Security & Content Distribution of Vehicular Ad-Hoc Network

Prachi B. Danak
M.TECH (Digital Communication)
Department of Electronics& communication
GITS, Udaipur, Rajasthan

Prof. M. D. Sabir
Assistant professor
Department of Electronics& communication
GITS, Udaipur, Rajasthan

***Abstract*--- VANET is a type of network. In this type of network vehicles act as different nodes and communicates with the roadside units.VANETs are in simple way works as implementation of ITS (Intelligence Transport System). ITS is developed with a view to provide traffic situation ,weather condition, space avaiblity for parking etc. which is useful for safety warning making unit(vehicle) a safety unit and also makes unit with comfort also. But while doing so the reliability factor plays vital role to make the system more acceptable and popular.Content distribution in Vehicular Ad-Hoc Networks (VANET) is particularly challenging due to the high mobility. Considerable research has been made focused on enhancing the security and reliability of such networksdesigned for VANETs.Reliability of any process or data is the most important factor for the end result and ultimately for decision making. Keeping in mind this aspect this paper is presented keeping in the aspect of improving reliability of VANET as central point. While doing so some technique is thought to be used.For improving reliability of VANET with the use of reliability metrics are defined for the evaluation of Random linier network coding technique and for security RSA algorithm is conceived in this paper.**

***Keywords*--Intelligent Transport Systems; VANETS; MANETS; Ad Hoc Networks; VANET Security; Traffic Management.**

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have attractedattentions as fortechnology the transportation systems. Concept of network vehicle was first proposed by a team of engineers from Delphi Delco Electronics Systems and IBM Corporation in the year 1998 [1]. The NS2 simulator is used to simulate the VANET for the research purpose. The VANET architecture could be classified based on: WLAN/Cellular, Ad-hoc,and Hybrid models (Vehicle to Vehicle (V2V) & Vehicle to Infrastructure (V2I), and Vehicle to Vehicle (V2V) & Vehicle to Roadside (V2R)) [3]. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs).

In mechanical engineers to increase road safety and to differentiate themselves from their, vehicles are becoming "computers on wheels", or rather "computer networks on wheels". Manufacturers are about to make a quantum step in terms of vehicular IT, by letting vehicles communicate with each other and with roadside infrastructure; in this way, vehicles will dramatically increase their awareness of their environment, thereby increasing safety and optimizing traffic. Re-searchers have investigated many aspects of vehicular communications[4, 6, 7, 8, and 9].

In turn, the IEEE and ASTM standardization bodies have proposed two standards specifically for vehicular environment, specified in the IEEE 802.11p and Wireless Access for Vehicular Environment (WAVE) standards. The WAVE standard supported two different stacks of Transport and Network layers namely the normal TCP/IP protocol stack and a new proprietary WAVE Short Message Protocol (WSMP).IEEE is working on a variation of 802.11 standard that would be applied to support communication between vehicles and the roadside, or, alternatively, among vehicles themselves, operating at speeds up to 200 km/h, handling communication ranges as high as 1,000 meters. PHY and MAC layers are based on IEEE 802.11a, shifted to the 5.9 GHz band (5.850-5.925 GHz within US). Estimated deployment cost is foreseen to be relatively low due to large production volumes.

Vehicular wireless networks differ from wireless ad-hoc network.

- Vehicles have far greater energy/power supply than normal mobile devices because more often energy can be derived from the vehicle itself.
- The size of the vehicle, a large number of sensors can be fitted onto the vehicles. This is particularly significant in case of having an intelligent transportation system with safety, security, communication and other services deployed.
- The vehicles usually travel at high speeds and thereby have great difficulty in consistently maintaining vehicle-to vehicle connectivity.

Fixed access points to cover all roads at short distance one from another, huge and expensive investment is required, which is practically impossible.

