DESIGN OF SECURE AND APPLICATION-ORIENTED VANETS

Yi Qian, and Nader Moayeri
National Institute of Standards and Technology
100 Bureau Drive, Stop 8920
Gaithersburg, MD 20899-8920, USA

Abstract — **Vehicular ad hoc networks (VANETs) are important components of Intelligent Transportation Systems. The main benefit of VANET communication is seen in active safety systems that increase passenger safety by exchanging warning messages between vehicles. Other applications and private services are also permitted in order to lower the cost and to encourage VANET deployment and adoption. Security is one of the major challenges that must be addressed before VANETs can be successfully deployed. Another crucial issue is support of different applications and services in VANETs. In this paper we propose a secure and application-oriented network design framework for VANETs. We consider both security requirements of the communications and other requirements of potential VANET applications and services. The proposed framework consists of two basic components: an application-aware control scheme and a unified routing scheme. We also study a number of key enabling technologies that are important to a practical VANET. Our study provides a guideline for the design of a more secure and practical VANET.**

Keywords: **VANET, security, safety, application-oriented.**

1. INTRODUCTION

To improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the traveling public, Intelligent Transportation Systems (ITS) have been developed, which apply rapidly emerging information technologies in vehicles and transportation infrastructures. The field of inter-vehicular communications (IVC), including both vehicle-to-vehicle communications (V2V) and vehicle-to-roadside communications (V2R), also known as VANET, is recognized as an important component of ITS in various national plans [1]. The ITS architecture provides a framework for the much needed overhaul of the highway system infrastructure. The immediate impacts include alleviating the vehicular traffic congestions and improving operation management in support of public safety goals, such as collision avoidance. Equipping vehicles with various kinds of on-board sensors, and V2V and V2R communication capabilities will allow large-scale sensing and decision / control actions in support of these objectives. Communication-based active safety is viewed as the next logical step towards proactive safety systems. These systems provide an extended information horizon to warn the driver or the vehicle of potentially dangerous situations at an early stage. The allocation of 75 MHz in the 5.9 GHz frequency band licensed for Dedicated Short Range Communications (DSRC), which supports seven separate channels, may also enable the future delivery of rich multimedia contents to vehicles at short- to medium-range via either V2V or V2R VANET links [2]. The US Department of Transportation and the automotive industry are aggressively developing DSRC technologies and applications. Their joint effort has identified safety applications enabled by DSRC and evaluated DSRC radio performance [3].

VANETs are a special case of the much studied mobile ad hoc networks (MANETs), where the vehicles are the mobile nodes. If and when deployed, VANETs will be the largest MANETs ever implemented. Therefore, the issues of stability, scalability, reliability, and security are of great concern. The main challenge in VANET operation is the rapid and frequent changes in network topology due to the high mobility of the network nodes. On the other hand, vehicles move only on predetermined roads and they do not have the battery power and storage limitations of nodes in typical MANETs. Furthermore, it is reasonable to assume that vehicles can obtain their geographic positions by using GPS, which can provide good time synchronization throughout the network as well. In general, good VANET protocol design should take into account fast topology changes as well as different kinds of applications for which transmissions will be established. Moreover, VANET protocols have to reduce the communication delay, which is very important for safety applications.

In spite of the ongoing academic and industrial research efforts on VANETs, many research challenges remain. From the network perspective, security is one of the most significant challenges. Vehicle safety applications are among the major drivers for VANETs. Where people's lives are at stake, it is of course essential to secure VANETs against abuse. As a special case of MANETs, VANETs inherit all the known and unknown security weaknesses that are associated with MANETs and could be subject to many security threats. Meanwhile, even as researchers are working on enabling the applications for VANETs that have been identified so far, new applications continue to be proposed.

978-1-4244-1645-5/08/$25.00 ©2008 IEEE

In this paper, we focus on two major issues in VANET design: security and support of existing and future VANET applications. In the rest of this paper, we first give a brief background on VANETs in Section 2. We then examine the details of the challenges and requirements of VANET design in Section 3, including the general requirements for VANET security and application scenarios. We present our secure and application-oriented VANET design framework in Section 4, followed by a number of important technologies instrumental to deployment of the proposed framework in Section 5. Conclusions are given in Section 6.

