© 2014 IJEDR | Volume 2, Issue 4 | ISSN: 2321-9939

# A Literature survey on Homomorphic based secure content distribution in VANET

Jigar R Amin[1], Krunal J. Panchal[2]
[1]Department of Computer Engineering, LJIET, Gujarat, India
[2]Asst.Professor, PG Department, LJIET, Gujarat, India

***Abstract* - Vehicular Ad-Hoc Network (VANET) commonly known as an Ad-Hoc on wheels, is a subclass of Mobile Ad-Hoc Network (MANET). Absence of fix infrastructure makes this network more dynamic and suitable for vehicular nodes. Vehicular communication is enabled by Ob-Board Unit (OBU) installed on each and every node. Security is a primary issue of life critical information flow in the network. Security can be achieved by making the data packet more complex to understand using conventional as well as new approaches of cryptography. By providing flexible security mechanism we can improve performance of the system.**

***Keywords* - Vehicular ad-hoc Network (VANET), security, Homomorphic encryption**

## I. INTRODUCTION

VANET [7], [8] is such type of emerging network which brings revolution in the field of wireless communication. VANETs are specialized type of Mobile ad-hoc networks (MANET). VANETs are developed to facilitate human safety, vehicular safety and other commercial applications. Vehicular nodes of VANETs are the mobile nodes communicating with each other and with nearby roadside unit (RSU). For vehicular communication the Federal Communication Commission (FCC) established Dedicated Short Range Communications (DSRC) in 2003. Communication service DSRC uses 5.850-5.925 GHz band for the safety and private applications [10].

Nowadays, road traffic activities are one of the most essential daily routines worldwide[9]. Passenger and goods transport are crucial for human development. Thus, new improvements in this area are achieved day by day for better safety mechanisms, greener fuels, etc. Driving is required factor of traffic safety, so there is an unambiguous need to make it safer[9].

VANET is network of vehicles which are mobile nodes to the network and pretending as “computer on wheels”. VANET communication gives birth to two specifications which are vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) also called vehicle-to-road side unit (RSU). Vehicular nodes can communicate with other nodes directly forming one-hope communication as vehicle-to-vehicle (V2V) or communicate with fixed infrastructure nearby known as road side unit forming vehicle-to-infrastructure (V2I) communication.

VANET node must be equipped with some radio interface or On Board Unit (OBU) that enables short-range ad-hoc network to be formed. Characteristics like high mobility, distributed communication, dynamic load, larger span area, unreliable channel conditions makes VANET differ from other ad-hoc networks.

## II. VANET ARCHITECTURE AND BACKGROUND THEORY

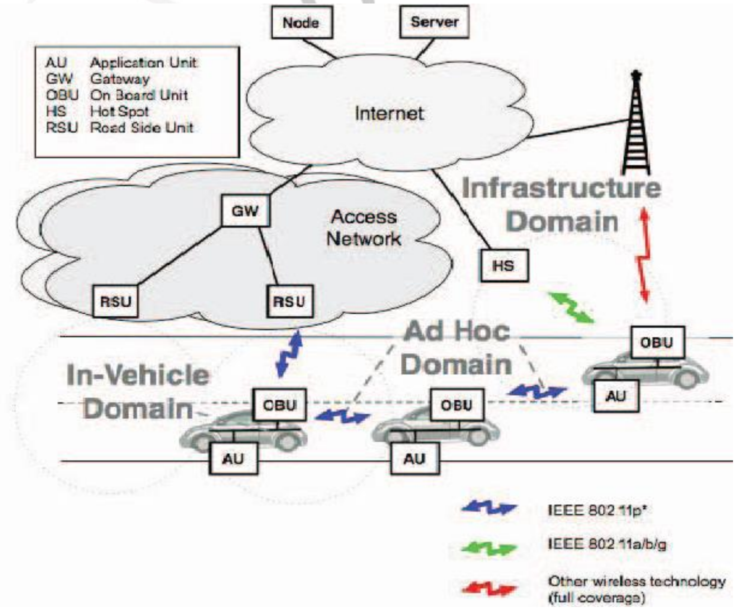

Figure 1: Architecture of VANET[2]

Vehicular nodes of VANET are equipped with wireless communication devices as On Board Unit (OBU). While moving on the road, vehicular node exchanges information with another vehicles and road side unit in their radio range. So there are two types of communications in VANET: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. V2I can provide real-time information on road traffic conditions, weather, and basic Internet service via communication with backbone networks as shown in architecture. In V2Vcommunication environments, vehicles are wirelessly connected using multi-hop communication without access to any fixed infrastructure [1].

