Transportation System of Security Issues in Vehicular Ad Hoc Networks

A. Singaravelan[*]**, A. Manikandan**[**]

[*] Prof. & Head, Dept. of MCA,King College of Technology,Namakkal, TN,India.
[**] Asst. Prof, Dept. of CSE, Paavai Engineering College, Namakkal, T.N

Abstract- Vehicular Ad Hoc Networks is a part of wireless ad hoc network that it has the characteristics of high node mobility and fast topology changes. The Vehicular Networks can provide wide variety of services, ranges from safety and crash avoidance to Internet access and multimedia applications. These vehicular communication problems include network architecture, protocols for physical and link layers, routing algorithms, as well as security issues. In this paper, we deal with the multiple issues in the vehicular ad hoc network communications and solution about these problems.

Index Terms- Mobility, Protocols, Rebroadcast, VANET, Vehicular Communication

I. Introduction

Every year peoples are injured in vehicle accidents. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. VANETs collect and distribute safety information to massively reduce the number of accidents. Such networks consist of sensors and On Board Units (OBU) installed in the vehicle as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. The RSU distributes data and road sensors, weather centers, traffic control centers, etc to the vehicles. It's also provides commercial services such as parking space booking, Internet access and gas payment. This paper deal with the structure of VANET systems, the characteristics and applications, IEEE WAVE standard for vehicular communications, the routing algorithms for VANET and its security issues.

II. HISTORY OF VEHICULAR COMMUNICATION

Vehicular communications were safety on the road, many lives were lost and much more injuries have been incurred due to vehicle crashes. A driver realizing the brake lights of the vehicle in front of him has only a few seconds to respond, and even if he has responded in time vehicle behind him could crash since they are unaware of what is going at the front. This has motivated one of the first applications for vehicular communications, namely cooperative collision warning which uses V2V communication. Other safety applications soon emerged as well as applications for more efficient use of the transportation network, less congestion and faster and safer routes for drivers. These applications cannot functions efficiently using only V2V communications therefore an infrastructure is needed in the form of RSU. The safety applications are important for governments to allocate frequencies for vehicular communications, non-safety applications for Intelligent Transportation Systems (ITS). Besides road safety, new applications are proposed for vehicular networks, among these are Electronic Toll Collection, travel & tourism information distribution, multimedia & game applications etc.

III. VANET COMPONENTS & FEATURES

A VANET consists of vehicles and roadside base stations that exchange primarily safety messages to give drivers the time to react to life-endangering events. A vehicle in a VANET is equipped with processing, recording and positioning features and is capable of running wireless security protocols as shown in Fig.1.

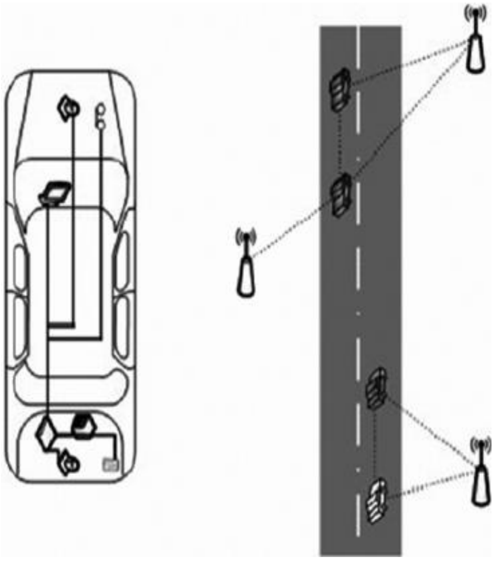

Fig.1: VANET,s Architecture

3.2. Features

Though vehicular ad hoc networks share general features with conventional ad hoc networks, VANETs have individual characteristics that are decisive in the design of the communication system, these include:

i. *Dynamic topology,*

ii. Mobility models,
iii. Infinite energy supply and
Iv Localization functionality.

3.3. Applications

VANETs enable vehicle-to-vehicle (v2v) and vehicle-to infrastructure (v2i) communication. It can exchange information about traffic issues, road conditions and added value information. VANET's applications are

- Warning
- Traffic management
- Added value

IV. IEEE STANDARDS

While ASTM E2213 standard is being developed, the IEEE standards IEEE P1609.1, P1609.2, P1609.3 & P1609.4 were prepared for vehicular networks. P1609.1 is the standard for Wireless Access for Vehicular Environment Resource Manager. It defines the services & interfaces of the RM application, the message & data formats. It provides access for applications to the rest of the architecture. P1609.2 defines security, message formatting, processing & exchanging the message. P1609.3 defines routing, transport services & the management information base for the protocol stack. P1609.4 covers how the multiple channels specified in the DSRC standard should be used.

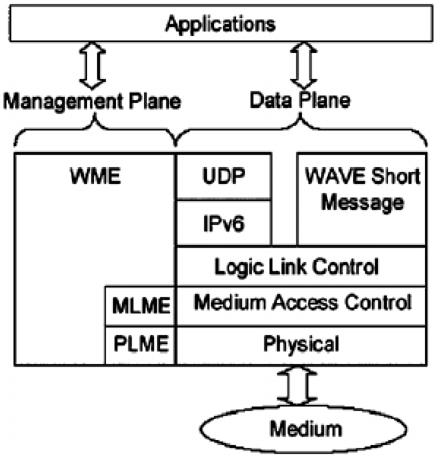

Fig.2: Protocol Architecture

The WAVE stack uses a modified version of IEEE 802.11a for its Medium Access Control (MAC) known as IEEE 802.11p.

