2012 International Conference on Information and Network Technology (ICINT 2012)

IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

A Cluster Based Authentic Vehicular Environment for Simple Highway Communication

R. Lakshmi Devi, C. Maheswari [+] and Lynette Maria

Department of ECE, Sri Sairam Institute of Technology, Chennai

Abstract. Vehicular Ad hoc Network (VANET) is an advanced version of Mobile Ad hoc Network (MANET) that provides comfort and safety for passengers from road accidents. This paper discusses cluster based model for VANET in highway communication. Security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. There are number of attacks like spoofing, traffic tampering, Denial of Service etc that create problems in accessing the network. This paper identifies these security issues and provides solutions to overcome them. To prevent impersonation, certification authority is used to ensure privacy for every user. To thwart traffic tampering, threshold based event validation Scheme to validate an event. To enhance security, we present technology switching method for Denial of Service (DOS) attack.

Keywords: VANET, MANET, SHWM, DSRC, OBU, CBVANET and CBSHWM.

1. Introduction

Vehicular ad hoc network (VANET) is a kind of mobile ad hoc network. It enables communication between moving vehicles and the road side units (RSU's) that have to access to the internet through backbone network. In a VANET, the vehicles are considered as nodes. The vehicles equipped with the communication device known as On Board Unit (OBU) equipped with GPS, will be able to receive and transmit message. The vehicles move either with high speed or low speed with no power constraint. The vehicles of a VANET are equipped with the DSRC (Dedicated Short Range Communication). Communication from the source node can either directly reach the destination or through an intermediate node which may be a router or a road side unit. The movement of the vehicles is limited by the road condition such as narrow or curved and traffic congestion. High speed vehicles form quick dynamic network topology and it requires real time packet transfer. These characteristics of VANET play an important role in creating a vehicular ad hoc network, new protocols and architectures. Unlike previous model this paper attempts to propose a new clustering model with security solution for VANET communication that can be used both inside and outside the city.

2. VANET

VANET is an advanced version of Mobile ad hoc network (MANET). Most of the MANET features can be applied in the VANET environment also. However these works cannot be directly applicable to VANET due to the fundamental difference between VANET and MANET. In MANET, nodes are moving at random and their speed is normal but in VANET, nodes are high speed moving vehicles in an organized and predefined road. Due to the high speed of the vehicle nodes, their network topology changes very quickly. Hence the usual mobile ad hoc technology IEEE802.11 is not well suited for VANET. For this reason a suitable amendment is made on the existing standard 802.11 that becomes a new vehicular technology, IEEE802.11p called Wireless Access in Vehicular Environment (WAVE). Its

[+] Corresponding author. Tel.: + 044 24610778.
E-mail address: mahe.eswari17@gmail.com.

bandwidth is 75 MHz at 5.9GHz. It has seven 10MHz channel with one control channel and six service channels.

3. Work Related to VANET

In most of the existing VANET models, communication at any point is done through a VANET node to another VANET node through a Fixed Roadside Unit only. In this all the nearby vehicles are connected to this road side units and all the road side units are in turn connected together to form mobile ad hoc network.

This scenario is valid inside a city where the vehicle moves slowly and more number of fixed base stations is available. But if the vehicle moves with high speed on a highway outside the city, where there is very little or no roadside units, it is not possible to consider the city model of VANET. Hence there is a requirement to propose a new model for VANET on a highway [1]. However, this model is not suitable for wider roads like in highways. Hence, vehicle to vehicle communication is adopted without the use of RSU [2]. This is done by two ways: Single-hop and multi-hop. In single-hop-relevant applications (such as emergency braking or lane change alerts), only one or a few vehicles – those vehicles involved in the event – will send out a notification to nearby vehicles. Such traffic information is irrelevant to vehicles multiple network hops away. In multi-hop-relevant applications (such as road hazard and congestion notification systems) a large number of vehicles are involved and report the event to vehicles that are potentially multiple network hops away, so recipients can respond appropriately. But if there are no RSUs, vehicles cannot get pre-defined data about the vicinity and also the information cannot be transmitted to a longer distance. Therefore, both Vehicle-to-Vehicle (V2V) and Vehicle-to - Infrastructure (V2I) communication is necessary [3]. The dynamic and dense VANET topology and the harsh VANET environment, produce many challenges for communication and networking. In traditional Mobile Ad hoc Network (MANET) research, these difficulties were often overcome by a clustered topology. As a result, clustering is implemented in VANET environment.

