A Study of Safe and Efficient Road Transport System Using Vehicular Ad Hoc Networks (VANETs)

Anish A
Syscon Metering solution, Bangalore, India
msgtoanish@gmail.com

EscalinTresa L
Research Scholar, ETCE Dept,
Sathyabama University, Chennai, India
escalintresa83@gmail.com

Abstract. Vehicular Ad Hoc Networks (VANET) is a special class of Mobile ad hoc networks which provides a distinguished approach for Road Transport System (RTS). The potential role of VANETs in Road Transport System is to improve traffic management, safety, convenience and commercial applications and also enable a wide range of value-added services such as collision warning/avoidance and work zone warning. The study of Road Transport System using VANETs is important and necessary for Autonomous vehicle in Intelligent Transport system environment. This paper discusses the communication domain, security challenges, simulation methodologies and various routing protocols for vehicular ad hoc networks. It explores the motivation behind the designed, and traces the evolution of VANETs.

Keywords: VANETs, MANETs, RSU, RTS, ITS, Delay Tolerant network.

1. Introduction

Nowadays, traffic congestion and road safety are the major problems in all cities. The congestion and related vehicle accommodation problem is accompanied by a constant threat of accidents as well. Absence of road traffic safety takes a toll of precious human lives and poses a direct threat to our environment as well. Other negative consequences are related to energy waste and environmental pollution.

According to Association for Safe International Road Travel, the following figures indicate the Annual Global Road Crash Statistics, Nearly 1.3 million people die in road crashes each year, on average 3,287 deaths a day. In addition to that 20-50 million are injured or disabled. Road traffic crashes rank as the 9th leading cause of death and account for 2.2% of all deaths globally. Over 90% of all road fatalities occur in low and middle-income countries, which have less than half of the world's vehicles. Road crashes cost USD $518 billion globally, costing individual countries from 1-2% of their annual GDP. Road crashes cost low and middle-income countries USD $65 billion annually, exceeding the total amount received in developmental assistance. According to their survey, unless action is taken, road traffic injuries are predicted to become the fifth leading cause of death by 2030.

Today the increasing number of vehicles on roads and the sharp advancement of wireless networks in recent years, there is an immense potential to deploy intelligent transportation systems and application on our streets and roads. Vehicular Ad Hoc Network (VANET) is a self-organized network formed between two or more vehicles equipped with wireless communication devices. Messages in VANETs can be transmitted directly to other vehicles within the radio range of the transmitter as direct communication or can be transmitted to vehicles outside the radio range of the transmitter by the means of multi-hop communication. Delivering a message from a source vehicle to one or more destinations is usually achieved via VANET multi-hop routing. In order to efficiently deliver a message from a source vehicle to a destination vehicle, a reliable VANET routing protocol should govern the routing process. A VANET routing protocol is a set of rules and criteria used in making routing decisions and for finding the best transmission path between source and destination.

The implementation process in VANET is quite challenging comparing to other mobile networks such as MANET. High speed mobility, intermittent network, dynamic topology and the lack of central coordination and management entity are all special characteristics for VANET. To overcome these difficulties, we provide an overall structure of the VANETs for the benefit of the researches.

2. Vehicular Ad Hoc Networks (VANETs)

VANET is a special class of Mobile Ad hoc Networks (MANET), in which the nodes are the vehicles which communicate with other vehicles or with the base station which acts as a roadside infrastructure for using security and services application. Though the nodes are mobile in VANETs as well as MANETs, the mobility in VANET is constrained to the boundaries of the road unlike the nodes in MANETs, where movement is more random in nature. Nodes in VANET are also characterized by high node mobility and fast topology changes. Unlike MANET, power is not of great concern in VANETs as the vehicle batteries have sufficient and rechargeable power. The concept of network vehicle was first proposed by a team of engineers from Delphi Delco Electronics Systems and IBM Corporation in the year 1998.

The three major classes of applications possible in VANET are safety oriented, convenience oriented and commercial oriented. Safety applications will monitor the surrounding road, approaching vehicles, surface of the road, road curves etc. They will exchange messages and co-operate to help other vehicles out under such scenario. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Convenience application will be mainly of traffic management type. Their goal would be to enhance traffic efficiency by boosting the degree of convenience for drivers. Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video.

3. Overview of VANETs Architecture

This part describes the system architecture of vehicular ad hoc networks. Here we discuss the main component of the VANETs architecture.

