iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** V **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review of Secure Routing Over VANET

Harpreet Kaur
Student M.Tech (IT), Department of Computer Science, Lovely Professional University, Phagwara, India

Abstract- Vehicular Ad-hoc network is a special class of wireless ad hoc network which utilizes the cellular and wireless LAN for data exchange at very high velocity. VANET topology mainly suffers from number of concrete obstacles inside the roads and wireless links disconnection due to the velocity. VANET is a scalable network and it covers large volume of area. Data delivery over VANET is insecure due to lake of trust model which can authenticate received/sent data over VANET. It is also necessary to track the authenticated vehicle and the data transmitted by that vehicle. In case of large network, it is not possible to use the traditional security schemes to secure the data transmission over VANET and it is not feasible to maintain the keys at large scale for each vehicle. So there is need to develop a secure routing scheme for vehicle which can easily identify the vehicles and can authenticate the data deliver by them. This survey will explore the requirements of the authentication during data delivery and as well as they way to authenticate the vehicles involved in communication.

Keywords- Multicast Ad hoc Networks, Multicast Routing, Wireless, Qos, MANETs

I. INTRODUCTION

Vehicular Ad-hoc network uses wireless links to communicate with the vehicles using infrastructure network. They can establish a long distance connection using roadside units. Vehicles move at high speed and their mobility pattern is uncertain, and depends upon the road/traffic conditions and road map etc. In case of VANET, we use Vehicles as nodes which can establish a network for information exchange. VANETs support different type of communication; it may be either Unicast or Multicast. Communication based on Unicast approach can deliver the message from a sender to a specific receiver but in case of Multicast approach, group communication is possible. A sender can send a message to the multiple receivers. Communication over VANET suffers from the following factors: [16]

Velocity
Different Mobility Patterns of Sender and Receivers
Traffic Conditions
Obstacles i.e. building signal jammers, traffic lights etc
Frequency compatibility issues [16]

A. Communication over the VANETS Can Be Classified Into the Following Categories

1) Vehicle To Vehicle Based Communication: In this method, Vehicles can directly initiate the communication using wireless links.[9] without depending upon the RSUs. Micro waves can be used to establish wireless channel between vehicles.

2) Vehicle to Infrastructure Based Communication: In this, Vehicles communicate using road side units/ hotspots/base station etc. [9] at the frequency of 5.9GZ. RSUs can be used for identification of Vehicles.

3) Hybrid Approach Utilizes Above Both Techniques: We can also combine the features of V2V and V2I approach to make the better use of resources [9].

B. Characteristics of VANET

Scalable Networks, Shared Channel, Less error prone links, Centralized Infrastructure, Sufficient Resources [10]

C. Application Area for VANET

Assistance for Drivers
Broadcast of traffic conditions
Medical Emergency and rescue operations
Education/Training and Simulation [10]

D. Behavior of VANET'S Routing Protocols

As per the communication method used by protocols, they can be divided in to the following categories:

©IJRASET 2015: All Rights are Reserved

1) Broadcasting: In this category, protocol communicates though broadcast method and introduces data and control packets in large amount thus results in extra control overhead and can degrade the performance.
2) Topology: In this category, protocols use routing tables built according to the current topological conditions and these protocols are further subdivide into table driven and on demand classes.
*3) Geographical Routing***:** In this category, protocols deals with the nodes located at distant location. They use their location to forward the packets over network. [10]

E. Security Constraints for VANET'S Routing Protocols
Routing protocol suffers from the following issues:
Vehicle Identification
Key Generation and Distribution
Key Management
High Velocity [10]

F. Authentication Issues for VANET
*1) Vehicle Authentication***:** It is necessary to authentication the vehicles involved in communication, verification of the received data over the network and signature of the vehicle etc.[1]
*2) Data Exchange Authentication***:** Any vehicle can exchange the data over network by hiding his actual identity, transmitted data should be verified by the trusted routing method.[1]

