$

Forwarding: Encoding already encoded packets

- Set of encoded packets: $(g_1, X_1), ..., (g_m, X_m)$
- A new encoded packet: (g', X')
  where $X' = \sum_j h_j X_j$ where j=1 to m
  ($h_1, ..., h_m$ are randomly chosen coefficients) and $g_i' = \sum_j h_j g_i^j$, where j=1to m

Decoding

- Set of received packets: $(g_1', X_1'), ..., (g_m', X_m')$
- System of M linear equations $X_j' = \sum_i g_j' M_i$

with M_is as unknowns [7]

By applying RLNC, encoding vectors are kept in header part so only nodes which are aware of network coding they can only decode by doing inverse of that if they get sufficient number of innovative packets. But again, vectors are susceptible for getting corrupted or sniffed by malicious node so for that again we can provide any cryptography based mechanism to protect the encoding vectors.

V. CONCLUSION AND OPEN ISSUES

As the security and reliability are the essential requirement for VANET, we must find the method which provides both at a time. Each reviewed scheme provides some of the aspect related to security but our proposed scheme including network coding which is based on linear algebra is able to deal with security as well as reliability at the same instant. Though computational overhead may increase but the level of security and reliability is increased.

VI. FUTURE WORK

We will implement above proposed security mechanism in RLNC variants called Generation-by-Generation RLNC and RLNC with Multi Generation Mixing (MGM). MGM increases the decodable rate of encoded packets. [13]

REFERENCES

[1]. Maxim Raya, Jean-Pierre Hubaux "Securing vehicular ad hoc networks", Journal of Computer Security 15 (2007), page 39-68.
[2]. Seyed Mohammad Safi, Ali Movaghar, Misagh Mohammadizadeh, "A Novel Approach for Avoiding Wormhole Attacks in VANET" , Second International Workshop on Computer Science and Engineering (2009), page 1-6.
[3]. Ali Osman Bayrak, and Tankut Acarman, "A Secure and Privacy Protecting Protocol for VANET", 2010 IEEE Intelligent Vehicles Symposium, University of California, San Diego, CA, USA, June 21-24, 2010.
[4]. Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, "A Novel Defense Mechanism against Sybil Attacks in VANET", SIN'10, Sept. 7–11, 2010, Taganrog, Rostov-on-Don, Russian Federation.
[5]. Sanjay K. Dhurandher, Mohammad S. Obaidat, Ankur Tyagi, "Securing Vehicular Networks: A Reputation and Plausibility Checks-based Approach", IEEE Globecom 2010 Workshop on Web and Pervasive Security.
[6]. Xiaoping XUE, Nizhong LIN, Jia DING, Yiwen JI, "A trusted neighbor table based location verification for VANET Routing", IET 3rd International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2010), 26-29 Sept. 2010.
[7]. Jitendra B Bhatia, Ankit patel, Zunnun Narmawala, "Review on variants of Network Coding in Wireless Ad-Hoc Networks", Nirma University International Conference on Engineering (December 2011), pp. 1-6, DOI:10.1109/NUiCONE.2011.6153236
[8]. Danda B. Rawat, Bhed B. Bista, Gongjun Yan, Michele C. Weigle, "Securing Vehicular Ad-hoc Networks against Malicious Drivers: A Probabilistic Approach", 2011 International Conference on Complex, Intelligent, and Software Intensive Systems.
[9]. Irshad Ahmed Sumra, Halabi Hasbullah, J.Ab Manan, Mohsan Iftikhar ,Iftikhar Ahmad, Abdullah S Alghamdi, "A Novel Vehicular SMS System (VSS) Approach for Intelligent Transport System (ITS)", 2011 11th International Conference on ITS Telecommunications, page 1-7.
[10]. Lifang Huang, Hongwei Meng, Cong Tang, Wenlue Song, "DIFO: Discovering Faulty OBUs in VANETs", 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery.
[11]. Zunnun Narmawala, Sanjay Srivastav, "MIDTONE-MultiCast In Delay Tolerant Network", Communication and Networking in china 2009, ChinaCOM 2009, 4th International Conference. Page(s): 1-8
[12]. Rodica Stoian, Lucian Andrei Perisoara, Radu Stoica, "Random Network Coding for Wireless Ad-Hoc Networks", Wireless Communications and Networking Conference xWCNC IEE 2010
[13]. Mohammed Halloush, Hayder Radha, "Network Coding with Multi-generation Mixing", ICC 2008proceedings

AUTHORS:

Jitendra Bhatia received the M.Tech (CSE) in 2012, from Nirma University Ahmedabad, Gujarat. Currently he is an Assistant Professor in Computer Science and Engineering department at Nirma University, Ahmedabad, Gujarat, India. He is having 8 years of teaching experience and his current research interest is in secure content distribution in VANET.

Bhumit R. Shah is a 3rd year computer science engineering student at Nirma University, Ahmedabad, Gujarat, India. He has done number of projects during his academics on various subjects such as network security, graphics, android application etc. He is also in a study of security architecture of cloud computing applications.