### *VANET Background Theory*

The Federal Communication Commission (FCC) allocated a specific frequency spectrum for wireless communication vehicle-vehicle and vehicle-roadside. In 2003, Dedicated Short Range Communications (DSRC) Service is established by FCC. DSRC is a communication service that uses the 5.850-5.925 GHz band for the use of public safety and private applications[2]. Newly developed services and the allocated frequency enable vehicles and roadside units to form Vehicular Ad Hoc Networks (VANETs), in which the nodes can communicate wirelessly with each other without central access point[2].

In US, FCC allocated DSRC spectrum to “increase traveler safety, reduce fuel consumption and pollution, and continue to advance the nation's economy[2]”. The Car 2 Car Communications Consortium developed the C2C-CC project[2] in Europe. The Internet ITS (Intelligent Transportation Systems) Consortium in Japan is one of the samples of VANETs projects.

## III. LITERATURE SURVEY

### 1. Requirements for achieving security[3]

**Authentication:** Authentication is required for sender’s messages; so that response of the vehicles to roads events will be based on messages from legitimate senders.
**Consistency:** In addition to authentication, consistency of the data must be required for the latest data. It may happen that the sender is found to be authenticated but the data are sent to be false.
**Availability:** It is necessary to have alternative forms of communication even in the presence of strong communication channels, for denial of service attacks (DoS) attacks in some cases can create serious problems in the operation of the network.
**Identification:** In case of accidents, must be identify the drivers of the vehicles in order to study the flow of data elapsed between vehicles and neighbor vehicles in times prior to the accident.
**Privacy:** The privacy of vehicles should be ensured as much as possible. It should be avoid the unauthorized control of users to the tracking the vehicle movements.
**Real-time constraints**: Due to the high mobility of vehicles in the network, one needs the ability to react in real time to various events.
**Verification of the positions:** It is a necessary to verify the data received from the GPS through their neighbor nodes, to avoid the attacks on GPS coordinates.

### 2. Identity-Based Security systems[4]

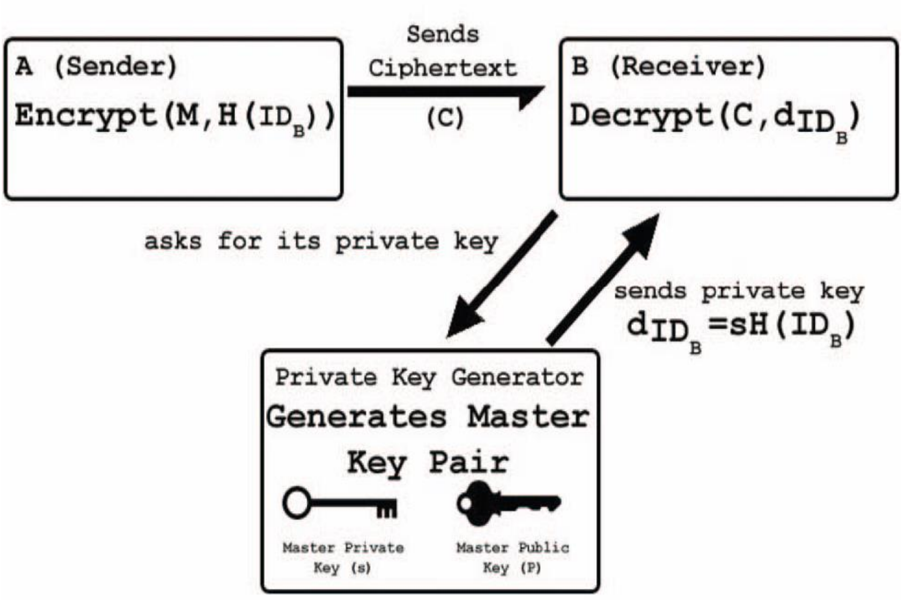

Figure 2. Identity Based Encryption Scheme [4]

Encryption using identity based cryptography worksas in figure 2 Node A wants to send an encrypted message to node B. In order to encrypt the message M, instead of asking for B’s public key it uses the (publicly known) identifier of B. H is a hash function, which is known by each node in the system and used for creating public keys of equal length and same form from the id strings. Note that A performs the encryption even if B doesn’t have its private key yet. After receiving the ciphertext C, B can use its private key to decryptthe message if it already has its private key. Otherwise, B asks to the private key generator for its private key. Private Key Generator generates the private key dIDB for node B using hashed value of B’s identity string H(IDB) and the master private key s.

The author propose distributed generation of private keys. In this approach there are several regional private key generators generate a small part of private keys for any entity. Distribyted generators generates and knows only those part of the key they have generates, in this way private key is more secure in this approach.

### 3. Security Framework For Low Latency Applications [5]

This framework utilizes both traditional cryptographic schemes; asymmetric PKI and symmetric respectively[5]. The asymmetric cryptography scheme is used to securely exchange the key and authentication process and symmetric cryptography scheme is used for low latency safety application (especially time critical safety applications)[5].