H. Security Attacks for VANET
We will discuss some common attacks over VANETs which are as follows:
1) Denial of Service Attack: interrupts the normal behavior of the network and try to isolate the network resources from its user, finally results in unavailability of the service. As shown in figure: D is intruder that intruded the Denial of service Attack for the vehicles a, b and c and finally these vehicles cannot communication with base station. It can be distributed and can be introduce in VANET from different location [1].
2) Black Hole Attack over VANET: In this type of attack, intruder drops all the ongoing packets and tries to bring down the network traffic. Intruder can also change the routing information in such a way that all nodes forward the packets using intruder's modified routing information thus results in large amount of packet drop over network.[1]
3) Access Control Hijacking: VANET use centralized monitoring authority which can define the resource access rules for each vehicle that wants to communicate over network. Intruder can alter the access right matrix and can get control over the entire network.[1] .
4) Data Integrity: In VANET, it is more complex to maintain the data integrity because transmitted data can be intercepted by Intruder and he can easily alter the data quickly in network database.

II. LITERATURE REVIEW

Before the selection of "Network Security" as my broad area of dissertation, I have studied many research papers, base papers, books and manuals. These papers helped me to find a particular problem area where I can start my work for thesis. Under the network security I have chosen "Key Distribution" as my sub area. The papers relevant with my problem domain defined below with their purpose of study and year of publication. kumar [1] explored the various issues and security threats that exists for VANET. They discussed about the different attacks which can be launched on the different network resources such as network services, vehicles, communication channel etc. They focused on the identification of the data, its transmission and identification of the vehicles. They also discussed the various algorithms those can be used to authenticate the data integrity and authentication. discussed the various issues and the security threats related to VANET. They
reviewed the different attacks and the prevention techniques which can be used to authenticate the data integrity and authentication.
Chim et al.[2] presented a method for VANET to assist drivers using online data in distributed environment. It can calculate and authenticate road side information. It can hide the actual identity of the users in order to maintain the confidentiality. Proposed method is suitable for path finding which is done through centralized server, that is responsible for data collection and verification from Road Side Units. The verification is done using signatures by server. It does not support the scalable VANETs and ca not be

©IJRASET 2015: All Rights are Reserved

implemented in large cities. Simulation results show its efficiency on the basis of parameters such as delay and time. developed a method for driver's guidance which can hide the identity of the users. It is suitable for path finding, data collection and verification from Road Side Units using signatures offered by the server. There is no support for scalability. Simulation results show its efficiency on the basis of parameters such as delay and time.

Ravi et al. [3] developed a scheme that offers secure and authenticated routes, called Elliptic Curve Digital Signature Algorithm (ECDSA). It uses elliptic curve algorithm with AODV protocol and results show that it can perform well by maintaining delay and packet delivery etc. Proposed scheme can be extended to provide the support for large cities. developed a scheme for route security and authentication called the Elliptic Curve Digital Signature Algorithm (ECDSA). It uses the elliptic curve algorithm with AODV protocol. Simulation results show its performance in terms of delay and packet delivery. The proposed scheme can be extended to provide the support for large cities.

Hou et al. [4] proposed a secure routing protocol which can identify the modified routes by the intruders, packet loss due to the altered routes etc. It uses signatures for end point packet delivery and the next hop to identify packet drop. It puts overhead on delay while maintaining confidentiality, throughput and packet loss ratio in the presence of intruders. Proposed scheme can be used to identify the modified routes by the intruders. It uses signatures for end point packet delivery and the next hop to identify packet drop. The performance issues related to the proposed protocol are overhead and delay.

Kumar et al. [5] Introduced a concept of Intelligent Transport Systems (ITS) for VANETs using AODV routing protocol. It provides security and trusted information exchange by finding the efficient paths on the basis of authentication and the presence of intruder can be ignored. Simulation results show its performance in terms of packet drop ratio and throughput. presented a Intelligent Transport Systems (ITS) for VANETs that uses AODV routing protocol. It provides security and trusted information exchange by finding the authenticated paths. Simulation results show its performance in terms of packet drop ratio and throughput.