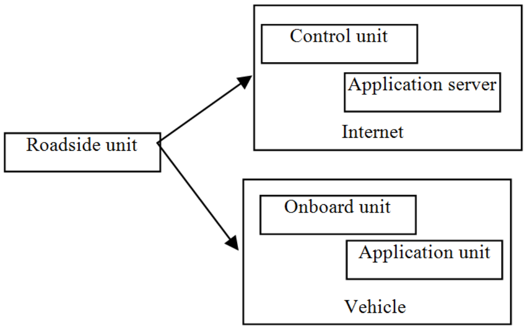

Fig 1: VANETs Architecture

On Board Unit (OBU)

The on board unit contains communication and sensing devices are mounted on the vehicles. With the help of on board unit the vehicle can communicate with other vehicles or the road side unit (RSU).

Application Unit (AU)

The application unit is a device executing application by using road side unit's communication capabilities. It also take care of more number of application that can be categories by: safety applications and non-safety applications.

Road Side Unit (RSU)

The road side unit contain a communication unit located aside the roads. The RSU communicate with vehicle and also connects with application server and trusted authorities in the VANETs environment.

4. VANETs Communication Domain

According to the architecture standard guidelines, the VANETs communication can be classified into three domains: In vehicles domain, Ad hoc domain and Infrastructural domain.

In vehicle domain

It is one of the more necessary and important domain in VANETs communication. This domain communicate with the components which are connected in on-board, to provide safe and efficient road transportation. It also detects vehicle performance.

Ad hoc domain

The ad hoc domain is also called as vehicle to vehicle (V2V) communication. It provides driver assistance, by exchanging data between the drivers to share information and warning messages.

Infrastructural domain

The infrastructural domain perform two types of communication: they are, vehicle to infrastructure (V2I) and vehicle to broadband (V2B).

The vehicle to infrastructure (V2I) communication provides real time data such as, traffic data, weather data, etc., to the drivers.

The vehicle to broadband (V2B) communication enables communication to outside world via 3G/4G. This types of communication will be useful for both the driver and the passenger in terms of safety, convenience and entertainment.

5. VANETS Service Model

The VANETs service model provide seven different types of service. Each of the service model provides a specific service for users.

Information as a service (INAAS)

In this model, several type of virtualization take place. Here, the infrastructure devices and hardware are virtualized, that enables user to install the operating system and operate software applications.

Entertainment as a service (ENAAS)

The aim of this service is to provide passenger's comfortable journey on the road, to make their journey as enjoyable as possible, this service provide content such as movies, online games, audio, etc.,

Computation as a service

In most of the case some vehicles are parked in the parking lot for a period of time, the computing and storage resources of these vehicles are unused for long time and the opportunity for their use is unexploited. VANETs can aggregate the computing and storage capabilities of parked vehicle and it as a new service to customers.

Cooperation as a service (CAAS)

It provides several free services without any additional infrastructure, by exploiting the advantages of VANETs. CaaS uses a mechanism by which the drivers express their interest for a service or a set of services network where the vehicle having the same service subscribed to cooperate.

Storage as a service (STAAS)

The storage as a service in VANETs is different from other services. It provides storage for backup purpose and the real time data about the vehicle and the road will be stored in the centralized storage unit, for safety purpose and real time traffic management system.

Network as a service (NAAS)

If a vehicle need internet, on the road while driving. This service provide internet to the vehicle, using this service, the vehicle can access many other service in the VANETs environment.

6. Characteristics of VANETs

In order to design an effective system, we need to understand the characteristics of the network. It, depending on the specific study, have been classified in a variety of different ways. Here we summarize some of the VANETs characteristics.

Providing safe driving

In a critical situation, data transmitted from a RSU to a vehicle may warn a driver about road accident, traffic congestion, etc.,. Effective communication between nodes (vehicle) and the Rode Side Unit (RSU) can save many lives and prevent injuries. When a vehicle significantly changes its speed, the application relay such information to its neighboring vehicles via broadcast message. This way, drivers further behind are notified by an alarm signal, and as a result, potential accidents can be avoided. This type of application can lead to reduce the number of collisions.

Improving passenger comfort

It aims to improve passenger comfort levels (make journey more pleasant). It also provides passenger with weather and traffic information and provide detailed information about location such as nearest hotel, restaurant, shopping mall, etc.,. Passenger can also access Internet while the node is connected to the infrastructure network.

Enhancing traffic efficiency

If any node (vehicle) detects any change in traffic or road hazard, can inform neighboring node (vehicles) and the Road Side Unit (RSU) about the situation by transmitting Broadcast message. For example, a node (vehicles) found there is an accident or hazard in road, then it could help its neighboring nodes by relay this information to vehicles approaching the location. This would allow vehicles approaching the congested area ample time to take alternate routes.