2. Background on VANETs

In VANETs, each vehicle is equipped with the technology that allows the drivers to communicate with each other as well as with the roadside infrastructure, e.g., base stations also known as Roadside Units (RSUs), located in some critical sections of the road, such as traffic lights, intersections, or stop signs, to improve the driving experience and make driving safer. By using such communication devices, also known as On-Board Units (OBUs), vehicles can communicate with each other as well as with RSUs. A VANET is a self-organized network that enables communications between vehicles and RSUs, and the RSUs can be connected to a backbone network, so that many other network applications and services, including Internet access, can be provided to the vehicles. Figure 1 shows an example of a VANET.

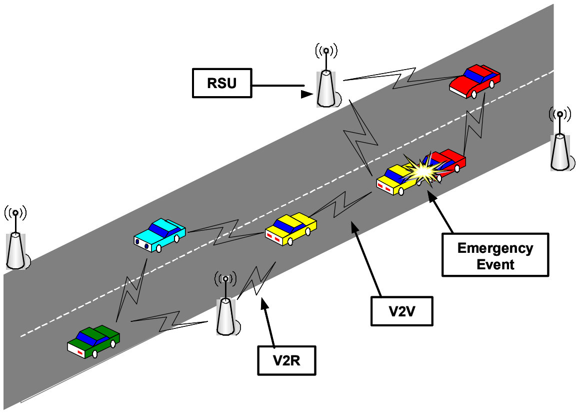

Figure 1. An Example of a VANET

The U.S. Federal Communications Commission (FCC) recently allocated 75 MHz of DSRC spectrum at 5.9 GHz to be used exclusively for V2V and V2R communications [2]. The primary purpose is to enable public safety applications that save lives and improve vehicular traffic flow. Private services are also permitted in order to lower the network deployment and maintenance costs to encourage DSRC development and adoption. The DSRC spectrum is divided into seven 10-MHz wide channels as shown in Figure 2. Channel 178 is the control channel, which is generally restricted to safety communications only. The two channels at the edges of the spectrum are reserved for future advanced accident avoidance applications and high-power public safety communication usages. The rest are service channels and are available for both safety and non-safety applications.

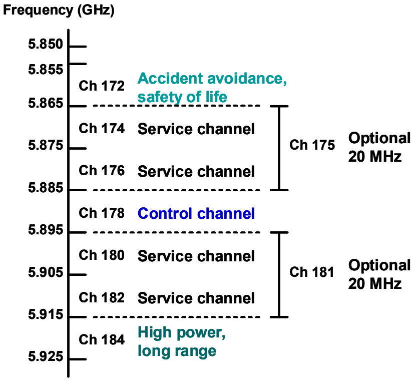

Figure 2. DSRC Channel assignment in North America

The IEEE has completed the standards IEEE P1609.1, P1609.2, and P1609.4 for vehicular networks and recently released them for trial use [4]. A fourth standard, P1609.3, is still under development. P1609.1 is the standard for the Wireless Access for Vehicular Environments (WAVE) Resource Manager. It defines the services and interfaces of the WAVE resource manager application as well as the message data formats. It provides access for applications to the other architectures. P1609.2 defines security, secure message formatting, processing, and message exchange. P1609.3 defines routing and transport services. It provides an alternative to IPv6. It also defines the management information base for the protocol stack. P1609.4 deals mainly with specification of the multiple channels in the DSRC standard.

The WAVE stack uses a modified version of the IEEE 802.11a, known as IEEE 802.11p [5], for its Medium Access Control (MAC) layer protocol. It uses CSMA/CA as the basic medium access scheme for link sharing and uses one control channel to set up transmissions, which then are carried over some transmission channels. The 802.11p PHY layer is expected to work in the 5.850 – 5.925 GHz DSRC spectrum in North America, which is a licensed ITS Radio Services Band in the United States. By using the OFDM system, it provides both V2V and V2R wireless communications over distances up to 1000 m, while taking into account the environment, that is, high absolute and relative velocities (up to 200 km/h), fast multipath fading and different scenarios (rural, highway, and urban). Operating in 10-MHz channels, it should allow data payload communication rates of 3, 4, 5, 6, 9, 12, 18, 24, and 27 Mb/s. By using the optional 20 MHz channels, it allows data payload capabilities up to 54 Mb/s.