Taha et al. [6] developed a key based authentication method without using certificates, called CL-AKA for security of the hotspots. On the basis of mutual authentication, it produces a common key between sender and receiver. Simulation results show that it is energy efficient, puts less overhead on network performance and capable to provide secure environment for communication over VANETs.] offered a key based authentication method that does not use certificates, called CL-AKA for security of the hotspots. Mutual authentication produces a common key for sender and receiver. Simulation results show that it is energy efficient and there is less overhead.

Chen [7] et al. proposed a protocol to secure the information exchange using ambulance over VANET. Vehicles as ambulance, require an optimal path to its destination which cannot be computed using shortest path problem. It can select the path on the basis of event and its position. To maintain the confidentiality of the selected optimal path, they used cryptography algorithms along with the digital signatures. Simulation results show that it can perform well by managing the delay, processing interval and number of hopes etc.

Pooja. B [8] et al. developed a solution base on public key infrastructure which can work in the presence of Denial of services threat using signature identification. It can deal with the inside and outside intruders also. It identifies the fake packets by verifying their signatures. Signatures are calculated on the basis of key pairs assigned to the users and key pairs are distributed using public key infrastructure. Results show that there is no overhead on the performance of the network and its strength against threat.

Mikki et al. [9] presented a protocol for secure communication over the VANET, called privacy preserving secure communication protocol (PPSCP). It is used for message authentication. It can maintain the level of confidentiality by isolating the user identity and suitable for Dos attack detection and prevention. Its performance is evaluated using different parameters such as delay, throughput, packet delivery ratio as compared to S3P. It provides confidentiality by isolating the user identity and offers Dos attack detection and prevention. Its performance is evaluated using different parameters i.e. delay, throughput, packet delivery ratio etc.

III. PROBLEM FORMULATION

The major issues in VANET are message authentication, information exchange, user identification, authorization, key distribution, key management, secure routing, detection and prevention of the security threats. The issues are due to the scalable property of the VANET. The topology of VANET can be changed at any time and distributed keys may be no longer required. So the obsolete keys should be replaced by another key. The problem is that identification of the existing users should be known to distribute the new key. Authors did a survey and observed that confidentiality [1] is major concern for VANETs due to open access to wireless channel. There are various security threats exists for VANETs such as Denial of Service, Black hole, violation of data integrity and access control constraint, intrusion etc. They examined some approaches which can be used to protect network i.e. digital signatures,

©IJRASET 2015: All Rights are Reserved

SHA-1, AES, HASH function etc. Authors just provided a theoretical study about the security threats and their remedies but did not produce any practical results. Authors [2] proposed a authentication method which utilizes the services of centralized authority and due to dependency over infrastructure, it is not suitable for large networks. Authors [3] developed a framework for message integrity and authentication and it measured its impact over delay and packet delivery ratio but did not discuss about throughput, packet loss and routing load etc. Authors [4] developed a secure location based routing protocol that offers optimize authentication services for message delivery on the cost of delay. Authors [5] a solution using AODV for secure and reliable routing over VANET. They just evaluated its performance against throughput and packet drop but did not consider the delay and packet delivery ratio etc. Authors [6] developed a solution using power aware public key cryptography to secure hotspots. They just focused on energy consumption parameter but did evaluate the performance of proposed method in terms of delay, packet delivery ratio and throughput etc. which are necessary parameters to measure the performance. Authors [7] proposed a infrastructure based solution for various common threats and considered delay and various security goals as its achievement but did not evaluated its performance using parameters like packet delivery ratio and throughput etc. In this survey, authors did not explore the number of ways through which key can be distributed for message authentication. Some of them used infrastructure based distribution which does not support property of scalability. Dependency on infrastructure may result in terms of performance, delay, power consumption etc

