International Journal of Engineering & Scientific Research
Vol.4 Issue 10, October 2016,
ISSN: 2347-6532 Impact Factor: 5.900
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

SUITABLE PATH SELECTION AND SECURITY MECHANISM IN VANETS

Sushant Sharma*

Shakti Arora*

Er. Sunil Panjeta(Research Supervisor)*

Abstract: Vehicular ad-hoc networks (VANET) are self organized network which is a subset of Mobile Ad-hoc network (MANET). It is a wireless ad-hoc network provides communication between vehicles in vehicular environment. VANET is challenging area of research because of its high mobility and frequently changed topology. VANET have its own many challenges such as security, optimal path selection, traffic congestion and securely transmit warning message or any other data from sender to receiver. So In this paper proposed solution designed to overcome these challenges like securely transmit data from sender to receiver by using Pretty Good Privacy (PGP) security and remove the traffic congestion or ignore the unnecessary load of network by selecting dynamic path for data transmission. In this, the hybrid protocol that is Ad-hoc on demand distance vector (AODV) and Ad-hoc On demand multi path distance vector (AOMDV) is used for to select the dynamic path in Vanet. Central authority is provide the certificates to each node and verifies its certification. To measure the performance of network with end to end delay, throughput and packet delivery fraction performance matrices.

Keywords: VANET, Hybrid Protocol, PGP, CA, SECURITY

* Dept of Electronics and Communication Engineering, YIET,Gadholi,Yamuna Nagar Haryana

INTRODUCTION:

VANET is vehicular ad-hoc network type of Mobile ad-hoc network (MANET). It is a wireless ad-hoc network technology which integrates cellular technology, ad-hoc network and wireless LAN to achieve roadside to vehicle (RVC) and intelligent vehicular communication (IVC). Communication in VANET is Inter vehicular communication (V2V) and Road Side to vehicle/ vehicle to road side (R2V/V2R) communication. Now a day, vehicles are rapidly increased day by day in the whole world. In highways and metropolitan cities many number of vehicles moves so the chances of accidents are increased with number of vehicles increased. When sender sends the warning message to destination that there is accident occurred. The main issue in VANET to securely transmit the data like warning message from sender to receiver, removing the traffic congestion and dynamically selection of optimal path for data transmission in vehicular network. Security is the main issue in VANET for delivering data between vehicles. Dedicated Short Range Communication (DSRC) as a range radio used in VANET. Vehicular nodes are communicated with each other by the help of Dedicated Short Range Communication like as Wi-Fi.

VANET have two types of mobile nodes that is ON BOARD UNIT (OBU) which is a type of mobile node and ROAD SIDE UNIT (RSU) which is stationary node. Central Authority (CA) is used for node recognition and provides certification to each node. It also discusses the security requirements of VANET.

1.1 **Overview of Vanet:**

1. ROAD SIDE UNIT: RSU act as a regional authority for their regions. RSU is stationary node mounted in centralized locations such as gas stations and parking lots. It is responsible for communication between CA and vehicles working as router.

2. ON BOARD UNIT: It is a device that is equipped in each vehicle and knows their current location. It contact trust authorities through RSU and send public key. An OBU resembles central processing unit for on-board sensors and warning devices in vehicles. OBU signs a safety message using its private key and then sends the signature, message and its certificate.

3. TAMPER PROOF DEVICE: it is a device that is on board equipment in vehicles which collect data from the interior and exterior of vehicles and deliver it to a central processing unit that can analyze this data to boost the road safety while increasing the on-board luxury. It is

responsible for to store the vehicles private key, secret information and signing outgoing messages. TPD contain set of sensors that erase all the stored keys to prevent them from being compromised. Trusted Platform Module is used in vehicles for secure communication. It is used for storage, computations and provides security.

1.2 Security requirement of VANET:

1. Authentication: In Vehicular Communication each and every vehicles are authenticated. To achieve this requirement every message must be authenticated so vehicles will assign every message with their private key along with its certificate. At the receiver side the receiver will receive the message and check for the key and certificate. Some cryptographic systems are used to achieving authentication.

