Channel Quality Adaptive Protocol with Secure Routing in VANET

S. Santha Preethi[1], R. Rajadurai[2]

[1] PG SCHOLAR, [2]ASSISTANT PROFESSOR, , SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE, PUDUCHERRY.

ABSTRACT

Multihop wireless broadcast is an important component in vehicular networks. Moreover applications are built on broadcast communications make efficient routing methods critical for their success. Broadcast protocols tailored to vehicular networking must be adaptive to variation in these factors. In the spatial distribution channel quality adaptive protocol also have the security issues like DOS attack and man in the middle attack. For solving this security issues, security algorithm is proposed to reduce the attacks in the multihop wireless broadcasting. To make the communication secure in the key exchange we implement the Diffie-Hellman algorithm and with the RSA security which makes our spatial distribution secure.

Keywords— statistical broadcast, broadcast storm, VANET, rebroadcasting.

1.INTRODUCTION

Vehicular Ad Hoc Network (VANET) is a Vehicle To Vehicle (Inter-vehicle communication-IVC) and Roadside to Vehicle Communication (RVC) system. The VANET integrates WLAN/cellular and Ad Hoc networks to achieve the continuous connectivity. The ad hoc network is put forth with the novel objectives of providing safety and comfort related services to vehicle users.

Collision warning, traffic congestion alarm, road blockade alarm (due to construction works etc.) and lane-change warning are among the major safety related services are directed by VANET [1]. In the other category of related services are equipped with Internet and Multimedia connectivity.

The major research challenges in the area are present in designing of routing protocol with data sharing includes security and privacy to form network .We aim here to study the efficiency of communication network in VANET on the basis of a predictable mobility model [2].

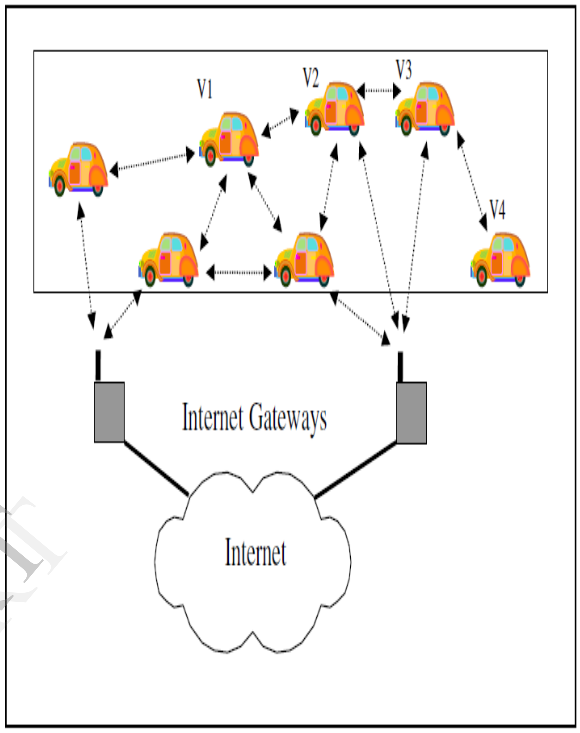

Fig.1: Vehicular Ad hoc Network

The process of algorithm suitable to VANET, as suggested from different routing protocols, largely depends on an authentic mobility model and decision parameters of nodes to forward the packets to other nodes.

Again to set a realistic mobility model, the parameters include street map structure, urban or geographic conditions including obstacles such as buildings and trees need to be properly verified. Basic methodologies applied in the mobility model are explained below.

RWP (Random Way Point): In this, a random destination point and a uniform speed is attributed to each node. When destination point arrives, another random destination point is assumed. RWP is widely used in ad hoc network simulation (example: NS-2) but the model as such is far from a realistic one.

STRAW (Street Random Waypoint): In an attempt to make the above model more realistic, it uses a car-following model with US road information to simulate the realistic traffic situation that includes, traffic controls, traffic congestions, car interactions etc in an urban environment.