As the overall DSRC communication stack between the link and application layers is being standardized by the IEEE 1609 Working Group, the overall DSRC communication architecture in the draft IEEE 1609 standard contains two parallel stacks: one for TCP/IP-based communications and the other for safety messaging.

For safety messaging, the amount of information to be transmitted is relatively small, but the transmission reliability as well as the latency and packet dissemination are of great importance.

3. CHALLENGES AND REQUIREMENTS IN VANET DESIGN

In the previous section we provided a brief overview of VANETs. In reality, a number of challenging issues must be addressed before VANETs can be successfully deployed. In the following we focus on two major issues in network layer design: security and support of existing and future VANET applications. In the rest of this section we first discuss the common requirements of security in VANETs and possible attacks on these networks. We then address the current and potential applications of VANETs.

3.1. SECURITY CHALLENGES IN VANETS

VANETs pose some of the most challenging problems in wireless ad hoc and sensor network research. In addition, the issue of security in VANETs is particularly challenging due to the unique features of the network, such as high-speed mobility of network nodes or vehicles and the shear size of the network. Specifically, it is essential to make sure that "life-critical safety" information cannot be inserted or modified by an attacker. While the system has to be capable of establishing the liability of drivers, it should protect their privacy as much as possible. It is obvious that any malicious user behavior, such as a modification and replay attack of the disseminated messages, could be fatal to other users.

In the past few years, considerable effort has been spent in research on VANET networking protocols and applications. However, research on security threats and solutions and reliability of VANETs started only recently, e.g., [6-11]. As suggested by the cited references, VANET security should satisfy the following requirements: message authentication and integrity, message non-repudiation, entity authentication, access control, message confidentiality, availability, privacy and anonymity, and liability identification.

Message Authentication and Integrity: Messages must be protected from any alteration and the receiver of a message must corroborate the sender of the message. But integrity does not necessarily imply identification of the sender of the message.

Message Non-Repudiation: The sender of a message cannot deny having sent the message.

Entity Authentication: The receiver is not only ensured that the sender generated the message, but in addition has evidence that the sender is a bona fide network node.

Access Control: Access to specific services provided by the infrastructure node and other node, is determined through local policies. As part of access control, authorization establishes what each network node is allowed to do.

Message Confidentiality: The content of a message is kept secret from those nodes that are not authorized to access it.

Availability: The network and applications should remain operational even in the presence of faults or malicious conditions. This requires not only secure but also fault-tolerant design, resilience to resource depletion attacks, as well as survivable protocols, which resume their normal operations after the removal of the faulty participants.

Privacy and Anonymity: Conditional privacy must be achieved in the sense that the user-related information has to be protected from unauthorized access, while the authorities should be able to access such information to look for witnesses in case of a dispute such as a crime/car accident scene investigation. The user-related information includes the driver name, license plate, speed, position, and traveling routes.

Liability Identification: Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes or the transportation system. As part of the "conditional privacy" requirement, the authorities should be able to determine the identities of message senders in the case of a dispute.

Several attacks have been identified that can be classified depending on the layer the attacker uses. At the physical and link layers the attacker can disturb the system either by jamming or overloading the communication channel with messages. Injecting false messages or rebroadcasting an old message is also a possible attack. The attacker can also steal or tamper with a car OBU 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 their positions. The same attacks can also be achieved using the application layer. In the following, we summarize the major vulnerabilities and security threats of VANETs.

Jamming: The jammer deliberately generates interfering transmissions that prevent legitimate communications within their reception range. In the VANET scenario, an attacker can relatively easily partition the network without compromising cryptographic mechanisms and with limited transmission power.