During the process of study for better system various models were adopted and reviewed. One of them is the model

for routing protocol formaking effective routing using the Secure AODVfor any real world traffic environments.Previous paper refers to Secure AODV (Ad-hoc On Demand Vector)routing protocol which is used in VANET for privacy purpose [15].Previous studies on VANET security concentrate on particular security mechanisms and solutions on VANET communications (e.g., [10-13]).VANET security design should guarantee authentication, non-repudiation, integrity and in some specific application scenarios, confidentiality and to protect the network against external threats. Reliability is also one of the important factors in VANET because of high mobility.High mobility of vehicle may affect the reliability of data. So improving reliability and security of data are given more importance in this paper. IEEE 802.11P based on DSRC (Dedicated Short Range Communication)technology is used forreliability&securitypurpose in VANET [14].because of high mobility in VANET for improving reliability. Because reliability is a major challenge in Vehicular Ad-hoc Network

Security and safety is a matter of prime concern in our life. One of them is safety and security of assets, particularly moveable assets like vehicle. Everyone wants to have utmost security of their vehicle. Everyone wishes to be most secure. Besides security ease in life is also a matter of prime importance. It is human nature that thrive for ease in all facets of life. Search of VANET technology has helped a lot to solve these problems.

II. PROBLEM DEFINATION

The safety threats is of majorconcern when we use VANET. Here we can use RSA technique for security which is encryption & decryption method. It is proposed technique well described in following section. To develop a reliability aware network coding based protocol to deliver information inVANET.While using AODV in VANET the reliability factor is considerably reduced because of high mobility so, the ongoing researches have gifted new and mordent technique. This technique are well described in next section.

III. INTRODUCTION TO PROPOSED TECHNIQUES

VANETs are a subgroup of mobile ad-hoc networks with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles.

Reliability andSecurity are main concerns in Vehicular Ad-hoc Network. AODV protocol which is used in MANET for improving reliability is not affective for VANET.The other issue with reliability is described in the shown in figure.

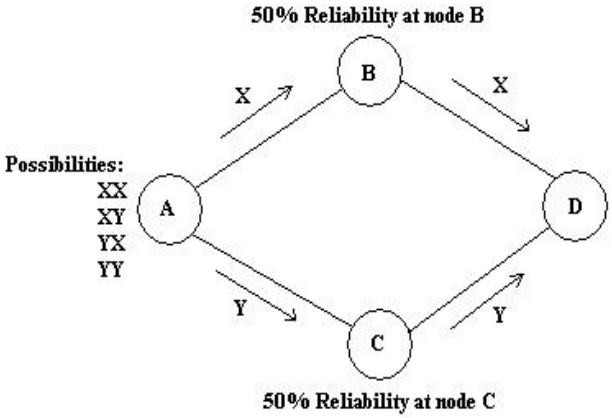

Fig. 1 Reliabilityissue

Suppose we have a message having two elements. Each message can have symbol ‘X’ or ‘Y’. Thus we have four possibilities: XX, XY, YX or YY.

Here, single path is allocated to node B and to node C. So, only element can be transmitted through either path. As a result only ‘X’ is transmitted to node B and element ‘Y’ to node C.

The whole scenario is shown in the figure 1. As a result, reliability at node B & C is only 50%. A new techniquewhich uses Random Linear Algebra is proposed to improve reliability. It is described in the later sections.

Security is another major concern in VANET. RSA algorithm technique provides better security in our network.

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret [16].

IV. PROPOSED ARCHITECTURE

A.Reliability

As discussed earlier, there is a need to improve reliability. Generated matrices, G & G’ are used in a technique to improve the same.

Suppose we have a message of size nx1 and n generated metrics G, G’, G’’, up to $G^{(n-1)}$ of size nxn. suppose there are n levels. At first level message is multiplied by G and at second level the result of first level is multiplied by G’, at third level the result of second level is multiplied by G’’ and so on. This continues up to n^{th} level.

The final result generated at the n^{th} level is transmitted in the network. This contains elements of the original message. The generated metrics are also transmitted within the packet.

By using the final result and generated metrics received at the destination node within the packet,original message can be reproduced.

This improves overall packet delivery reliability.

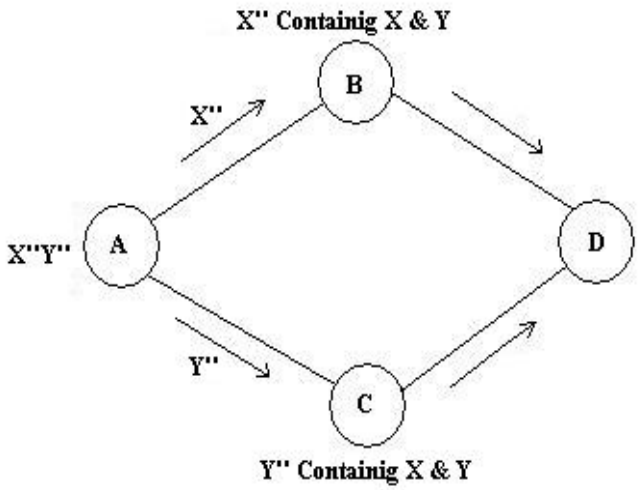

Fig.2 Basic idea of proposed architecture

Above figure represents the basic idea of the discussed technique. The example has message of size 2x1 and two levels to produce final result.