4. Proposed Work

4.1 Cluster based simple highway mobility model (CBSHWM)

In this architecture the VANET area has been split up into a number of clusters using the proposed cluster formation algorithm. Each cluster has a cluster head. The cluster head may be either RSU or any one of the vehicles with lowest speed. All the cluster heads in the VANET are regularly updated if a new service enters the network.

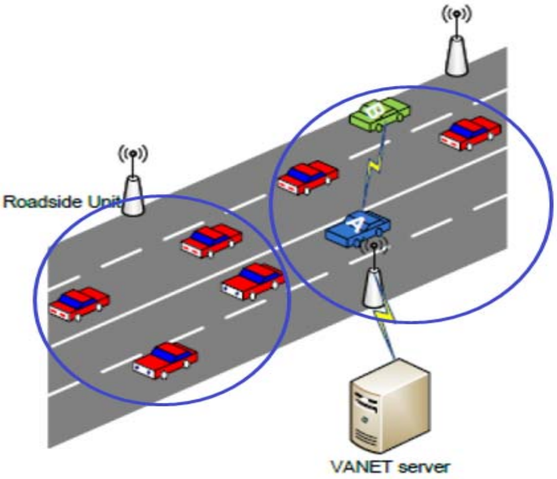

Fig. 1: Architecture of VANET

The Cluster creation in the proposed model is different from the existing model. In MANET, clusters are created dynamically but in the VANET the cluster area remains same and predefined. The size of the cluster changes only during unavoidable situations like sudden increase in the number of vehicles moving in a particular road due to traffic changes. In our system the cluster remains in the same frequency. So the cluster areas are created as fixed ones but the process involves a series of steps to ensure that the node created cluster is efficient and it gives better efficiency. While creating cluster, it should be ensured that the cluster head is not frequently crossing its boundary. If the vehicle moves out frequently then the Cluster head election algorithm is implemented to elect a new cluster head.

5. Security Issues in VANET

VANET suffers from different type of attacks and probably more than Mobile ad hoc networks due to their highly dynamic and volatile nature. The systems that are designed to provide security in VANET should be efficient and at the same time the computation cost for computing messages should be less.

The various attacks are as follows (i) Attackers track vehicles to obtain those drivers' private information. Attackers use false identities to pretend like other vehicles (ii) Attackers diffuse false information to affect the behavior of other drivers (iii) Attacker attacks the communication medium in VANET to cause the channel jam or to create some problems for the nodes from accessing the network

6. Proposed Security Solutions

6.1. Certification Authority

The proposed VANET system requires having a VANET server. VANET servers are responsible for evaluating, maintaining and storing the records of the registered vehicles in its database. These records include old IDs to new IDs issued. These IDs will be used to verify the authenticity of each node in the VANET. Every node before entering into the network should be registered to the VANET server. It provides a unique ID to the node which will be used for transmission within the cluster. For every cluster, the ID of the node will be changed hence making it difficult for the attacker to identify the sending node hence providing message privacy.

6.2. Threshold based event validation protocol

In order to prevent false information attack or to prevent the abuse of emergency alarms, an efficient and secure threshold based event validation protocol is proposed. In VANET applications, a threshold value is assumed according to the density of nodes and conditions of the road. Hence it is assumed that the system knows a priori what values are appropriate for a given scenario. Only if the total number of alerts surpasses the threshold, is considered to be valid. Otherwise, it is treated as false information and ignored. It is also assumed that the number false information is lesser than the number of authentic information.

6.3. Solution for DOS Attack

The proposed model also includes solution to prevent DOS attack .This model relies on the use of On-Board-Unit (OBU) that is fitted on each vehicle to make decision as to deter a DOS attack. In the case of DOS attack, the Processing Unit will suggest to the OBU to switch technology, or to use frequency hopping technique.