Impersonation: An attacker can electronically masquerade as an emergency vehicle to mislead other vehicles to slow down and yield. An adversary can also impersonate roadside units, spoofing service advertisements or safety messages. So an impersonator can be a threat. Message fabrication, alteration, and replay can all be used towards impersonation.

Privacy Violation: The collection of vehicle-specific information from overheard vehicular communications will be easy when VANETs are deployed. Then inferences on the personal data of drivers could be made, thus violating the privacy of the drivers.

Forgery: An attacker can forge and transmit false hazard warning information or other messages, which can rapidly contaminate large portions of the VANET coverage area. The correctness and timely receipt of application data is a major vulnerability.

In-Transit Traffic Tampering: A node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. Attackers can also replay messages, e.g., to illegitimately obtain services such as traversing a toll collection point. Tampering with in-transit messages may be simpler and more powerful than forgery attacks.

On-Board Tampering: The attacker may select to tinker with vehicle/driver-specific data, e.g., velocity, location, status of vehicle parts at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler for the attacker to replace or bypass the real-time clock or the wiring of a sensor in his vehicle rather than modifying the binary code implementation of the data collection and communication protocols.

3.2. VANET APPLICATIONS

Earlier we addressed the network design issue from the security perspective. In practice, a good system design also depends on understanding the applications that will be carried in the network. These applications not only have diverse requirements, such as bandwidth, delay, security, and reliability, but also exhibit different communication patterns, such as one-to-one, one-to-many, many-to-one, and many-to-many. However, most existing wireless network architectures cannot efficiently support such demands. Therefore, it becomes a major challenge to support and enable diverse applications and services.

Here we summarize the existing applications and several potential applications that have been proposed for VANETs. We also elaborate on the functions of each application that shall be provided in the MAC layer and the network layer, so as to fulfill the requirements of these applications.

VANETs would support life-critical safety applications, safety warning applications, electronic toll collection, Internet access, group communications, roadside service finder, etc.

Life-Critical Safety Applications: Intersection collision warning/avoidance and cooperative collision warning are examples of this category of applications. In the MAC layer, the life-critical safety applications can access the DSRC control channel and other channels with the highest priority. The messages can be broadcasted to all the nearby VANET nodes.

Safety Warning Applications: These applications include work zone warning and public safety vehicle signal priority. The differences between life-critical safety applications and safety warning applications are the allowable latency requirements. While the former usually require the messages to be delivered to the nearby nodes within 100 milliseconds, the latter can afford up to 1000 milliseconds of delay. In the MAC layer, the safety warning applications can access the DSRC control channel and the other channels with the 2nd highest priority. The messages can be broadcast to all the nearby VANET nodes.

Electronic Toll Collection (ETC): It is desirable to have each vehicle pay the toll electronically and without stopping when it passes through a toll collection point (a special RSU). The toll collection point will scan the electrical license plate stored in the OBU of the vehicle, and issue a receipt message to the vehicle, including the toll amount, time and location of the toll collection point. In the MAC layer, the electronic toll collection application should be able to access the DSRC service channels except the control channel with the 3rd highest priority. There should be a direct one-hop wireless link between the toll collection point and the vehicle.

Internet Access: Future vehicles will be equipped with this capability so that the passengers on the vehicles can connect to the Internet. In the MAC layer, the Internet access applications can use DSRC service channels except the control channel with the lowest priority compared with the previous applications. In the network layer, to support VANET Internet access, a straightforward method is to provide a unicast connection between the OBU of the vehicle and a RSU, which is assumed to be connected to the Internet.

Group Communications: Many drivers may share some common interests when they are on the same road driving in the same direction, making the case for a VANET group communications functionality. In the MAC layer, the group communications application can use DSRC service channels except the control channel with the lowest priority compared with the safety related applications and ETC. In the network layer, multicast is the key technology to support such application scenarios. Internet multicast has so far not been successful due to its complexity and, more importantly, because it requires global deployment, which is virtually impossible. In a VANET, however, since all nodes are located in a relatively bounded geographic area, implementing group communications becomes feasible.