Node density

Here the nodes are vehicle that could involve the vehicles in several city, several states, or even a country. So the VANETs node density is always high and because of the high mobility of the nodes, the nodes in the network will change instantaneously.

High mobility

In VANETs, the nodes are vehicle, usually they are moving at high speed. So, the motion of the node is constrained by the VANETs topology.

Network topology

Due to the density and high mobility of the node, the network topology in the VANETs has a tendency to change frequently. This leads VANETs became a topology less network.

7. Security Challenges in VANETs

One of the main challenges in VANETs is high mobility of nodes that causes several security challenges in VANETs environment.

Privacy

This ensures that the vehicle information is not transparent to unauthorized person. The third party should not track vehicle movements as such would be a violation of personal privacy. Thus, a certain degree of anonymity should be maintained when delivering messages and initiating transactions between vehicles. However, in liability related cases, specified authorities should be able to trace user identities to determine responsibility. Location privacy is also important so that information regarding the past or future locations of vehicles is not made known.

Scalability

The security schemes must be scalable to handle high mobility of nodes in VANETs. The security schemes of VANETs must handle both the low density and high density of the nodes, because based on the density of the node produce dynamic demands on security

Key management

The key management is comprised of three aspects: key assignment, key verification and key revocation.

Key assignment

Initially, a vehicle will obtain a key pair from the vehicle manufacturer or governmental transportation authority. Key assignment is on the basis of a unique ID

Key verification

The Key validation can be done at the CAs or sub-CAs, we assume that every vehicle trusts CAs and that CAs are tamper-proof.

Key revocation

In VANETs environment key revocation is an important and effective way to prevent attack. In certain cases, when key pairs will be hacked by the attackers. It is mandatory to disable the exposed key pair.

Establishing trust relationship

Trust is one of the key factor in any security systems. In VANETs, environment, it is difficult to build trust relationships. Many applications need multi- hop routing, with multiple nodes involved in communication. Therefore, the VC has inherited the challenge of establishing trust relationships among multiple vehicles, roadside infrastructure and service providers.

Authentication of high mobility nodes

It is a challenging task to authenticate a vehicle's identity in VANETs, because the nodes are high mobility in nature.

Heterogeneous network nodes

In VANETs the number of nodes are always high. Based on the vehicle models the device capabilities such as speed of processor, volume of memory, and storage will be vary. These nodes are difficulties to adapting security strategies. For example, PKI encryption and decryption algorithms will require vehicles to meet certain hardware conditions.

Data security

To ensure the confidentiality of a sensitive message, the message will be both signed and encrypted. To implement the system with a higher level of security for sensitive messages, one must design active security mechanisms.

8. VANETs Attacks

Due to the nature of open wireless transmission mediums used in VANET, there are too many different attacks for each of one to be individually enumerated. However, these attacks can be classified based on the nature, target, and impact of the attack.

Network attack

It is one of the most dangerous attack in VANETs. A single unsuccessful attack may easily affect the whole network.

DOS attack

DOS attack occurs when the communication medium falls under attack in order to cause a channel jam or prevent vehicles from accessing the network service. The attack may result in devastation and over tiredness of the vehicles and network resources. The DOS attack can be classified into following types: SYN flood attack, Smurf attack, UDF flood attack, Teardrop attack, Land attack, Flood attack, Fraggle attack, Ping of death attack, and Buffer overflow attack,

Sybil Attack

The goal of this attack is to create an “illusion” by sending wrong messages to other vehicles. In this attack, a vehicle sends multiple messages to other vehicles and each message contains a different fabricated source identity such that the originator is unknown.

Monitoring attack

In monitoring attack the attacker will monitor the whole network, listen the communication between V2V and V2I. The attacker may be either local or outsider would silently monitor and track important information, which are not supposed to release on public.

Social attack

The main goal is to indirectly create problem in the network. The social attack is a non-technical method of intrusion, which contain all unmoral and emotional messages.

Application attack

In application attack the attacker will alter the actual message and change it with a false content which may cause harm to other vehicle. This type of attack might be done by malicious node for their own benefit.

9. VANETs Routing Protocol

To design an efficient routing protocols for VANETs is challenging task due to the high node mobility nodes. In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, Geo cast routing protocol and Broadcast routing protocol.

Topology based routing protocol

The routing protocols use links information that exists in the network to perform packet forwarding to its neighboring nodes. They are further divided into Proactive, Reactive & Hybrid Protocols.

