IJCSMS International Journal of Computer Science & Management Studies, Special Issue of Vol. 12, June 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Apply Different Techniques to Face Vehicular Ad-Hoc Network Challenges for Making Secure Systems

Parveen Kumar

Research Scholar, CMJ, Shillong, Meghalaya (India)

Abstract

In this paper, the concept of VANET is discussed in detail. The different concepts used in VANET are explained with very good style. The applications of VANET are also discussed here. In the near future, most new vehicles will be equipped with short range radios capable of communicating with other vehicles or with highway infrastructure at distances of at least one kilometer. The radios will allow new applications that will revolutionize the driving experience, providing everything from instant, localized traffic updates to warning signals when the car ahead abruptly brakes. While resembling traditional sensor and ad hoc networks in some respects, vehicular networks pose a number of unique challenges. The different challenges of VANET are explained and explained in detail in this paper.

Keywords: *VANET, MANET, VANET Challenges, VANET Applications, VANET Technology.*

Introduction

A Vehicular Ad-Hoc Network 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 meters 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.

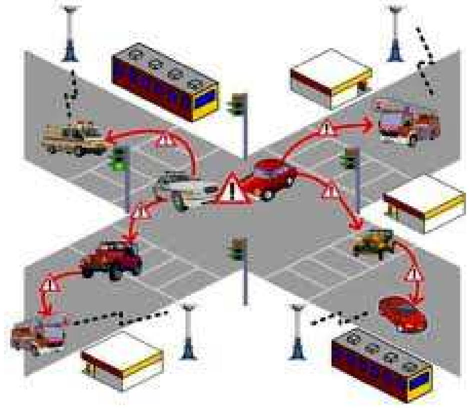

Figure 1: VANET Demonstration

Applications

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 several benefits to organizations of any size. 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. GPS and navigation systems can benefit, as they can be integrated with traffic reports to provide the fastest route to work. 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. It would also allow for free, VoIP services such as Google Talk or Skype between employees, lowering telecommunications costs. Future applications could involve cruise control making automatic adjustments to maintain safe distances between vehicles or alerting the driver of emergency vehicles in the area.

To support message differentiation in VANET, IEEE 802.11e standard is incorporated in vehicular communication.

Technology

In VANET, or Intelligent Vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking. In VANET integrates on multiple ad-hoc networking technologies such as Wi-Fi IEEE 802.11p, WAVE IEEE 1609, WI-MAX IEEE 802.16, Bluetooth, IRA, and ZIG-BEE for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well as methods to track the automotive vehicles.

In VANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and TELE-MATICS.

Vehicular Ad-hoc Networks are expected to implement a variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are Cellular, Satellite, and WI-MAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).

As envisioned in ITS, vehicles communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC), the optimal goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities.

Mobile ad hoc network

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose".

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptops and 802.11/Wi-Fi wireless networking, have made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

Classification of Attacks on MANETs

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan on individual layer are as under:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding

- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

Intelligent vehicular ad-hoc network

Intelligent vehicular ad-hoc networks (In VANETs) use Wi-Fi IEEE 802.11p (WAVE standard) and WI-MAX IEEE 802.16 for easy and effective communication between vehicles with dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track automotive vehicles. In VANET is not foreseen to replace current mobile (cellular phone) communication standards.

"Older" designs within the IEEE 802.11 scope may refer just to IEEE 802.11b/g. More recent designs refer to the latest issues of IEEE 802.11p (WAVE, draft status). Due to inherent lag times, only the latter one in the IEEE 802.11 scope is capable of coping with the typical dynamics of vehicle operation.

Automotive vehicular information can be viewed on electronic maps using the Internet or specialized software. The advantage of WiFi based navigation system function is that it can effectively locate a vehicle which is inside big campuses like universities, airports, and tunnels. In VANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city.

Communication capabilities in vehicles are the basis of an envisioned In VANET or intelligent transportation systems (ITS). Vehicles are enabled to communicate among themselves (vehicle-to-vehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial because V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available.

Providing vehicle–vehicle and vehicle–roadside communication can considerably improve traffic safety and comfort of driving and traveling. For communication in vehicular ad hoc networks, position-based routing has emerged as a promising candidate. For Internet access, Mobile IPv6 is a widely accepted solution to provide session continuity and reach ability to the Internet for mobile nodes. While integrated solutions for usage of Mobile IPv6 in (non-vehicular) mobile ad hoc networks exist, a solution has been proposed that, built upon on a Mobile IPv6 proxy-based architecture, selects the optimal communication mode (direct in-vehicle, vehicle–vehicle, and vehicle–roadside communication) and provides dynamic switching between vehicle–vehicle and vehicle–roadside communication mode during a communication session in case that more than one communication mode is simultaneously available.

Currently there is ongoing research in the field of In VANETs for several scenarios. The main interest is in applications for traffic scenarios, mobile phone systems, sensor networks and future combat systems. Recent research has focused on topology related problems such as range optimization, routing mechanisms, or address systems, as well as security issues like traceability or encryption. In addition, there are very specific research interests such as the effects of directional antennas for In VANETs and minimal power consumption for sensor networks. Most of this research aims either at a general approach to wireless networks in a broad setting or focus on an extremely specific issue.

Vehicular Network Challenges

Vehicular network challenges include technical problems like key distribution as well as more abstract difficulties, such as the need to appeal simultaneously to three very different markets.