Roadside Service Finder: Finding restaurants, gas stations, etc., in the nearby areas along the road are examples of such applications. A roadside service database will be installed in the local area and connected to the corresponding RSUs. In the MAC layer, the roadside service finder application can use DSRC service channels except the control channel with the lowest priority compared with the safety related applications and ETC. Each vehicle can issue a service finder request message that can be routed to the nearest RSU, and a service finder response message can be routed back to the vehicle.

In short, the application layer requirements must be addressed in the MAC layer and network layer design. In the next section we provide a network design framework to accommodate the above applications while providing adequate security.

4. NETWORK DESIGN FRAMEWORK

In this section we elaborate on a network design framework to address the security requirements in VANETs and meet the demands of existing and future applications discussed above.

4.1. COMPONENTS

In this framework there are two major components.

Application-Aware Control Scheme – To efficiently support different applications, the network control scheme shall be aware of the availability of different applications in the local area. In general, the application can be either located in a single node (RSU or OBU) or distributed in multiple nodes (RSUs and/or OBUs) in the VANET. To enable these applications, the servers must register the type and availability of applications to the control scheme. Moreover, the availability information shall be updated periodically or based on predefined events. Upon receiving these messages, the control scheme will also be responsible for distributing such message to nodes in the VANET.

Unified Routing Scheme Meeting Security Requirements – With the availability information of an application, a unified routing scheme shall be designed such that all the applications discussed in the last section shall be supported. The packets of a certain flow will be forwarded based on the specific requirements of that application and its security needs.

4.2. CASE STUDIES

We use the following cases as examples to illustrate the behavior of the framework.

Case 1 – All the OBUs and RSUs have been registered for the safety related applications (life-critical safety applications and safety warning applications) in the control scheme. The safety related application messages will be sent to all the nearby VANET nodes through broadcasting. Such messages do not have to be encrypted, as there are typically no confidentiality requirements, but they must satisfy the message authentication and integrity, message non-repudiation, and entity authentication requirements. Security mechanisms must be in place to defend against in-transit traffic tampering.

Case 2 – For the OBUs registered for electronic toll collection application in the control scheme, each ETC related message is carried over a one-hop wireless link between the toll collection point and the vehicle. The ETC related application messages need to satisfy the message confidentiality, message authentication and integrity, message non-repudiation, and entity authentication requirements.

Case 3 – Assume that each RSU has been registered as a gateway for Internet access in the control scheme. Now suppose a regular best-effort Internet access request from an OBU arrives at the control framework. A single-path unicast route between the OBU and a nearby RSU is established to carry the request. Notice that in such a scenario, the single path routing scheme cannot defend compromised OBUs in a multihop situation. Security mechanisms must be in place to defend against in-transit traffic tampering.

Case 4 – For the OBUs registered for group communications in the control scheme, multicast is used to realize the application. In such a case, security mechanisms must be in place to ensure the security of multicasting in VANETs. While the security of multicasting in MANET have been studied for a while, e.g., [12, 13], secure multicasting schemes for VANETs still need to be addressed.

Case 5 – For the OBUs registered for roadside service finder application in the control scheme, a unicast path is set up between the requesting OBU and a nearby RSU. Same security mechanisms need to be in place as those in Case 3.

5. ENABLING TECHNOLOGIES

To deploy the proposed framework, a number of key technologies must be addressed. In the rest of this section we discuss these issues, including security management, key management, secure routing and network coding.

5.1. SECURITY MANAGEMENT

In the proposed framework the security management scheme is a very important issue. Similar to [14], we consider a security management scheme responsible for monitoring the operation of the VANET and quickly identify possible security attacks and threats.

5.2. KEY MANAGEMENT

In addition to the MAC layer, key management is also important to the network layer. To provide a secure communication channel between any two nodes in a VANET, it is important to develop a key management scheme to establish a unique key for each session. Another potential research topic in key management is the key distribution scheme required for group communications. One simple solution for group communications is to utilize a single group key. However, such an approach is not efficient due to two factors: (i) the key will be exposed if a single group member is compromised and (ii) the communication overhead will become a large burden if a member can frequently join or leave the group, which can typically happen in a VANET with mobile nodes. More work needs to be done on key management for VANETs.