2. Availability: Vehicular network must be available all the time no route link breakage so a delay in seconds or milliseconds for some applications makes the message meaningless and maybe the result will be devastating.

3. Privacy: Privacy means the information of drivers keeping away from unauthorized observers. So to achieve this using the keys cryptographic model.

4. Integrity: The integrity of messages that means message is send by a sender same at receiver end. It should be protected to prevent attackers from altering the message contents trusted.

5. Confidentiality: Confidentiality means the privacy of each driver against unauthorized observers must be protected. The messages should be encrypted.

2. OVERVIEW OF DYNAMIC PATH SELECTION FOR DATA TRANSMISSION AND PROBLEM FORMULATION

Securely data transmit from sender to receiver is main issue in VANET. Data is altered by many attackers and attack on vehicular nodes. Static path for data transmission is created problem when traffic congestion is occurred so there is no optimal path for data transmission. So avoid this problem optimal path is selected by each node to transmit data. Dynamic path selection

when there is congestion occurred near any node then it will dynamically select the optimal path to transmit data.

2.1 **Related Works:**

[1] Message transmit securely from sender to destination node is big issue in vehicular ad-hoc network because security is the main big issue of vehicular ad-hoc network. In this existing system, chooses the static path for data transmission from sender to receiver. This system use optimal node generation algorithm to choose only the best node for data transmission. So when the traffic congestion is occurred then there is no optimal path for data transmission.

[2] This paper describes that Vehicular Ad hoc Network (VANET) is a vehicular network which is highly dependent upon the security i.e PKI/ECDSA type security mechanism which is asymmetric or symmetric but symmetric provides faster communication by reducing security expense. This security mechanism provides a security framework which is hardware based by using asymmetric PKI and symmetric PKI to exchange message faster and securely. So it improves the security of VANET by using Trusted Platform Module (TPM). This module helps to form a trusted groups by establish the trust relationship between neighboring nodes. Trusted Platform Module is being used in all new PCs and laptop for secure communication because it provides security.

[3] In this paper it discussed some threats and attacks that can be exits on vehicular network and in response present some viable security solutions. This paper provides brief survey of security related issues and existing solutions in the vehicular network environment. It discussed about robust security system in VANET.

[4] This paper defines a new algorithm which is ECDSA. Elliptic Curve Digital Signature Algorithm (ECDSA) provides an efficient message authentication scheme. In this, the combination of P2P, ECDSA and VANET can make the scenario more efficient and perform better in terms of time delay in message delivery. Elliptic Curve Digital Signature Algorithm (ECDSA) signature have to be attached for each message. ECDSA is used to encrypt the message and decrypt the message by authorized user for access the information adding more strength to the Security.

3. PGP SECURITY

Pretty good Privacy (PGP) is a security model that is used for encryption and decryption of data which sends from source to destination. It responsible for securely transmit data from source to destination. It activates with central authority (CA) for providing certificate to each node when it is used in wireless ad-hoc network. It provides security to ad-hoc network and improves the performance of network. It using certificates, digital signature and key issuing can authenticate message, identify valid vehicles or malicious vehicles. PGP is used for to encrypt the message at source node and decrypt the message at destination node after selecting the path. It is asymmetric cryptographic, web of trust model. This model fulfills the security requirements such as authentication, integrity, privacy, confidentiality and Non-repudiation of VANET. It protects the message (or its contents) from being altered or destroyed. CA is used to provide session keys with PGP. PGP algorithm is implemented for security which is faster as well as secure than previously implemented algorithms.

PGP ALGORITHMS:

1. PGP security activated to provide the keys to each node.
2. Source node uses the session key to encrypt the data.
3. Checks the neighbor node is certified or not.
4. If neighbor node is certified/valid then it decrypt the data with same session key.
5. If not then discards that node.