Proactive routing protocol

In proactive routing the routing information, like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of using proactive routing protocol is that there is no route discovery since the destination route is stored in the background. The various types of proactive routing protocol are: Fisheye state routing protocol, Destination sequenced distance vector routing protocol, Optimized link state routing protocol, Cluster head gateway switch routing protocol, Wireless routing protocol, and Topology Dissemination based on reverse-path forwarding routing protocol.

Reactive routing protocol

The Reactive routing protocol enables the route only when it is necessary for a node to communicate with each other. It consists of route discovery phase in which the query packets are broadcast the network for the path search and this phase completes when route is found. The various types of reactive routing protocol are: Ad hoc demand distance vector routing protocol, preferred group broadcast routing protocol, Dynamic source routing protocol, temporally ordered routing protocol, and Junction based adaptive reactive routing protocol.

Hybrid routing protocol

It is the combination of both the proactive routing protocol and the reactive routing protocol. It also reduce the control overhead of proactive routing protocols and decrease the initial route discovery delay in reactive routing protocols. The various types of hybrid routing protocol are: Zone routing protocol and Hybrid ad hoc routing protocol.

Position based routing protocol

The position based routing protocol share the property of using geographic positioning information in order to select the next forwarding hops. The position based routing algorithm further divided into: Non DTN, DTN and Hybrid.

Non DTN position based routing protocol

The non DTN do not consider discontinuous connectivity in highly congested VANETs. If there is no neighbor node in the position based routing, then forwarding strategy fails to deliver a packet. In this situation the non DTN routing protocol perform a recovery strategy to deal with such a failure. The various types of non DTN routing protocols are: Greedy perimeter state less routing protocol, Position based routing with distance vector recovery, Greedy perimeter with abstract neighbor table, Greedy perimeter coordinator routing, Connectivity aware routing protocol, Geographic source routing, Street topology based routing, Greedy traffic aware routing protocol, Diagonal intersection based routing protocol, Landmark overlays for urban vehicular routing environment, Receive on most stable group path, Adaptive moment aware routing protocol, Edge node based greedy routing protocol, Associativity based routing, movement based routing, Vertex based predictive greedy routing, Mobile infrastructure based VANET routing, Contention based Routing, Topology assist Geo-opportunistic routing, dynamic time stable geocast outing, and Border node based most forward within radious routing protocol.

DTN position based routing protocol

The DTN position based routing protocol use carry and forward strategy to cater for frequent disconnection of nodes in the network. In carry and forward strategy when a not able to contact another node it stores the packet and forward them upon connection to a neighboring node. The various types of DTN position based routing protocol are: Vehicle assisted data delivery and Geographical opportunistic routing.

Hybrid position based routing protocol

It is the combination of non-DTN and DTN position based routing protocol that includes the greedy mode and the perimeter mode. The hybrid position based routing protocol are: GeoDTN+VAV.

Cluster based routing protocol

The cluster based routing protocol is to identify a group of nodes in the network, that identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. The various types of cluster based routing protocols are: Cluster based directional routing protocol, Traffic infrastructure based cluster routing protocol with hadoof, Location routing algorithm with cluster based flooding, clustering for open IVC network, Hierarchical cluster based routing, and Cluster based location routing.

Geo-Cast routing protocol

The Geo-Cast routing protocol is a location based multi cast routing. It deliver the packet from source node to all other nodes within a specified geographical region. The various types of geo-cast routing protocols are: Inter-vehicle geocast, Direction based geocast routing protocol for query dissemination in VANET, Distributed robust geocast, Robust vehicular routing, dynamic time stable geocast routing, and broadcast based routing protocol.

Broadcast routing protocol

Broadcast routing protocol is used to broadcast the massage to its neighboring nodes in the network. It frequently use VANET for sharing, traffic, weather and emergency, and road conditions among vehicles. The various types of broadcast routing are: BROADCOMM, Urban multihop broadcast protocol, Vector based tracking detection, Distributed vehicular broadcast protocol, Edge-aware epidemic protocol, Secure ring broadcasting, and Parameter less broadcasting in static to highly mobile wireless ad hoc.

10. VANETs Simulation Model

Simulation is one of the essential step before implementing any new technology. The simulation of VANETs can be performed in two different models: software oriented model and synthetic model

Software oriented model

The various method of software oriented models are: Network simulator (NS2 and NS3), GlomoSim, MOVE (MObility model generator for Vehicular networks), TraNS (Traffic and Network Simulator environment), VANET MobiSim, NCTUns (National Chiao Tung University simulator environment), VISIM (Visual Simulator Tool), CORSIM, TRANSIMS (The Transportation Analysis and Simulation System), and ALMSUN.