5.3. SECURE ROUTING AND NETWORK CODING

Secure routing has been discussed for MANETs in a number of previous studies (e.g., [15]). However, we note that none of these studies fully address the scenarios encountered in VANET applications discussed in the previous section. The emerging network coding techniques can be applied to address routing security, because they can provide the optimum solution and reduce the computational complexity for many problems [16]. Our recent work reveals that one can incorporate the security and reliability requirements into network coding design. With the proposed design guidelines for MANETs [17], we can see that the network coding approach can be utilized to improve both the security and the reliability as follows. First, the network coding scheme can be designed in a way that none of the intermediate nodes can decode the original message. In this manner, an adversary may not be able to overhear the whole message unless it is near to the source or destination of a connection. Second, the coding scheme can be designed such that the destination can still correctly decode the original message even if parts of the data are dropped in the network or are modified deliberately by intermediate nodes. We will explore the details of the netwok coding schemes appropriate for VANET design in future work.

6. CONCLUSIONS

Vehicular ad hoc networking is a promising wireless communication technology for improving highway safety and information services. In this paper we proposed a secure and application-oriented network design framework in which both security concerns and the requirements of potential VANET applications are taken into account. We also listed several enabling technologies for the design framework. They include security management, key management, secure routing and network coding. We believe that our study can provide a guideline for the design of a more secure and practical VANET.

REFERENCES

[1] U.S. Department of Transportation, Intelligent Transportation Systems (ITS) Home, http://www.its.dot.gov/index.htm

[2] Dedicated Short Range Communications (DSRC) Home. http://www.leearmstrong.com/DSRC/DSRCHomeset.htm

[3] Crash Avoidance Metric Partnership, "Vehicle Safety Communication Project Final Report", available through U.S. Department of Transportation.

[4] IEEE Draft P1609.0/D01, February 2007.

[5] IEEE Draft P802.11p/D2.0, November 2006.

[6] P. Papadimitratos, V. Gligor, J-P. Hubaux, "Securing Vehicular Communications – Assumptions, Requirements, and Principles", Proceedings of the Workshop on Embeded Security on Cars (ESCAR) 2006, November 2006.

[7] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, October 2006.

[8] Tim Leinmuller, Elmar Schoch, and Frank Kargl, "Position Verfication Approaches for Vehicular Ah Hoc Networks", IEEE Wireless Communications, October 2006.

[9] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya, "Architecture for Secure and Priviate Vehicular Communications", Proceedings of the 7th International Conference on ITS Telecommunications, June 2007.

[10] Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, Vol.15, No.1, pp.39-68, 2007.

[11] Tim Leinmuller, Elmar Schoch, and Christian Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks", Proceedings of Forth Annual Conference on Wireless on Demand Network Systems and Services, 2007.

[12] Haibing Mu, Yun Liu, and Changlun Zhang, "A Composite Multicast Key Management Scheme for MANET", Proceedings of 6th International Conference on ITS Telecommunications, Page(s):794 – 797, June 2006.

[13] Tzu-Chiang Chiang; Yueh-Min Huang, "Group keys and the multicast security in ad hoc networks", Proceedings of 2003 International Conference on Parallel Processing Workshops, Page(s):385 - 390, 6-9 Oct. 2003.

[14] N. Ben Salem, and J.-P. Hubaux, "Securing wireless mesh networks", IEEE Wireless Communications, Vol.13, No.2, pp.50-55, April 2006.

[15] Hongmei Deng, Wei Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, Vol.40, No.10, pp.70-75, October 2002.

[16] D. S. Lun, N. Ratnakar, M. Medard, R. Koetter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, "Minimum-cost Multicast over Coded Packet Networks", IEEE Transactions on Information Theory, Vol.52, No.6, pp.2608-2623, June 2006.

[17] Kejie Lu, Shengli Fu, and Yi Qian, "On the Design of Future Wireless Ah Hoc Networks", Proceedings of IEEE GLOBECOM'2007, November 2007.