J. of Comp. and I.T. Vol. 3(1&2), 27-34 (2012).

Vehicular Ad Hoc Networks for Security Aspects

RAMESH KAIT[1], KULDEEP KHERWAL[2] and C. NELSON KENNEDY BABU[3]

[1]Department of Computer Science & Applications
Kurukshetra University Kurukshetra (INDIA)
[2]Research Scholar,Singhania University Rajsthan (INDIA)
[3]PG Computer Science & Engineering,Shri Sowdambiga College of Engineering,
Aruppukottai,Tamilnadu (INDIA)
rameshkait@kuk.ac.in, ks.kherwal@gmail.com
cnkbabu63@yahoo.in

(Acceptance Date 6th June, 2012)

Abstract

Vehicular networks are very likely to be deployed in the coming years and thus become the most relevant form of mobile ad hoc networks. In this paper, we address the security of these networks. We provide a detailed threat analysis and devise appropriate security architecture. We also describe some major design decisions still to be made, which in some cases have more than mere technical implications. In this paper we review the standardization work and researches related to vehicular networks and discuss the challenges Security Aspect for vehicular networks.

Key word: Vehicular ad hoc networks, Wireless, Security.

1. Introduction

A Vehicular Ad-Hoc Network[1,2] or VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Most of the concerns of interest to MANets are of interest in VANets, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to

follow a paved highway. In addition, in the year 2006 the term MANet mostly describes an academic area of research, and the term VANet perhaps its most promising area of application. VANET offers countless benefits to organizations of any size. Automobile high speed Internet access would transform the vehicle's on-board computer from a nifty gadget to an essential productivity tool, making virtually any web technology available in the car. While such a network does pose certain safety concerns (for example, one cannot safely type an email while driving), this does not limit VANET's potential as a productivity tool. It allows for "dead time"—time that is being wasted while waiting for something—to be transformed into "live time"—time that is being used to accomplish tasks. A commuter can turn a traffic jam into a productive work time by having his email downloaded and read to him by the on-board computer, or if traffic slows to a halt, read it himself. While waiting in the car to pick up a friend or relative, one can surf the Internet. Even GPS systems can benefit, as they can be integrated with traffic reports to provide the fastest route to work. Lastly, it would allow for free, VoIP services such as Google Talk or Skype between employees, lowering telecommunications costs.

In this paper we provide an overview of the technologies and ongoing research related to VANET. The history and the first generation VANET systems around the world are reviewed in the next section. Current frequency allocation and physical layer standards are presented in section three. In section four the IEEE WAVE standards for vehicular communications are discussed. The fifth part presents the link layer followed by a review of the routing and broadcasting algorithms designed for VANET in section six. An overview of VANET applications is provided in section seven along with some current prototypes of these applications. A discussion about security issues followed by open research problems are presented in sections eight and nine, and then finally the paper is concluded.

2.Background of Vehicular :

Communications :

The original motives behind vehicular communications were safety on the road, many lives were lost and much more injuries have been incurred due to car crashes. A driver realizing the brake lights of the car in front of him has only a few seconds to respond, and even if he has responded in time cars 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 vehicle to vehicle communication[4]. 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 function efficiently using only vehicle to vehicle communications therefore an infrastructure is needed in the form of RSU. Although safety applications are important for governments to allocate frequencies for vehicular communications, nonsafety applications are as important for Intelligent Transportation Systems (ITS) for three reasons[5]:

1) ITS systems rely on essential equipment which should be installed in every car and is widely available to the users. However, it is unlikely that individuals can afford such expensive equipment.

2) Safety applications generally require limited bandwidth for short intervals of time. Since bandwidth efficiency is an important factor, nonsafety applications are important to increase bandwidth efficiency.

3) The availability of RSU provides an infrastructure which can be used to provide a lot of services with only a little increase in cost. Besides road safety, new applications are proposed for vehicular networks, among these are Electronic Toll Collection (ETC), car to home communications, travel and tourism information distribution, multimedia and game applications just to name a few. However these applications need reliable communication equipment which is capable of achieving high data rates and stable connectivity between the transmitter and the receiver under high mobility conditions and different surroundings. Different frequencies for VANET were allocated in different parts of the world. In North America the Dedicated Short Range Communications (DSRC) band 902928 MHz was allocated. It provided short range communications (<30m) and low data rates (500 kbps). It is still used for some types of electronic toll collection systems but its performance is too limited to satisfy the demanding requirements of ITS applications.