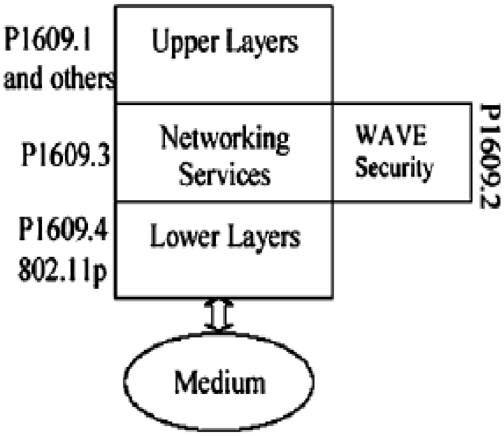

Fig 3: IEEE Architecture

V. ROUTING ALGORITHMS

Broadcasting and routing algorithms for VANET were studied in FleetNet project. Three routing protocols were considered,

- Position Based Forwarding (PBF),
- Contention Based Forwarding (CBF)
- Ad hoc On Demand Distance Vector (AODV).

These reactive protocols discover the route to a destination only when a message is to be delivered counter to proactive protocols which tend to store routing tables for every destination and update these routing tables continuously.

- PBF and CBF use location service algorithms to find the position of the destination.
- In CBF the source transmits the message with the position of the destination; every node receiving the message sets a timer proportional to the difference between its position and the destination. If the timer expires and no other node has broadcasted the message, the node forwards the message to the destination.
- In AODV the source floods the network with a route request for the destination. Nodes receiving the request calculate a distance vector & forward the message, this process is repeated till the destination is reached which sends a route reply.

CBF performs better than the other algorithms and it adapts to changes in the topology which interrupt routes in the other two protocols. It requires the assistance of maps in cities when multiple roads intersect and run in parallel, its performance in congested areas also requires more investigation. A broadcasting algorithm based on CBF suggested for safety applications. A car encountering an accident broadcasts a safety message and its current position. Other cars receiving this message set a retransmission timer inversely proportional to their distance from the source and rebroadcast the message if no other node broadcasts first and keeps rebroadcasting till it receives a message from another node or the message is no longer relevant.

Another routing algorithm called Greedy Traffic Aware Routing (GyTAR) targets the routing problem. It works with the aid of maps & traffic density information to calculate the best direction in junctions the packet should take to reach its destination. This calculation based on the distance, number of cars within that distance, their movement and speed. This paper proposed a system for collect and distributes information about the road & traffic conditions. GyTAR as well as other algorithms that its provide a solution to the routing problem in VANET.

VI. SECURITY ISSUES

Most of the critical messages in VANETs are broadcast oriented safety messages that should have a deep saturation and delivered in a short time. Additionally these messages must be secure and must not leak personal, identifying, or linkable information to unauthorized parties, as the owners of the vehicles involved in the communication have a right to privacy. Attacks can be sending false information, cheating with position information, tracking a location of a vehicle and jamming the channel for Denial of Service. A security system in VANETs must have the features of Authentication & Data Integrity, Anonymity & Availability, Low Overhead & Privacy and Real-time Constraints

VII. CONCLUSION

Vehicles are becoming a part of the global network. In this paper we have provided an overview of the development of the communication standards and ongoing research for vehicular networks. Although many problems are not yet solved, the general feeling is that vehicles could benefit from spontaneous wireless communications in a near future, making VANETs a reality. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users.

REFERENCES

[1] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in Vanets," in Proc. of the 1 ACM International Workshop on Vehicular Adhoc Networks, ACM Press, 2004, pp. 29-37

[2] J.P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles.," in Proc. of the IEEE Security and Privacy Magazine, 2, May-June 2004, pp. 49-55.

[3] K. Matheus, R. Morich, and A. Lübke, "Economic Background of Car to Car Communication," http:// www.network–on– wheels.de/documents.html, 2004.

[4] K. Plossl, T. Nowey, and C. Mletzko, "Towards a Security Architecture for Vehicular Ad hoc Networks," in ARES'06, p. 8, 20-22 April 2006.

[5] M. TorrentMoreno,F. Schmidt Eisenlohr, H. Füßler, and H. Hartenstein, "Packet Forwarding in VANETs, the Complete Set of Results," Dept. of Computer Science Universität Karlsruhe (TH) 2006.

[6] A. Zanella & E. Fasolo, "Inter-vehicular Communication Networks: a Survey," in 2nd 4 Internal NEWCOM Workshop, 2006.

[7]

AUTHORS

First Author – A. Singaravelan, Prof. & Head, Dept. of MCA,King College of Technology,Namakkal, TN,India.
singaravelan.appar@gmail.com
Second Author – A. Manikandan, Asst. Prof, Dept. of CSE, Paavai Engineering College, Namakkal, T.N,
s.a.manikandan@gmail.com