In the latest technique of more realistic mobility model building, vehicles are checked frequently by recording their one dimensional position and lane on the highways on every discrete time steps of 0.5 sec. After combining the valid traces [3],a realistic mobility scenario is developed.

The mobility model incorporated trace date obtained from MMTS (Multi-agent Microscopic Traffic Simulator) which is capable of simulating public and private traffic over a real road map in Switzerland with a high degree of realism.

To make an effective VANET application, a realistic mobility model and appropriate routing protocol is desired.

To evaluate the performance of VANET with a routing protocol, we have used VanetMobiSim-1.1 /NS-2 combination of application tool to run it. The result gives a realistic mobility model that supports both micro-mobility or macro-mobility features.

Macro mobility model relates to road topology, road structure such as number of lanes, single way or double-way movement etc, traffic light constraints, speed limits where as micro mobility relates more to driving behaviour. In present study, we have used a mobility model belonging to IDM-LC (Intelligent Driver Model with Lane changes) family.

The output from VANET Mobility simulation is a traffic generator trace file that corresponds to position coordinates of each vehicular node at every time steps. This traffic generated trace file is the mobility model that goes through network simulation (by NS-2 package in present study) and ultimately generates a communication trace file.

2. Proposed System

Security is the main issue in communication. Threshold function is allowed in the proposed DADCQ protocol. The earlier contribution of this work is the proposed multihop broadcast protocol DADCQ. Many applications and protocols are built on this issue for routing and data delivery. In DADCQ protocol mainly focus on the routing issues, for that channel quality adaptive protocol is implemented to solve the routing issues. A key insight proposed here is a methodology for incorporating more information into the protocol[4]. In the spatial distribution channel quality adaptive protocol also have the security issues like DOS attack and man in the middle attack. For solving this security issues, security algorithm is proposed to reduce the attacks in the multihop wireless broadcasting.

2.1 Architecture

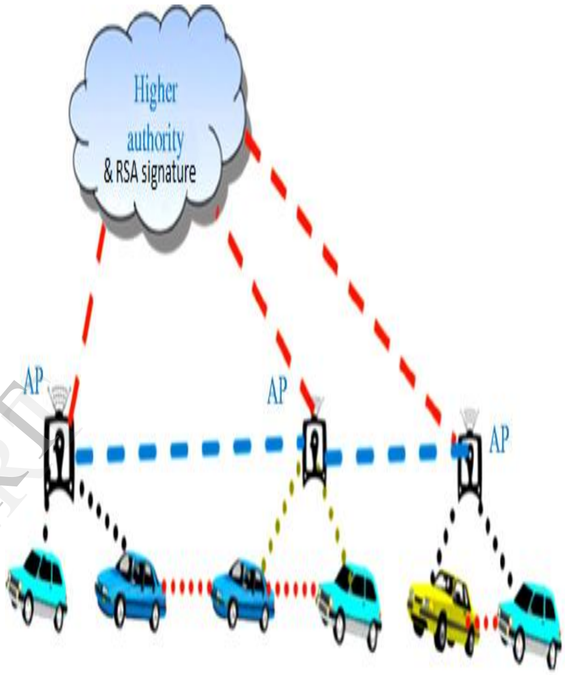

Fig.2: Architecture

2.2 RSA with Digital Signature

A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption. One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data [6]. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

However, encrypting all data to provide a digital signature is impractical for three reasons:

- The ciphertext signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors, so network and computer performance can be significantly degraded.
- Encrypting the entire contents of information produces large amounts of cipher text, which can be used for cryptanalysis attacks, especially known plaintext attacks (where certain parts of the encrypted data, such as e-mail headers, are known beforehand to the attacker).