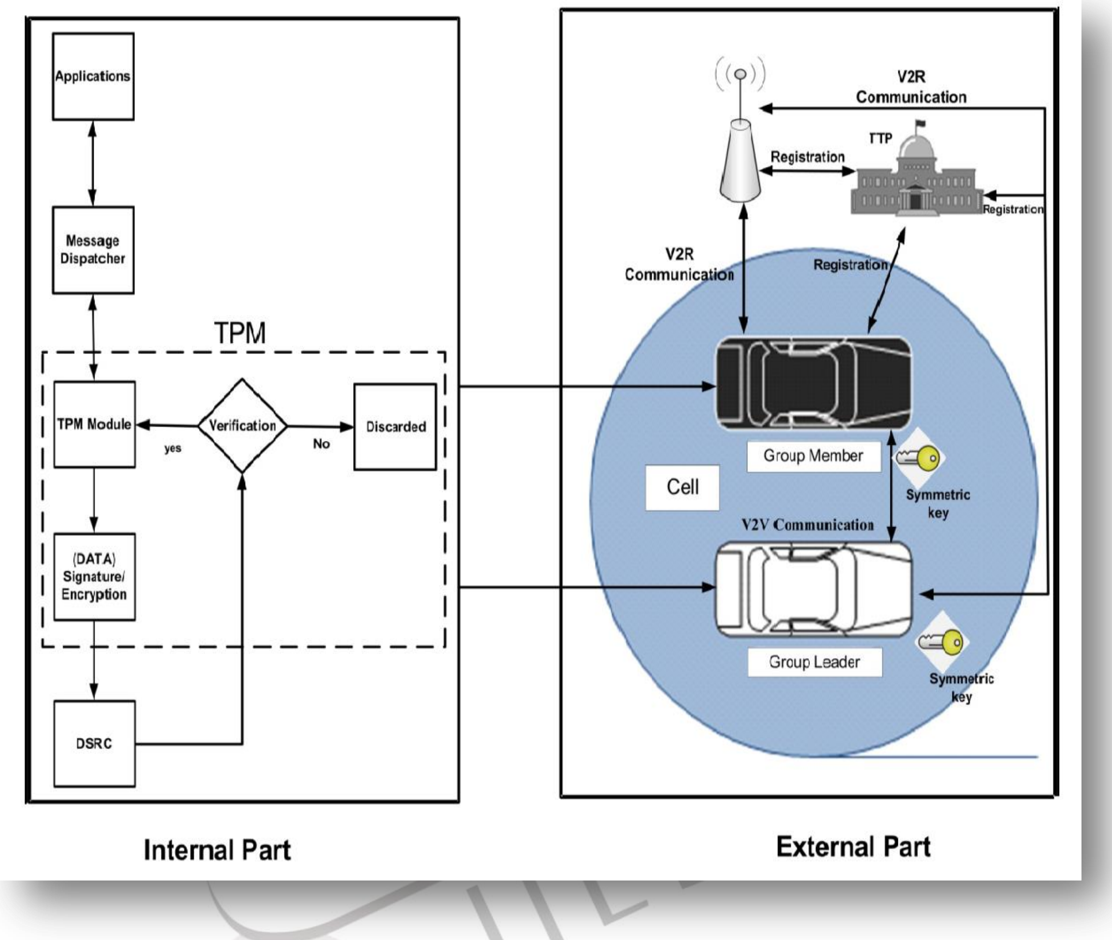

Figure 3. The VANET security framework [5]

There are mainly three types of messages; one at the time when any new vehicle enters in the cell to join the group. At that time, (APPData||PCR||SML||CertPs||KeyECDSA) is the message format, where APPData is applications data, which is around 180 bytes [6], PCR and SML,these are hash values which are called message digest. These message digest values are required to authenticate a platform components states. CertPs is a TTP certificate for user authentication and there is one key, denoted as KeyECDSA for digital signature. The second type of message is used when the symmetric key is shared; the message format = (SK||CertPs||KeyECDH,)[6]. SK is symmetric key that is sent to newly arrived vehicular node after the authentication process. The third type of message is used for safety message broadcasts, and its message format is (APPDATA||SK)[5].

Using this framework as a working model author successed to lower the comuptational cost for low latency application data. Using Two Rey Ground(TRG) as a propagation model, this framework achieves packet data ratio(PDR) about 86% approximately. The AES takes 53.4 ms (0.053 s) in receiving and in verifying 50 messages respectively[5].

### 4. Network coding & Homomorphic Encryption based security model [6]

Content distribution in vehicular networks, such as software updates and multimedia file sharing, poses a great challenge due to network dynamics and high-speed mobility [6]. Network coding has been shown to efficiently support distribution of content In such dynamic environment, Network coding has been shown to efficiently support distribution of content.