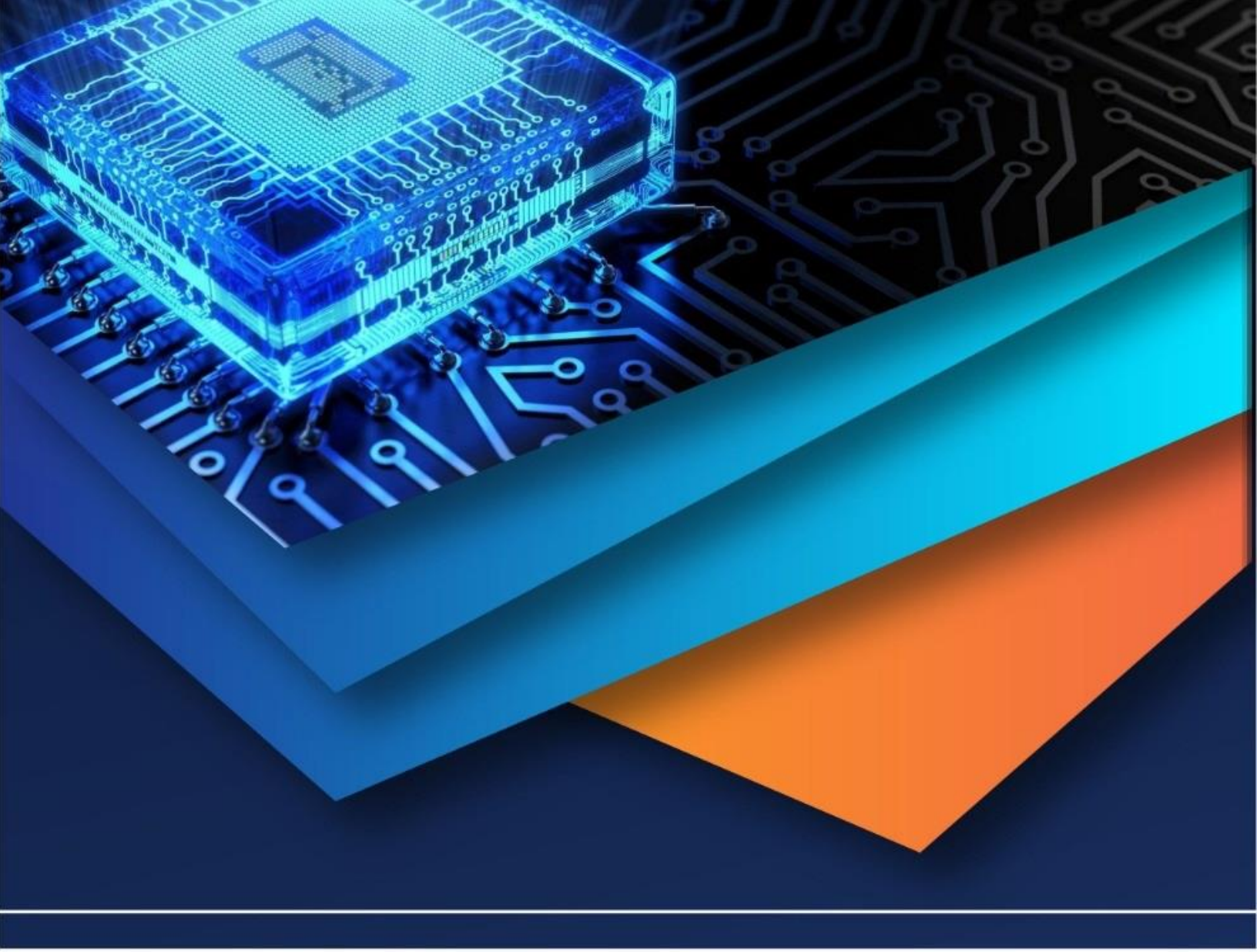
IV. CONCLUSION

To developed a routing protocol for secure data exchange using ambulance over VANET.
Vehicles as ambulance adopt optimal path to its destination on the basis of event and its position. To maintain the confidentiality of the selected optimal path, they used cryptography algorithms along with the digital signatures. Simulation results show that it can perform well by managing the delay , processing interval and number of hopes etc Authors did not calculate the cost of the security in terms of routing load, delay, resource consumption, throughput, packet delivery ratio etc. which may be increased due to the extra control over head caused by security implementation. So there is need to consider this factor also.

REFERENCES

[1] Ankit kumar, Madhavi Sinha“Overview on Vehicular Ad Hoc Network and its Security issues”, IEEE-2014, pp 792-797
[2] T.W. Chim, S.M. Yiu, Lucas C.K. Hui,"VSPN: VANET-Based Secure and Privacy- Preserving Navigation",IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014, pp 510-524
[3] Kalkundri Ravi, Kalkundri Praveen,"AODV Routing in VANET for Message Authentication Using ECDSA", International Conference on Communication and Signal Processing,2014, pp 1389-1393
[4] Jie Hou, Lei Han, "Secure and Efficient Protocol for Position-based Routing in VANETs", IEEE-2012, pp 142-148
[5] N.Arulkumar, Dr. E. George Dharma Prakash Raj, "A Simulation Based Study to implement Intelligent Transport Systems concepts in VANETs using AODV Routing Protocol in NS2", ICoAC 2012, IEEE
[6] Sanaa Taha, and Xuemin Sherman Shen, "A Link-layer Authentication and Key Agreement Scheme for Mobile Public Hotspots in NEMO based VANET", Globecom-2012, IEEE, pp 1004-1009