Algorithms use more efficient methods to create digital signatures. Common types of digital signatures today are created by signing message digests with the originator's private key to create a digital thumbprint of the data. When the message digest is signed, the signature is usually much shorter than the data that was signed. Hence a digital signatures place a relatively low load on computer processors can consume insignificant amounts of bandwidth, and produce small amounts of cipher text for cryptanalysis. Two of the most widely used digital signature algorithms today are the RSA digital signature process and the Digital Signature Algorithm (DSA).

2.3 Uses for Digital Signatures

Anyone with the public key can use it to perform a validity check of digital signatures created by the private key only. A digital signature when created by the appropriate private key decrypts and validates properly with the public key. In case, a different private key was used to sign the data, the validity check fails. When the contents of digitally signed data or the digital signature have been tampered are corrupted and the validity check fails. Valid digital signatures are used to perform the following functions:

- Authenticate online entities.
- Verify the source or origin of digital data.
- To make the integrity of digital data against tampering.

Algorithms use more efficient methods to create digital signatures. The common types of digital signatures today are created by signing message which digests the originator's private key to create a digital thumbprint of the data. Consequently the message digest is signed while the signature is usually much shorter than the data that was present[8]. Therefore, digital signatures place a relatively low load on computer processors during the signing process can consume insignificant amounts of bandwidth, and produce small amounts of cipher text for cryptanalysis. Most widely used digital signature algorithms today are the RSA digital signature process and the Digital Signature Algorithm (DSA).

2.4 RSA Data Security Digital Signature Process

The private key is used to encrypt only the message digest in the RSA digital signature process. The encrypted message digest begin to be the digital signature and is attached to the original data.

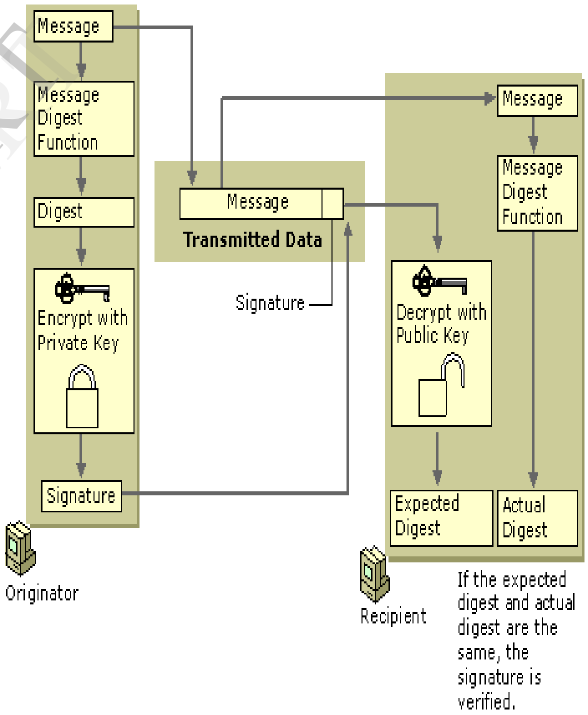

Fig.3: Basic RSA Data Security Digital Signature Process

WORKFLOW DIAGRAM

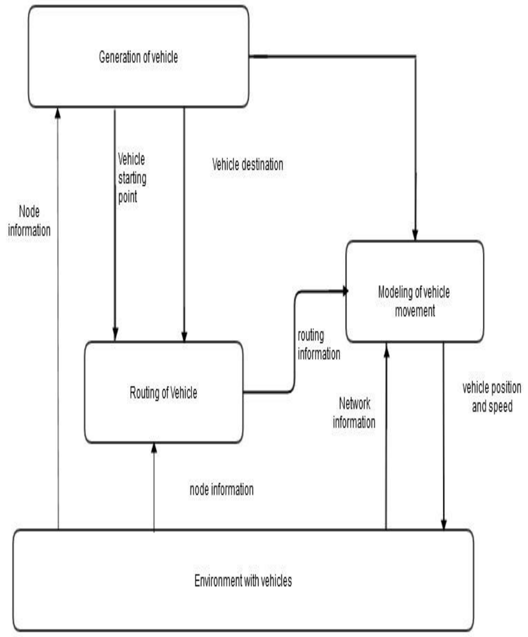

Fig. 4: Workflow of VANET

3 MODULE DESCRIPTION

a) VANET Formation:

Multi hop wireless broadcast is an important component in vehicular networks. Many applications are built on broadcast communications, so efficient routing methods are critical for their success. Here we concentrate on VANET, in VANET multihop wireless broadcast is an important component. Lot of applications and protocols are built on this issue for routing and data delivery [9]. Vehicular ad hoc networks (VANETs) are a subgroup of mobile ad hoc networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Because of the restricted node movement it is a feasible assumption that the VANET will be supported by some fixed infrastructure that assists with some services and can provide access to stationary networks. The fixed infrastructure will be deployed at critical locations like slip roads, service stations, and dangerous intersections or places well-known .for hazardous weather conditions.

b) Channel Quality:

In DADCQ protocol mainly focus on the routing issues, for that channel quality adaptive protocol is implemented to solve the routing issues. In the spatial distribution channel quality adaptive protocol also have the security issues like DOS attack and man in the middle attack.

c) Decision Threshold with Spatial Distribution:

The DADCQ protocol utilizes the distance method to select forwarding nodes. The performance of this method depends heavily on the value of the decision threshold, but it is difficult to choose a value those results in good performance across all scenarios. Node density, spatial distribution pattern, and wireless channel quality all affect the optimal value. The arrangement of a phenomenon across the Earth's surface and a graphical display of such an arrangement is an important tool in geographical and environmental statistics. A graphical display of a spatial distribution may summarize raw data directly or may reflect the outcome of more sophisticated data analysis.

d) Diffie Hellman With RSA(Key Exchange):

To make the communication secure in the key exchange we implement the Diffie-Hellman algorithm and with the RSA security which makes our spatial distribution secure. A public encryption method that relies on a public encryption algorithm, public decryption algorithm and a public encryption key. Using the public key and encryption algorithm, everyone can encrypt a message. The decryption key is known only to authorize parties. To check the RSA encryption each and every node need to be have the module to check the RSA encryption.

4 CONCLUSION

VANET is an emerging and attractive technology dedicated to safety and comfort services to the vehicle users. As a result of high dynamic topology and unpredictable channel distribution, it can pursue for a suitable routing protocol algorithm that can generate a near seamless network connectivity among the vehicular nodes. This major research challenges are available in VANET. In present VANET RBC/NS-2 guided simulation, we have used a near realistic mobility model with DSR as the routing protocol. The communication trace file generated from NS-2 contains large volume of information. In our work, a packet delivery ratio of 59.89% is achieved using 20 nodes and DSR routing protocol.

5 REFERENCES

[1] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen , and J.-P. Sheu, “The Broadcast Storm Problem in a Mobile Ad Hoc Network,” Proc. ACM/IEEE MobiCom, 1999.

[2] M.J. Slavik and I. Mahgoub, “Statistical Broadcast Protocol Design for Unreliable Channels in Wireless Ad-Hoc Networks,” Proc. IEEE GlobeCom, Dec. 2010.

[3] W. Lou and J. Wu, “Toward Broadcast Reliability in Mobile Ad Hoc Networks with Double Coverage,” IEEE Trans. Mobile Computing, vol. 6, no. 2, pp. 148-163, Feb. 2007.

[4] Y.-C. Tseng, S.-Y. Ni, and E.-Y. Shih, “Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network,” IEEE Trans. Computers, vol. 52, no. 5, May 2003.

[5] S. Biswas, R. Tatchikou, and F. Dion, “Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety,” IEEE Comm. Magazine, vol. 44, no. 1, pp. 74-82, Jan. 2006.

[6] F. Ye, R. Yim, J. Guo, J. Zhang, and S. Roy, “Prioritized Broadcast Contention Control in VANET,” Proc. IEEE Int’l Conf. Comm.(ICC), pp. 1-5, May 2010.