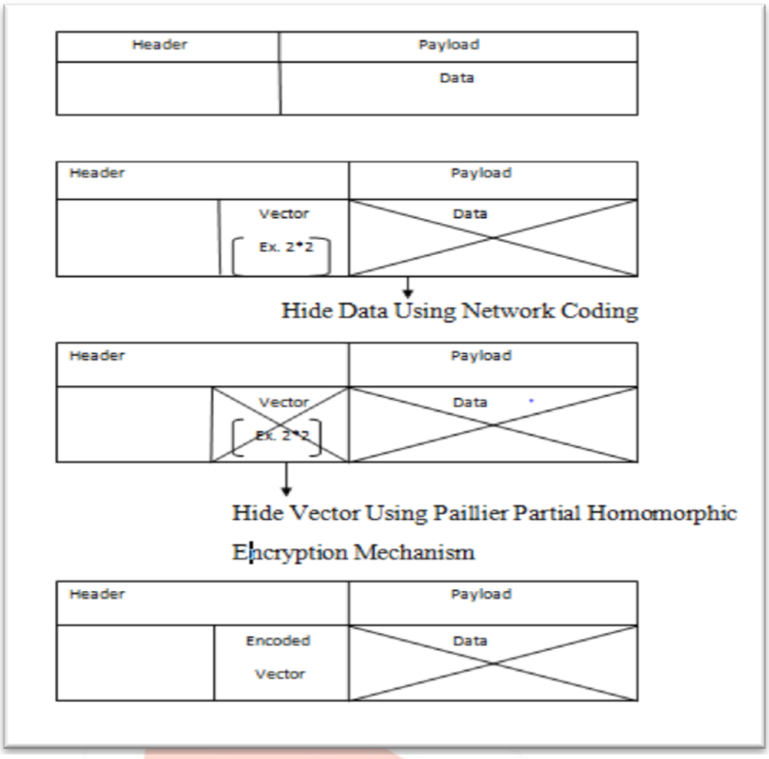

Figure 3. Packet structure[6]

This model is based on partial homomorphic cryptosystem method to hide co-efficient vector generated using random linear network coding [6]. In this work the authors propose packet structure that hides the data by network coding in the payload section and vectors generated by network coding will be added securely to the header section encrypted with traditional homomorphic cryptosystems.

## IV. Conclusion

This present survey illustrates various methods and techniques for making VANETs more secure. First of all we focus on security requirements required in VANET prior to the security mechanism to be used. VANETS are becoming more complex due to their rapid growth across the globe. Due to the growth this network must be made more flexible, reliable and secure. As far as security concerns, flexible security mechanism for secure information flow is required for better performance and reduction in cost.

## REFERENCES

[1] Kevin C. Lee, UCLA, USA Uichin Lee, UCLA, USA Mario Gerla, " Survey of Routing Protocols in Vehicular Ad Hoc Networks", July 2012

[2] Yue Liu, Jun Bi, Ju Yang. " Research on Vehicular Ad Hoc Networks", IEEE, 2009

[3] Mostofa Kamal Nasir, A.K.M. Kamrul Islam, Mohammad Touhidur Rahman and Mohammad Khaled Sohel. " Taxonomy of security in Vehicular Ad-Hoc Network". International Journal of Scientific and Research Publications ISSN: 2250-3153, Vol. 3, Iss. 3, March-2013.

[4] Gianmarco Baldini, Vincent Mahieu, Igor Nai FovinoJoint Research Centre Alberto Trombetta, Marco Taddeo Università dell'Insubria, Varese, Italy, "Identity-Based Security systems for Vehicular Ad-Hoc Networks", 2013 International Conference on Connected Vehicles and Expo (ICCVE) IEEE 2013.

[5] Asif Ali Wagan1 and Low Tang Jung2 Department Computer and Information Sciences University Technology PETRONAS Seri Iskandar Tronoh,Perak,Malaysia, "SECURITY FRAMEWORK FOR LOW LATENCY VANET APPLICATIONS", IEEE 2014

[6] Binoli Shah1 , Jitendra Bhatia2 Gujarat Technological University, Nirma University India, **"**Security Model based on Network coding & Homomorphic Encryption for Content Distribution in VANET" IJCSC Volume 5 • Number 1 March-Sep 2014.

[7] S. Zeadally, R. Hunt, Y. S. Chen , A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenge," *Telecommunication System*, Volume 50, Issue 4, pp. 217-241, August 2010

[8] H. Hartenstein, and K. P. Laberteaux, "A Tutorial Survey on Vehicular Ad Hoc Networks," *IEEE Communications Magazine*, pp. 164-171, Jun 2008

[9] Ankit kumar and Madhvi sinha, " Overview on Vehicular Ad Hoc Network and its Security Issues", International Conference on Computing for Sustainable Global Development, IEEE2014

[10] The FCC DSRC (Dedicated Short Range Communications) web site. http://wireless.fcc.gov/services/its/dsrc/.