Technology Switching. There are a number of communication technologies to work with VANET, such as Wi-MAX, Wi-Fi, and other technologies. Whenever attacker launches an attack, accessing to the network is switched between these technologies, making the attack terminated at a network type. Hence, the services of the overall network remain unaffected. The features of these technologies help the system to switch between technologies. If the intensity of the attack is low then low range technology is selected and when the level of attack or range of the DOS is large, then cellular technology is used.

7. Experimental Analysis

The Proposed protocol is simulated using NS2 linuxredhat9 system. The following are parameters for the test bed. VANET size 1500 * 1500 meters of highway with movement of vehicles. Number of nodes may vary between 10 and 50.

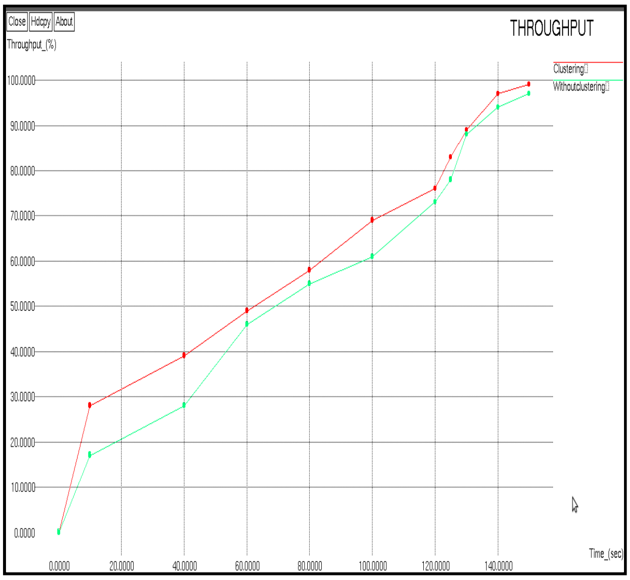

Fig. 2: Throughput Vs time with and without cluster

Fig.2 compares the throughput of clustering model with the centralized model. From the graph it is observed that the average throughput obtained by using the proposed clustering model is more efficient. For random node speeds the throughput is increased by 8%.

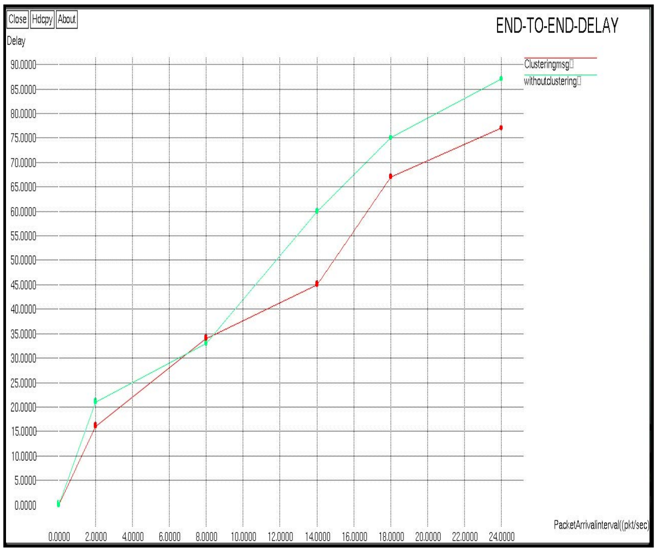

Fig. 3: End-to-End delay with and without cluster

The graph of End-to-End delay for both with and without clustering is shown in Fig.3. As the cluster heads are used to forward the packets in clustering model, there is a reduction in end to end delay by 14.1%. Hence the proposed model is more efficient than the existing models.