[7] Y. Bi, L. Cai, X. Shen, and H. Zhao, “A Cross Layer Broadcast Protocol for Multihop Emergency Message Dissemination in Inter Vehicle Communication,” Proc. IEEE Int’l Conf. Comm. (ICC), pp. 1-5, May 2010.

[8] J. Cartigny, D. Simplot, and J. Carle, “Stochastic Flooding Broadcast Protocols in Mobile Wireless Networks,” technical report, University ´ des Sciences et Technologies de Lille 1, http:// citeseer.ist.psu.edu/525199.html, May 2002.

[9] X.-Y. Li, K. Moaveninejad, and O. Frieder, “Regional Gossip Routing for Wireless Ad Hoc Networks,” Mobile Network Applications, vol. 10, nos. 1/2, pp. 61-77, 2005.

[10] S. al Humoud, L. Mackenzie, and J. Abdulai, “Neighbourhood-Aware Counter-Based Broadcast Scheme for Wireless Ad Hoc Networks,” Proc. IEEE GlobeCom Workshops, pp. 1-6, 2008.

[11] A.Mohammed,M.Ould-Khaoua,L.Mackenzie,andJ.-D. Abdulai, “Dynamic Probabilistic Counter-Based Broadcasting in Mobile Ad Hoc Networks,” Proc. Second Int’l Conf. Adaptive Science Technology (ICAST ’09), pp. 120-127, 2009.

[12] M. Slavik and I. Mahgoub, “Stochastic Broadcast for VANET,” Proc. Consumer Comm. and Networking Conf., Jan. 2010.

[13] O. Tonguz, N. Wisitpongphan, J. Parikh, F. Bai, P. Mudalige, and V. Sadekar, “On the Broadcast Storm Problem in Ad Hoc Wireless Networks,” Proc. Third Int’l Conf. Broadband Comm., Networks and Systems (BROADNETS ’06) pp. 1-11, Oct. 2006.

[14] O. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, “Broadcasting in VANET,” Proc. Mobile Networking for Vehicular Environments, pp. 7-12, May 2007.

[15] N. Wisitpongphan, O. Tonguz, J. Parikh, P. Mudalige, F. Bai, and V. Sadekar, “Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks,” IEEE Wireless Comm., vol. 14, no. 6, pp. 84-94, Dec. 2007.

[16] O. Tonguz, N. Wisitpongphan, and F. Bai, “DV-CAST: A Distributed Vehicular Broadcast Protocol for Vehicular Ad Hoc Networks,” IEEE Wireless Comm., vol. 17, no. 2, pp. 47-57, Apr. 2010.

[17] W. Viriyasitavat, F. Bai, and O. Tonguz, “UV-CAST: An Urban Vehicular Broadcast Protocol,” Proc. IEEE Vehicular Networking Conf. (VNC), pp. 25-32, Dec. 2010.

[18] P. Kyasanur, R. Choudhury, and I. Gupta, “Smart Gossip: An Adaptive Gossip-Based Broadcasting Service for Sensor Networks,” Proc. IEEE Int’l Conf. Mobile Adhoc and Sensor Systems, pp. 91-100, 2006.

[19] B. Bako, F. Kargl, E. Schoch, and M. Weber, “Advanced Adaptive Gossiping Using 2-Hop Neighborhood Information,” Proc. IEEE GlobeCom, pp. 1-6, Nov. 2008.

[20] T. Osafune, L. Lin, and M. Lenardi, “Multi-Hop Vehicular Broadcast (MHVB),” Proc. Sixth Int’l Conf. ITS Telecomm., pp. 757-760, June 2006.

[21] M. Mariyasagayam, T. Osafune, and M. Lenardi, “Enhanced Multi-Hop Vehicular Broadcast (MHVB) for Active Safety Applications,” Proc. Seventh Int’l Conf. ITS Telecomm. (ITST ’07), pp. 1-6, June 2007.