4. HYBRID PROTOCOL (AODV and AOMDV)

Hybrid protocol is the combination of AODV i.e. Ad-Hoc On demand distance vector and AOMDV i.e. Ad-hoc on demand Multi path Distance vector routing Protocol. In this thesis both protocol is combined to make the network performance better. The network performance of this protocol is measured through End to End Delay, Packet Delivery Fraction and Throughput performance metrics. Hybrid protocol used to set the thresh level for finding dynamic path in

vehicular network. This protocol uses the routing table on each node in network. When any node left or enter the range of network then nodes update their routing table. So thresh level is also updated by protocol. The main goal of dynamic is to find all available node-disjoint routes between a source-destination pair with minimum routing overhead. To achieve this goal protocol works in three phases: (i) Route Discovery Phase, (ii) Route Selection Phase and (iii) Route Maintenance Phase.

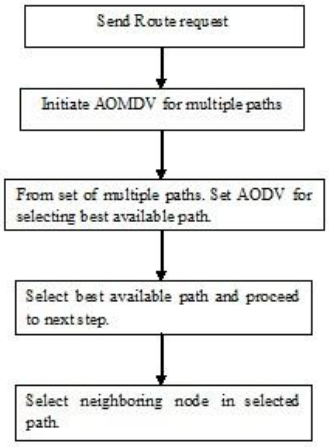


FIGURE 5.1- Hybrid Protocol

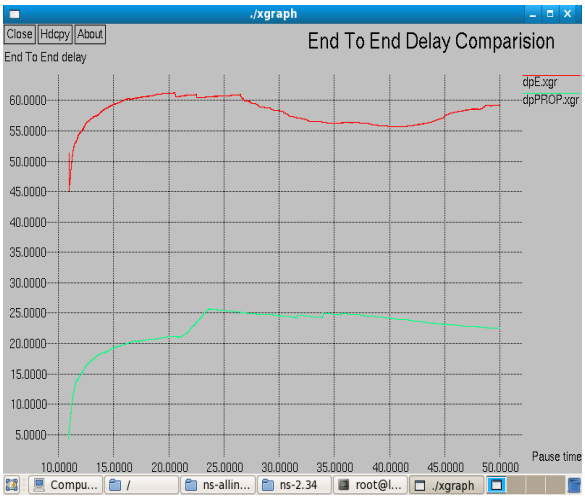
5. PERFORMANCE METRICS

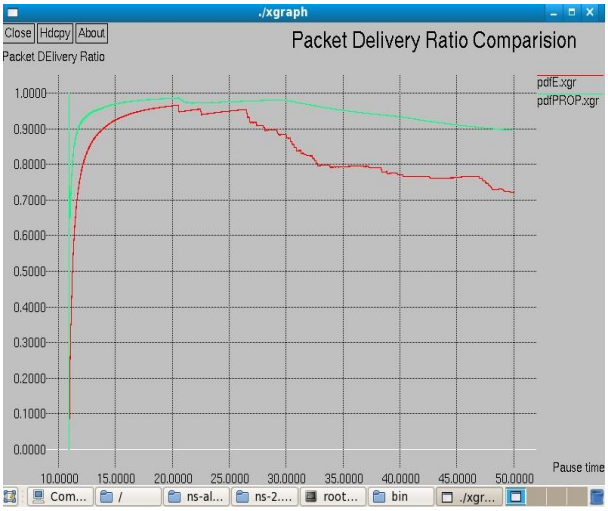
It is used to measure the performance of system.

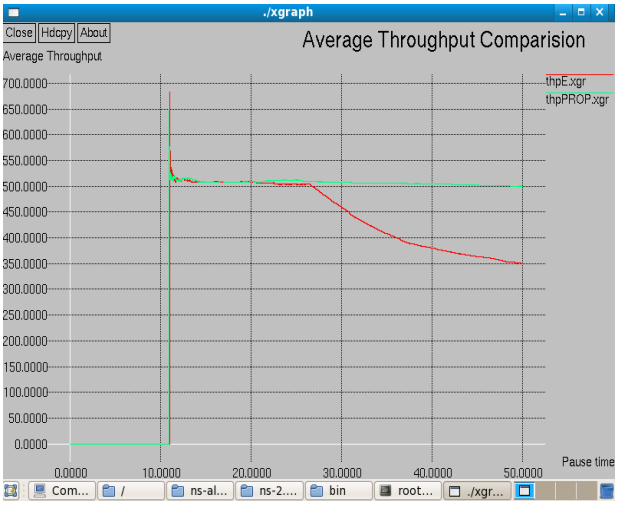
End To End Delay: It measuring by the time taken for a packet to be transmitted from source to destination on network.