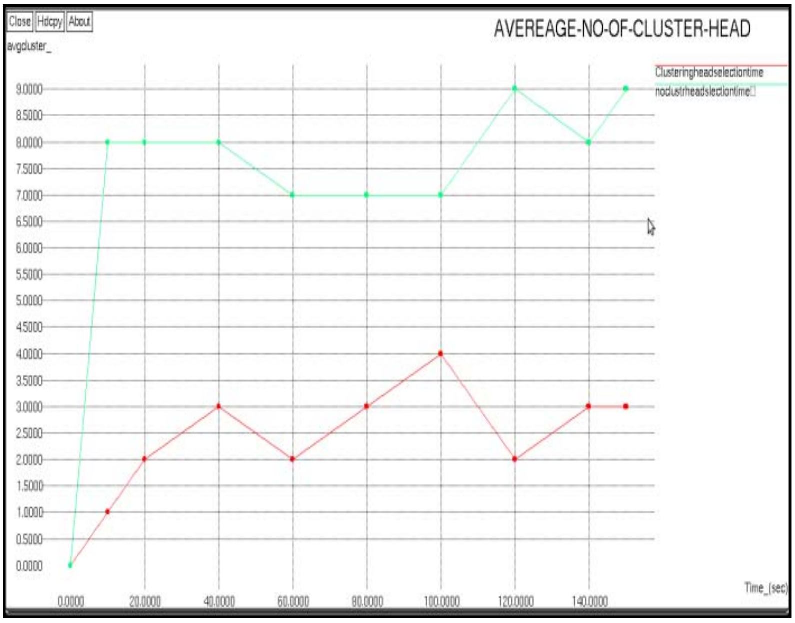

Fig. 4: Average number of cluster head

Fig.4 compares the average number of cluster heads required over a period of time with and without using cluster head election algorithm. It is inferred that using the proposed model number of cluster heads used is reduced.

8. Conclusion

Safety is the primary concern to many road users. VANET application has the opportunity to provide such safety requirements. However, life critical messages must be transmitted from node to node in the VANET network in reliable and timely manner. To achieve this, secure communication and network availability must be obtained in the VANET set up. This paper discusses a new cluster based model with central authority to ensure authentication. It also focuses the different types of attacks that may be applicable to VANET and provides solutions to overcome those attacks. The proposed clustering model increases throughput and reduces end to end delay thereby providing efficient communication between VANET users. The proposed security solutions to this cluster based model provide an authentic environment, and are to be tested by simulation.

9. References

[1] "An Information Propagation Scheme for VANETs" by T.D.C Little and A.Agarwal. In Proceedings of Intelligent Transportation Systems, September 2005. Page 155-56.

[2] "Analysis of Routing Protocols for Highway Models without Using Roadside Unit and Cluster" by B. Ramakrishnan, Dr. R. S. Rajesh, R. S. Shaji. In proceedings of International Journal of Scientific & Engineering Research, Volume 2, Issue1(2011). Page 5-13.

[3] "ROAMER: Roadside Units as Message Routers in VANETs" by Khaleel Mershad ,

Hassan Artail, Mario Gerla. In proceedings of Ad Hoc Networks Journal Volume10 (2012). Page 479–496.

[4] "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" by Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. In proceedings of New Trends in Information Science and Service Science (NISS), 2010 4th International Conference. Page 393-398.

[5] "Securing vehicular ad hoc networks", by Maxim Raya and Jean-Pierre Hubaux. In proceedings of Journal of Computer Security 15 (1) (2007). Special issue on Security of Ad Hoc and Sensor Networks. Page 39–68.

[6] J. Douceur," the Sybil Attack", First International Workshop on Peer-to-Peer Systems, 1st edition, USA, Springer, 2003.

[7] F. Karnadi, Z. Mo, “Rapid Generation of Realistic Mobility Models for VANET” . In proceedings of IEEE Wireless Communications and Networking Conference, 2007.

[8] X Lin, R Lu, C Zhang, H Zhu, P Ho,and X Shen. “Security in Vehicular AdHoc Networks“, IEEE Communications Magazine, volume 4, April 2008.

[9] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and JP Hubaux, “Eviction of Misbehaving and Faulty Nodes in Vehicular Networks “, IEEE Magazine, volume 10, October 2007.

[10] Analysis of Routing Protocols for Highway Model without Using Roadside Unit and Cluster by B. Ramakrishnan, Dr. R. S. Rajesh, R. S. Shaji. International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2011. ISSN 2229-5518.