The original message, [X Y] is reproduced at node B & C from X'' and Y'' received at node B and node C respectively. Here, X'' and Y'', both contains X & Y.

B.Security

The most common public key element is RSA, named for its inventors Rivest, Shamir, and Adleman(RSA).It uses two numbers ,e and d ,as the public and private keys as shown in figure ().

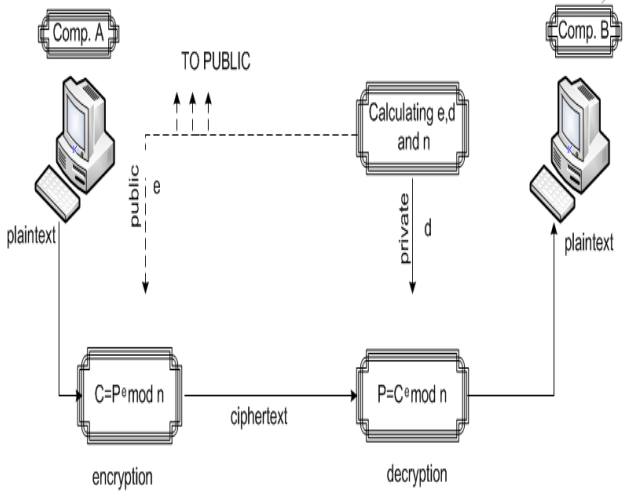

Fig.3 RSA Algorithm

The two keys, e and d, have a special relationship to each other, a discussion of this relationship is beyond the scope of this book. We just show how to calculate the keys without proof.

Selecting keys:

Computer A use the following steps to select the private and public keys:

- Computer A chooses two very large number p and q remember that prime number is one that can be divided evenly only by 1 and itself.
- Computer A multiplies the above to primes to find n, the modulus for encryption and decryption .In other words, $n=p\times q$.
- Computer A calculates another number $\phi = (p-1) \times (q-1)$.
- Computer A choses the random integer e. He then calculates d so that $d \times e=1 \bmod \phi$.
- Computer A announces e and n to the public; he keeps ϕ and d secret.

Encryption

Anyone who needs to send message to Computer A can use n and e. For example, if Computer B needs to send message to Computer A,she can change the message, usually a sort one,to an integer.This is the plain text. She then calculates the cipher text, using e and n.

$$C=P^e \pmod n$$

Computer a sends C, the cipher text, to Computer A.

Decryption

ComputerA keeps ϕ and d private .When he receives the cipher text, he uses his private key d to decrypt the message:

$$P=C^d \pmod n$$

C. Packet Structure

Data of our interest is put in the payload. This payload is needed to be sent to the desired destination securely and reliably.

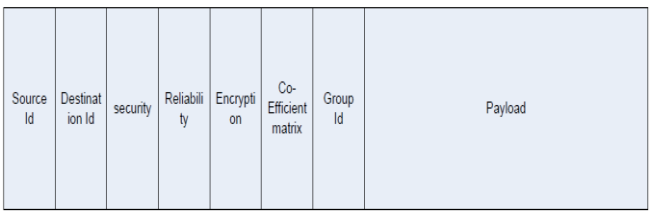

Fig. 4 Packet structure

So, the packet needs to have Source id, Destination id and other useful information which provides the same i.e. security and reliability.

We can also provide encryption to our message to prevent unauthorized access.

Another information which we need to have is generated metrics, to get our message back in the original form at the destination. This is transmitted in the Co-efficient matrix section. The packet structure is shown in Fig. 4

When Destination node Receive the message, according to packet structure it performs the decoding and getting the reliable message.

V. IMPLIMENTATION

A.For Reliability

We will show implementation of Random Linear Network Coding approach to improve reliability through a simple example.