Packet Delivery Fraction: it is the fraction of packets that are delivered to destination by comparing with the packets send by source.

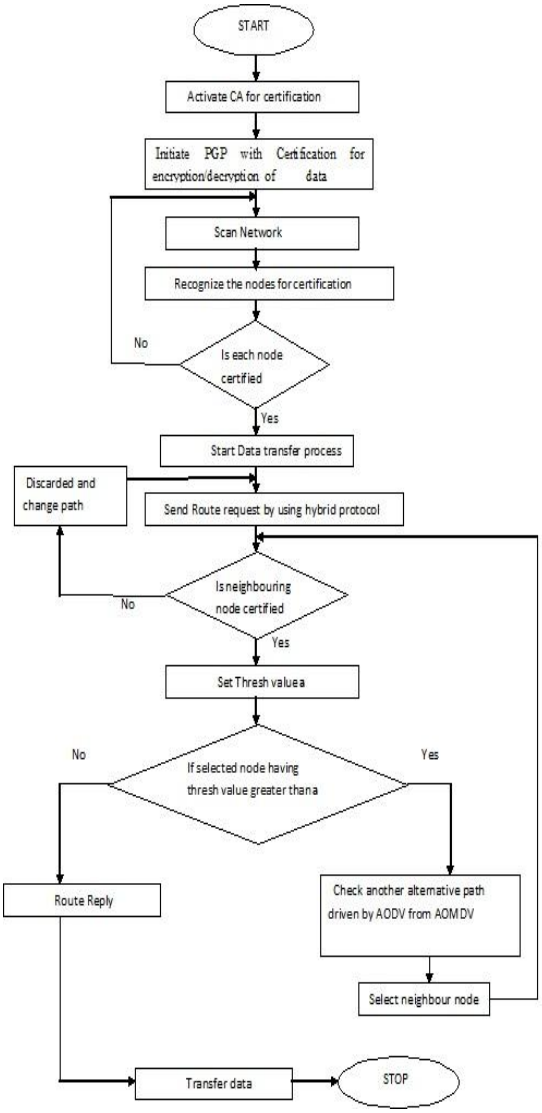
Throughput: It is the ratio of file size over transmission time that is calculated in seconds.


./xgraph
Close
Hdcpy
About
End To End delay
End To End Delay Comparision
dpE.xgr
dpPROP.xgr
60.0000
55.0000
50.0000
45.0000
40.0000
35.0000
30.0000
25.0000
20.0000
15.0000
10.0000
5.0000
10.0000
15.0000
20.0000
25.0000
30.0000
35.0000
40.0000
45.0000
50.0000
Pause time


./xgraph
Close
Hdcpy
About
Packet DElivery Ratio
Packet Delivery Ratio Comparision
pdfE.xgr
pdfPROP.xgr
1.0000
0.9000
0.8000
0.7000
0.6000
0.5000
0.4000
0.3000
0.2000
0.1000
0.0000
10.0000
15.0000
20.0000
25.0000
30.0000
35.0000
40.0000
45.0000
50.0000
Pause time


./xgraph
Close
Hdcpy
About
Average Throughput
Average Throughput Comparision
thpE.xgr
thpPROP.xgr
700.0000
650.0000
600.0000
550.0000
500.0000
450.0000
400.0000
350.0000
300.0000
250.0000
200.0000
150.0000
100.0000
50.0000
0.0000
0.0000
10.0000
20.0000
30.0000
40.0000
50.0000
Pause time

Central Authority is called Key/certificate generator. CA issues key certificate to each node and recognized each node that is valid or not. It also provides application and services to each node. CA responsible for to registered each vehicular node. It defines regions to identify the positions of each node. All of these researchers mentioned the CA to handle all the operations of certificate such as generating, renewing and revoking of certificates. CA must be responsible in initiating keys, storing, managing and broadcasting. An anonymous key pair is a public/private key pair that is authenticated by the CA.