In Japan the bands 58355840 and 58455850 MHz were allocated for uplink and 57905795 and 58005805 MHz for downlink for the Association of Radio Industries and Businesses standard ARIB STDT55.

The system relies on road architecture, as with DSRC, and provides ETC service. The standard uses ASK modulation for a data rate of 1Mbps with 8 slotTDMA/ FDD to provide service for a maximum of 8 cars within a range of 30m. Currently a new standard (ARIB STDT75) is being developed[3,5].

These systems can be regarded as the first generation for vehicular communications. The different standards and frequencies hindered the implementation of ITS systems since each country has its own specifications and operating systems. Moreover the low data rates and short distances were only suitable for a limited number of applications IEEE Standards While ASTM E2213 standard is being developed, the IEEE standards IEEE P1609.1, P1609.2, P1609.3 and P1609.4 were prepared for vehicular networks. P 1609.3 is still under further development but the other three were recently released for trial use. P1609.1 is the standard for Wireless Access for Vehicular Environment (WAVE) Resource Manager. It defines the services and interfaces of the WAVE resource manager application as well as the message and data formats. It provides access for applications to the rest of the architecture. P1609.2 defines security, secure message formatting, processing, and message exchange. P1609.3 defines routing and transport services. It provides an alternative for IPv6. It also defines the management information base for the protocol stack. P1609.4