[7] Chin-Ling Chen,Ing-Chau Chang, "A Secure Ambulance Communication Protocol for VANET", Wireless Pers Commun-2013 Springer, pp 1187-1213
[8] Pooja. B, Manohara Pai M.M, Radhika M Pai1, Nabil Ajam, Joseph Mouzna, "Migatiion of Insider and Outsider Dos Atatck against Signature Based Authentication in VANET", APCASE-2014, IEEE-152-15719
[9] Mohammad Mikki, Yousif M. Mansour, "Privacy Preserving Secure Communication Protocol for Vehicular Ad Hoc Networks", IEEE-2013, pp 188-195
[10] Ajit Singh, Mukesh Kumar, Rahul Rishi, and D.K. Madan, "A Relative Study of MANET and VANET: Its
Applications, Broadcasting Approaches and Challenging Issues", CCSIT 2011, Springer, pp. 627–632
[11] Nayak, A., Stojmenovic, "Cyptographic Algorithms", Wiley-IEEE Press-2008, PP 373 – 406
[12] M. Tolga SAKALLI, Ercan BULU$ and Fatma BUYUKSARACOGLU, "Cryptography Education for Students", IEEE-2004, pp 621-626
[13] Phan, R.C.-W. ; Inf. Security Res. Lab., Swinburne Univ. of Technol., Kuching ; Siddiqi, M.U., " A Framework for Describing Block Cipher Cryptanalysis ", computers, IEEE Transactions, Vol.55 (11) , pp 1402 – 1409
[14]C. Paar, J. Pelzl,"Understanding Cryptography", Springer-Verlag Berlin Heidelberg 2010, pp 29-54
[15]Chuanhua Zhou ; Baohua Zhao ; Gemei Zhu ; Wei Wei, "Study of One-way Hash Function to Digital Signature Technology", Computational Intelligence and Security, 2006 Vol.2, pp 1503 – 1506
[16] James Bernsen, D. Manivannan, "Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification", Pervasive and Mobile Computing, Elsevier-2008, pp 1-18

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)