Suppose we have a message containing two elements, M=$\begin{bmatrix}1\\2\end{bmatrix}$. Now instead of transmitting this message as it is in the network, we first convert it into E and then into E'. This is done by doing to level transformation. The transformation is shown below:

We take any generated random metrics G and G'.

$$G=\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix} \& \; G'=\begin{pmatrix}5 & 6\\7 & 0\end{pmatrix}$$

Now, E=G.M & E' = G'.E.

So,

$$E = \begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\begin{bmatrix}1\\2\end{bmatrix}=\begin{bmatrix}5\\11\end{bmatrix}$$

$$E' = \begin{pmatrix}5 & 6\\7 & 0\end{pmatrix}\begin{bmatrix}5\\11\end{bmatrix}=\begin{bmatrix}91\\35\end{bmatrix}$$

And k= G'.G.

So,

$$k = \begin{pmatrix}5 & 6\\7 & 0\end{pmatrix}\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix} = \begin{pmatrix}23 & 34\\7 & 14\end{pmatrix}$$

This E' and k is transmitted.

Now at the destination end, this E' and k are used to reproduce original message M.

Here, k.M= E'. So, k^{-1}. E'=M.

$$k^{-1} = 1/84\begin{pmatrix}14 & -34\\-7 & 23\end{pmatrix} = \begin{pmatrix}14/84 & -34/84\\-7/84 & 23/84\end{pmatrix}$$

Solution, M =$\begin{pmatrix}14/84 & -34/84\\-7/84 & 23/84\end{pmatrix}\begin{bmatrix}91\\35\end{bmatrix} = \begin{bmatrix}1\\2\end{bmatrix}$

B.For Security

The algorithm which is used for security purpose is shown below.

Sender_or_Intermediate_node()

set timer = fixed_interval

Divide the message in to n packets

encoding each packets using RSA Public key cryptography method // for

//security

Repeat until timer expires

for each adjacent node

calculate the velocity of a node from received RSSI value

set new_relay_node = node_with_lowest_RSSI value //reduces network overhead

if distance(node_with_lowest_RSSI) ==radio_range_radius //250meter

then select

new_relay_node =node_with_next_lowest_RSSI // to //avoid packet loss

End Repeat

if <timer Expires>

if no adjacent nodes

then call blind_forward()

send (packet) // send packet to new relay_node until the destination node is not found

Destination_node ()

decode (packet) using RSA Public key cryptography method

receive(packet)

VI. RESULT & OBSERVATION

Here, it is observed that if we improve number of elements in the message i.e. size, then our generated matrix's size also has to be increased. This increases packet size.

Now, if we increase level of transformation, the reliability improves. But this increases number of computations and computation complexity at the source and destination nodes.

By increasing the encoding set size, the delay also increases. The result is shown in Fig. 5.

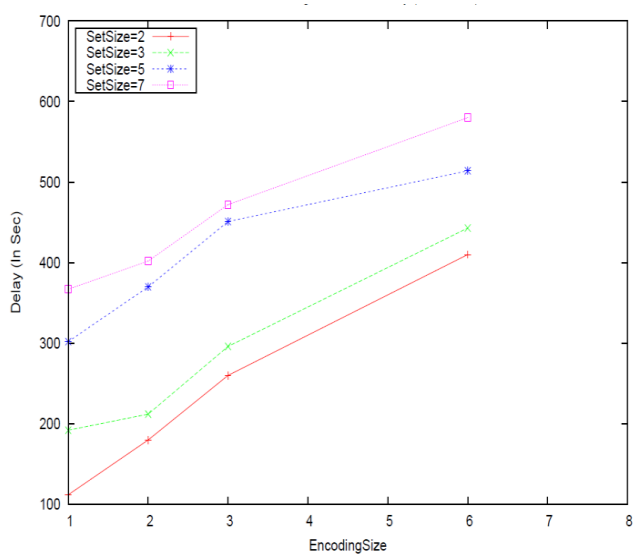

Fig. 5 Plot of Encoding set size Vs Delay

The above plot is drawn for different set sizes.

The comparison of VANET & AODV protocols in terms of number of nodes Vs delay is shown in Fig. 6.