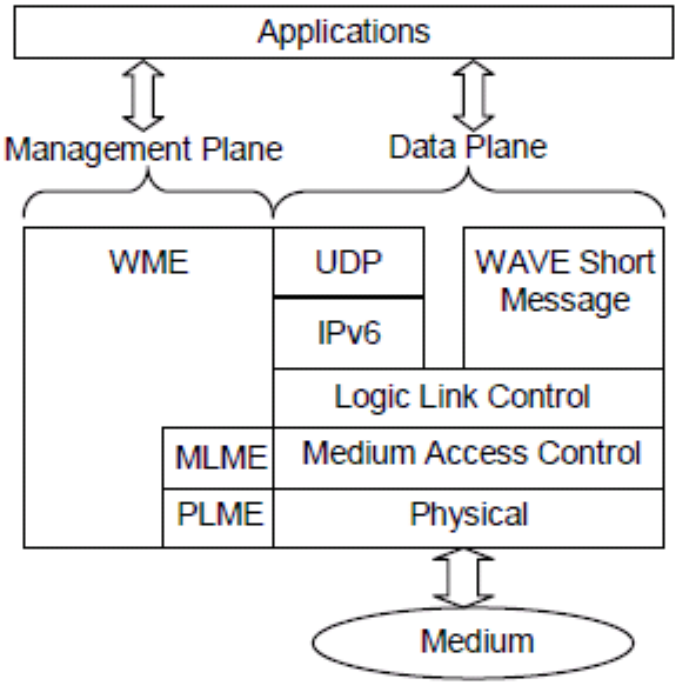

Fig. 1. IEEE Architecture

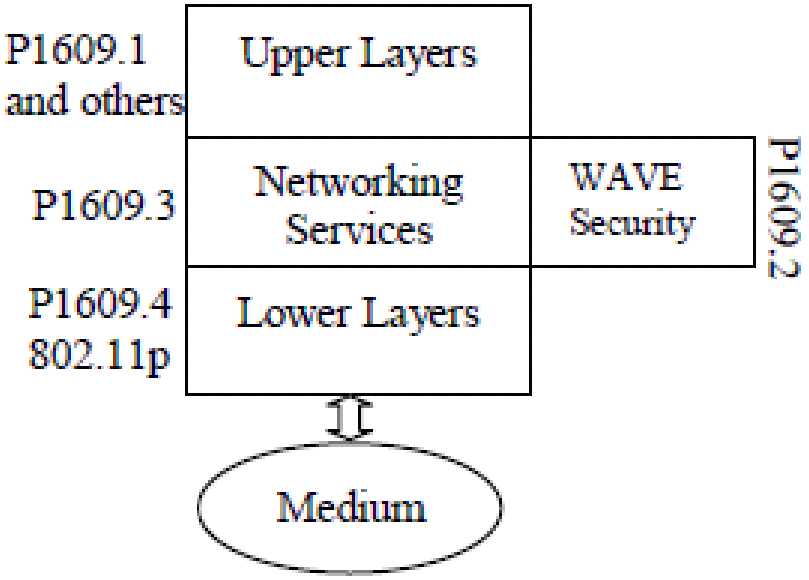

Fig. 2. WAVE Standards

covers mainly how the multiple channels specified in the DSRC standard should be used.

The WAVE stack uses a modified version of IEEE 802.11a for its Medium Access Control (MAC) known as IEEE 802.11p [13,14,6]. The protocol architecture defined by IEEE is shown in Fig. (1) and the WAVE standards in Fig. (2) [14].

3. Routing Algorithms :

Routing has always been a challenge in mobile ad hoc networks (MANET) since the positions of the nodes change with time. Existing solutions were generally optimized for slow movement and their design was constraint by the power consumption and/or the processing capabilities of the nodes. Such constraints are not essential in VANET. Moreover the movement in VANET is constraint by the road and highly predictable which is not the case in MANET where the mobility is random and in two dimensions. Broadcasting and routing algorithms for VANET were studied in FleetNet project. Their focus was on using the positioning information provided by GPS for routing and broadcasting. Three routing protocols were considered, Position Based Forwarding (PBF), Contention Based Forwarding (CBF) and Ad hoc On Demand Distance Vector (AODV). All these protocols are reactive protocols. 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. As the topology of VANET changes frequently, the signaling messages of proactive protocols can result in a large overhead load. PBF and CBF use location service algorithms to find the position of the destination, based on this position PBF selects one of the surrounding nodes to forward the message. This process is repeated till the message reaches it 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 and forward the message, this process is repeated till the destination is reached which sends a route reply. Once the reply is received the route is ready for sending the data. To reduce the flooding effects maximum hop count and Time To Live (TTL) fields are used in route messages. Simulations show that CBF performs better than the other algorithms and it adapts to changes in the topology which interrupt routes in the other two protocols. CBF, however, requires the assistance of maps in cities when multiple roads intersect and run in parallel, its performance in congested areas also requires more investigation since several cars might have the same distance to the destination which might cause collisions[15,16]. A broadcasting algorithm based on CBF has also been 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 rebroadcast till it receives a message from another node or the message is no longer relevant[8]. Another routing algorithm known as Greedy Traffic Aware Routing (GyTAR) has also been proposed[10,14]. The algorithm targets the routing problem in cities. It works with the aid of maps and traffic density information to calculate the best direction in junctions the packet should take to reach its destination. The calculation is based on the distance, number of cars within that distance, their movement and speed. The paper also proposed a system for collecting and distributing information about the road and traffic conditions which can be used with GyTAR as well as other algorithms. Although these algorithms, and others, provide a solution to the routing problem in VANET, still more research is required to examine their performance, applicability and overhead. A major issue of concern is the achievable throughput of the system. This has been examined[15]. According to their results the throughput decreases considerably with the number of hops and can be as low as 20kbps in 2Mbps links with 6 hops[12] 8.

4. Security Issues :

The ongoing Network On Wheels (NOW) project addresses a number of issues in vehicular networks with a focus on security. The project adopts an IEEE 802.11 standard for wireless access and aim at implementing a reference system. The project addresses a number of security issues for VANET[6]. VANET security should satisfy four goals, it should ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust. Several attacks can be identified and these can be generalized depending on the layer the attacker uses. At the physical and link layers the attacker can either disturb the system by jamming or overloading the channel with messages. Injecting false messages or rebroadcast an old message is another possible attack. The attacker can also steal or tamper with a car system or destroy a RSU. At the network layer the attacker can inject false routing messages or overload the system with routing Messages. The attacker can also compromise the privacy of drivers by revealing and tracking the positions of the nodes. The same attacks can be achieved from the application layer[7]. In the IEEE WAVE standard vehicles can change their IP addresses and use random MAC addresses to achieve security[11,13]. Vehicles also keep the message exchange to a minimum at the start of the journey for some time so that the messages cannot be tied to the vehicle. A number of security algorithms have been developed in France Telecom R&D department. The security proposal provides security at the link layer for vehicle safety and commercial applications, higher layer security protocols can also be used to further enhance the security or provide end to end security in a multihop link. The proposal makes use of four types of certificates, two long term and two short term. One long term and one short term certificates are used for ITS services while the others are for nonITS applications. Long term certificates are used for authentication while short term certificates