Synthetic model

The various methods of synthetic models are: Stochastic model, Traffic stream model, Car following model, Queue model, Behavioral model.

11. Conclusion

In this paper, we discuss the VANETs architecture, including communication model, service model and security challenges. Then we discuss the research issues of VANETs such as: security, attacks and routing protocols. In later section we also discuss the simulation model of VANETs.

This paper describe the vehicular ad hoc networks from the research perspective, and covers the entire structure if VANETs in terms of Road transport system and it will be a comprehensive reference on vehicular ad hoc networks.

12. References

[1] Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh, 2013, "VANET" Systems for vehicular applications, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231- 2307, Volume - 2, Issue – 6.

[2] Yeongkwun Kim, Injoo Kim, 2013, Security Issues in Vehicular Networks, IEEE.

[3] Uma Nagaraj, Dr. M. U. Kharat, Poonam Dhamal, 2011, Study of Various Routing Protocols in VANET, International Journal of Computer Science & Technology Vol . 2, Issue 4.

[4] Gongjun Yan, Ding Wen, Stephan Olariu, and Michele C. Weigle, 2013, Security Challenges in Vehicular Cloud Computing, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1.

[5] Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, Rajkumar Buyya, 2013, A survey on vehicular cloud computing, ournal of Network and Computer Applications, Elsevier Ltd

[6] Mostofa, Kamal Nasir, Mohammad KhaledSohel, Mohammad Touhidur Rahman, A K M Kamrul Islam, 2013, A review on position based routing protocol in vehicular ad hoc network, American journal of engineering research (AJER), volume-02, issue-02, pp-07-13.

[7] Arunkumar Thangavelu, k Bhuvaneshwari, k kumar, k Senthil Kumar, S N Sivanandam, 2007, Location identification and vehicle tracking using VANET (VETRAC), IEEE- ICSCN 2007, MIT Campus, Anna University, Chennai, India.

[8] Yi Wu, Kenneth W. Shum, Wing Shing Wong, Lianfeng Shen, 2014, Safety-Message broadcast in vehicular ad hoc networks based on protocol sequences, IEEE transaction on vehicular technology, vol. 63, no. 3.

[9] Swapnil G. Deshpande, 2013, Classification of security attack in vehicular ad hoc network: A survey, International journal of emerging trends and technology in computer science (IJETTCS), volume 2, issue 2.

[10] R I Meneguette and L A Villas, 2014, An Autonomic algorithm for data dissemination in vehicular ad hoc network, IEEE Latin America transactions, vol. 12, no. 3.

[11] Xiaoxiao Jiang, David H C Du, 2013, A bus vehicular network integrated with traffic infrastructure, International conference on connected vehicles and Expo (ICCVE).

[12] Divyalakshmi Dinesh, Manjusha Deshmukh, 2014, Challenges in vehicular ad hoc network, International journal of engineering, technology, management and applied science, volume 2, issue 7.

[13] Sabri M Hanshi, Mohammad M Kadhum, 2013, Geographic routing protocol issues in vehicular ad hoc networks, proceeding of the 2013 IEEE international conference on RFID technologies and applications.

[14] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, 2010, Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia.

[15] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, 2010, Security Analysis of Vehicular Ad Hoc Networks (VANET).Second International Conference on Network Applications, Protocols and Services.

[16] Patrick I. Offor. 2012, Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges. Nova Southeastern University (po125@nova.edu).

[17] Komal Mehta, Dr. L. G. Malik, Dr. Preeti Bajaj. 2013, Security Challenges, Issues And Their Solutions for VANET. International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, Ambedkar Institute of Advanced communication Technologies & Research Delhi, India.

[18] Bijan Paul, Md. Ibrahim, Md. Abu Naser Bikas. 2011, VANET Routing Protocols: Pros and Cons. International Journal of Computer Applications (0975 – 8887) Volume 20– No.3.

[19] Surmukh Singh, Sunil Agrawal, 2014, VANET Routing Protocols: Issues and Challenges Proceedings of 2014 RAECS UIET Panjab University Chandigarh.

[20] Euisin Lee, Eun-Kyu Lee, and Mario Gerla, 2014, Vehicular Cloud Networking: Architecture and Design Principles, IEEE Communications Magazine.

Anish A received the B.E. degree in computer science and engineering from Anna University, chennai, in 2009; and M.E degree in computer science and engineering from Annamalai University, chidambaram, in 2011. He is currently doing research in VANET.

His research interests include Vehicular ad hoc networks, network security and cloud computing.