Flow chart of dynamic path selection

5. PROPOSED WORK:

This proposed solution is used to select dynamic path when traffic is occurred in any path then select the alternative path with the help of hybrid protocol. So it overcomes the problem of traffic congestion and saves time. PGP security is used to securely transmit data by encrypting/decrypting. PGP and CA used to provide the session key between source and destination nodes. When source sends the data to certified neighbor node by encrypting it with session key and destination node receives the data by decrypting it with same session key. It protects from unauthorized intruders to alter the data. Each node is verified whether it is certified or not. CA provides the certificates to valid nodes in network and not to malicious nodes. PGP security model is web of trust model so each node is trusted node.

6. CONCLUSION AND FUTURE WORK

This thesis presented a new proposed solution uses the PGP security to securely transmit the data from source to destination by finding the dynamic path so it ignores the unnecessary load on the network and lesser the chances of accidents in network. This proposed solution is useful in traffic congestion to choose the optimal path. This thesis uses the hybrid protocol of AODV and AOMDV to make the performance better of VANET network. With this proposed solution the end-to-end delay is measured to be less in case of with PGP security and hybrid protocol as compared to system without PGP Security. Similarly the average throughput and packet delivery fraction is higher in case of system with PGP and hybrid protocol as compare to system without PGP. PGP security used to make the network secure and fastest of data transmission. Future work may be further adding the load balancing concept making efficient network. In future traffic lights needs to be addressed during the dynamic path creation. Also some multi cast protocol for VANET will be used so that same group of vehicles can be operated simultaneously.

7. PREFERENCES

[1]. Sourav Kumar Bhoi, Pabitra Mohan "A Secure Fault-Tolerant Smart Transportation System For Vehicular Ad hoc Network" Proceedings of 2012 IEEE.

[2]. Wagan, A.A; Mughal, B.M. and Hasbullah, H. "VANET Security Framework for Trusted Grouping Using TPM Hardware" 2012 2nd International Conference on Computer Science and Network Technology,IEEE.

3. Yeongkwun Kim, Injoo Kim "Security Issues In Vehicular Network" IEEE 2013.

[4].Sourav Kumar Bhoi, *Student Member, IEEE,* Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack"2013 International conference on Communication and Signal Processing, 2013.

[5]. Kavitha . M, Shrikant S. Tangade "A Survey on Trust & Trust-Based Schemes In VANET s" 4th ICCCNT – 13 July 4 - 6, 2013, Tiruchengode, India.

[6]. Shrikant S. Tangade, Sunilkumar S. Manvi "A Survey on Attacks, Security and Trust Management Solutions in VANETs" 4th ICCCNT – 2013 July 4 - 6, 2013, Tiruchengode, India

[7].Kalkundri Ravi, Dr. S.A Kulkarni "A Secure Message Authentication Scheme for VANET using ECDSA"Computing, Communications and Networking Technologies,2013 Fourth International Conference IEEE

[8].Smitha.A1,Manohara Pai M.M1,Ajam. N2,Joseph Mouzna2 "An optimized adaptive algorithm for authentication of safety critical messages in VANET" 2013 8th International ICST Conference,IEEE

[9].Harish Laxmichand Sharma, Pankaj Agrawal "Multipath Reliable Range Node Selection Distance Vector Routing for VANET: Design Approach" **(ICESC), 2014 International Conference,IEEE**

[10]. Jing Wu, Yuhao Wang "Performance Study of Multi-Path in VANETs and their Impact on Routing Protocols" Wireless Engineering and Technology, Vol. 2 No. 3, 2011