are used for data transmission using public/ private key cryptography. Safety messages are not encrypted as they are intended for broadcasting, but their validity must be checked; Therefore a source signs a message and sends it without encryption with its certificate, other nodes receiving the message validate it using the certificate and signature and may forward it without modification if it is a valid message.

NonITS data can rely on higher layer protocols to provide end to end security especially over a multihop link[16]. Another scheme has been proposed[9]. The proposal suggests the use of a long term certificate, issued by a governmental authority (GA), and temporary certificates, issued by private authorities (PA), as well as pseudonyms to protect the privacy of the drivers. For commercial services, if the user is communicating directly with the RSU, its identity is validated via the long term certificate by the GA and then it is issued a temporary certificate and pseudonym by the PA to be able to use the service. For communications via hops the source signs the message using the long term certificate, forwarding vehicles verify the message and sign it using their own certificates and so on till it reaches the RSU. The rest of the processing is similar to the direct case. The obvious limitation of this proposal is the overhead and processing time required especially when several hops are needed to reach the RSU.

5. Conclusion

In this paper we have provided an overview of the development of the communication standards and ongoing research for vehicular networks. Frequencies have already been allocated in North America and Japan and are expected soon in Europe. The IEEE 802.11p and WAVE suite were recently released for trial use. Routing protocols, broadcasting algorithms and security algorithms are being developed for vehicular networks as well as safety and commercial applications. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users.

References

1. K. Matheus, R. Morich, and A. Lübke, “Economic Background of CartoCar Communication,” http://www.network–on–wheels.de/documents.html, (2004).
2. K. Tokuda, “DSRCType Communication System for Realizing Telematics Services,” Oki Technical Review, Vol. *71*, No.*2*, pp. 6467, April (2004).
3. L. Armstrong, “Dedicated Short Range Communications (DSRC) at 5.9 GHZ,” Presentation,
4. “American Society for Testing and Materials (ASTM),” www.astm.org.
5. M. C. D. Maddocks, “An Introduction to Digital Modulation and OFDM Techniques,” BBC Research Department Report No RD 1993/10 (1993).
6. J. A. Stott, “The Effects of Frequency Errors in OFDM,” B BC Reseearch Department Report No RD 1995/15 (1995).
7. T. Wang, J. G. Proakis, E. Masry, and J. R. Zeidler, “Performance Degradation of OFDM Systems Due to Doppler Spreading,” *IEEE Transactions On Wireless Communications*, vol. 5, pp. 14221432, June (2006).

8. J. G. Proakis, Digital communications, 4th ed. Singapore: McGraw Hill, (2001).
9. B. O'Hara and A. Petrick, IEEE 802.11 Handbook A Designer's Companion. New York: Institute of Electrical and Electronics Engineers Inc., (1999).
10. S. Hess, "Frequency spectrum for ITS," COMeSafety July (2006).
11. "COMeSafety Forum," http://www.comesafety.org.] "IEEE Draft P802.11p/D2.0, November 2006."
12. "IEEE Draft P1609.0/D01, February (2007)."
13. "IEEE Draft P802.11p/D0.25, November (2005)."
14. M. Lott, "Performance of a Medium Access Scheme for Intervehicle Communication," in Proc. of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'02), San Diego, California, July (2002).
15. A. Ebner, H. Rohling, R. Halfmann, and M. Lott, "Synchronization in Ad Hoc Networks Based on UTRA TDD," in Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2002), Lisbon, Portugal, (2002).
16. A. Ebner, H. Rohling, M. Lott, and R. Halfmann, "Decentralized Slot Synchronization In Highly Dynamic Ad Hoc.