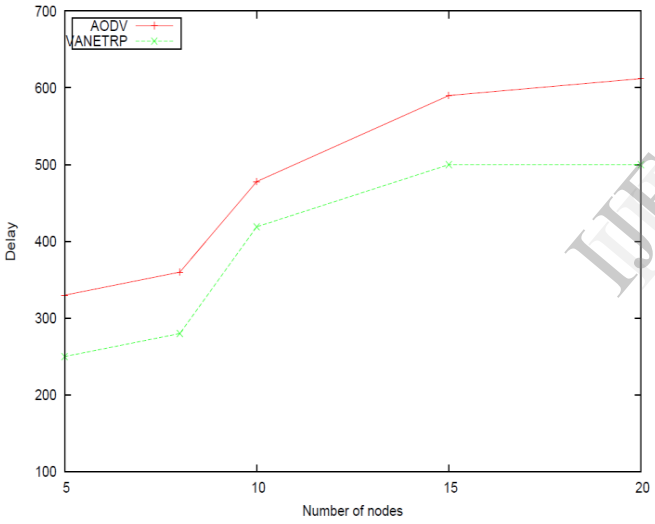

Fig. 6 Plot of no. of nodes versus delay

The plot shows that for the same number of nodes, packet delay is less for VANET protocol compared to that of AODV protocol.

VII. CONCLUSION

VANET is an Emerging Area in which prime focus is on Reliability which cannot be achieved through AODV protocol. AODV protocol which is used in MANET for improving reliability is not affective for VANET.It is improved through Random Linear Network Coding (RLNC) approach. RSA algorithm is used for secure data transmission. RSA algorithm technique provides better security in VANET.

VIII. REFERENCES

[1] SUN Xi, LI Xia-miao, "Study of the feasibilityof VANET and its routing protocols", IEEE2008.

[2] The Network Simulator - ns-2,www.isi.edu/ns nam/ns.

[3] Mingliu Zhang and Richard S. Wolff, "RoutingProtocols for Vehicular Ad Hoc Networks in RuralAreas", IEEE Communications Magazine,November 2008, pp. 126-131

[4] Jeremy Blum and Azim Eskandarian. The threat ofintelligent collisions. IT Professional, 6(1):24–29, Jan.-Feb. 2004.

[5] Sastry Duri, Marco Gruteser, Xuan Liu, PaulMoskowitz, Ronald Perez, Moninder Singh, andJung-Mu Tang. Framework for security and privacy in automotive telematics. In Proceedings of the 2nd international workshop on Mobile commerce, pages25–32. ACMPress, 2002.

[6] Wilfried Enkelmann. FleetNet - applications forinter-vehicle communication. In IEEE IntelligentVehicles Symposium, pages 162–167, June 2003.

[7] Lutz Gollan and Christoph Meinel. Digital signaturesfor automobiles. In Systemics, Cybernetics and Informatics (SCI), 2002.

[8] Marc Torrent-Moreno, Daniel Jiang, and HannesHartenstein. Broadcast reception rates and effects ofpriority access in 802.11-based vehicular ad-hocnetworks. In VANET '04: Proceedings of the firstACM workshop on Vehicular ad hoc networks, pages 10–18 ACM Press, 2004.

[9] Magda El Zarki, Sharad Mehrotra, Gene Tsudik, andNalini Venkatasubramanian. Security issues in afuture vehicular network. In European Wireless, 2002.

[10] Yi Qian, and Nader Moayeri, "Design Secure and Application-Oriented VANETs", Proceedings of IEEE*VTC'2008-Spring*, Singapore, May 11-14, 2008.

[11] Maxim Raya, Panos Papadimitratos, and Jean-PierreHubaux, "Securing Vehicular Communications",IEEE Wireless Communications, October 2006.

[12] Maxim Raya, and Jean-Pierre Hubaux, "Securingvehicular ad hoc networks", Journal of ComputerSecurity, Vol.15, No.1, pp.39-68, 2007.

[13] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, andXuemin Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications",IEEE Transactions on Vehicular Technology, Vol.56,No.6, pp.3442-3456, November 2007.

[14] RAMS consultans "On the Reliability of Safety Applications in VANETs" International Journal of Performability Engineering

[15]Dalip Kamboj, Pankaj Kumar Sehgal "Performance Evaluation of Secure Routing in Ad-hoc Network Environment " , 1st Int'l Conf. on Recent Advances in Information Technology ,RAIT-2012

[16] "Dr Clifford Cocks CB".Bristol Univercity.Retrieved 2011