Authentication versus Privacy

In a vehicular network, we would like to bind each driver to a single identity to prevent Sybil or other spoofing attacks. For instance, in the congestion avoidance scheme, we would like to prevent one vehicle from claiming to be hundreds in order to create the illusion of a congested road. Strong authentication also provides valuable forensic evidence and allows us to use external mechanisms, such as traditional law enforcement, to deter or prevent attacks on vehicular networks. However, drivers value their privacy and are unlikely to adopt systems that require them to abandon their anonymity. For example, if we try to prevent spoofing in a manner that reveals each vehicle's permanent identity, then we may violate drivers' privacy expectations. Balancing privacy concerns with security needs will require codifying legal, societal and practical considerations. Most countries have widely divergent laws concerning their citizens' right to privacy. Since most vehicle manufacturers operate in multinational markets, they will require security solutions that satisfy the most stringent privacy laws, or that can be customized to meet their legal obligations in each market. Authentication schemes must also weigh societal expectations of privacy against practical considerations. Most drivers would resent a system that allows others to track their movements, but from a practical perspective, vehicles today are only partially anonymous. Each vehicle has a publicly displayed license plate that uniquely identifies it (and identifies the owner of the car, given access to the appropriate records). Thus, individual drivers have already surrendered a portion of their privacy while driving. Ideally, a secure vehicular network would build on these existing compromises instead of encroaching any further upon a driver's right to privacy.

Availability

For many applications, vehicular networks will require real-time, or near real-time, responses as well as hard real time guarantees. While some applications may tolerate some margin in their response times, they will all typically require faster responses than those expected in traditional sensor networks, or even ad hoc networks. However, attempts to meet real-time demands typically make applications vulnerable to Denial of Service (DoS) attacks. In the deceleration application, a delay of even seconds can render the message meaningless. The problem is further exacerbated by the unreliable communication layer, since one potential way to cope with unreliable transmission is to store partial messages in the hopes that a second transmission will complete the message. Current plans for vehicular networks rely on the emerging standard for dedicated short-range communications (DSRC) [2], based on an extension to the IEEE 802.11 technology. Yin et al. provide a detailed, low-level evaluation of the performance of a simulated DSRC network and find that while the current DSRC standard provides an acceptable latency, the reliability is still lacking. According to their simulations, on average, only 50-60% of a vehicle's neighbors will receive a broadcast message. Since vehicles moving in opposite directions will remain within communications range for only a few seconds, opportunities to retry a broadcast will be limited. On a positive note, DSRC features a high data rate.

Low Tolerance for Errors

Many applications use protocols that rely on probabilistic schemes to provide security. However, given the life-or-death nature of many proposed vehicular applications, even a small probability of error will be unacceptable. In fact, since the U.S. Bureau of Transportation Statistics estimates that there are over 200 million cars in the U.S. , even if only 5% of vehicles use an application that functions correctly 99.99999% of the time, the application is still more likely to fail on at least one vehicle than function correctly on all vehicles. Thus, to provide the level of guarantees necessary for these scenarios, applications will have to rely on deterministic schemes or probabilistic schemes with security parameters large enough to make the probability of failure infinitesimally small. Furthermore, for many applications, security must focus on prevention of attacks, rather than detection and recovery. In an ad hoc network, it may suffice to detect an attack and alert the user, leaving recovery and clean-up to the humans. However, in many safety related vehicular network applications, detection will be insufficient, since by the time the driver can react, the warning may be too late. Instead, security must focus on preventing attacks in the first place, which will require extensive foresight into the types of attacks likely to occur.

Mobility

Traditional sensor networks frequently assume a relatively static network, and even ad hoc networks typically assume limited mobility, often focusing on handheld PDAs and laptops carried by users. For vehicular networks, mobility is the norm, and it will be measured in miles, not meters, per hour. Also, the mobility patterns of vehicles on the same road will exhibit strong correlations. Each vehicle will have a constantly shifting set of neighbors, many of whom it has never interacted with before and is unlikely to interact with again. The transitory nature of interactions in a vehicular network will restrict the utility of reputation-based schemes. For example, rating other vehicles based on the reliability of their congestion reports is unlikely to prove useful; a specific driver is unlikely to receive multiple reports from the same vehicle. Furthermore, since two vehicles may only be within communication range for a matter of seconds, we cannot rely on protocols that require significant interaction between the sender and receiver.

Key Distribution

Key distribution is often a fundamental building block for security protocols. In vehicular networks, distribution poses several significant challenges. First, vehicles are manufactured by many different companies, so installing keys at the factory would require coordination and interoperability between manufacturers. If manufacturers are unable or unwilling to agree on standards for key distribution, then we could turn to government-based distribution. Unfortunately, in the U.S., most transportation regulation takes place at the state level, again complicating coordination. The federal government can impose standards, but doing so would require significant changes to the current infrastructure for vehicle registration, and thus is unlikely to occur in the near future. However, without a system for key distribution, applications like traffic congestion detection may be vulnerable to spoofing. A potential approach for secure key distribution would be to empower the Department of Motor Vehicles (DMV) to take the role of a Certificate Authority (CA) and to certify each vehicle’s public key. Unfortunately, this approach has many shortcomings. First, assuming the role of a CA is a challenging operation which is not in line with the DMV’s current functionality. Extensive anecdotal evidence suggests that even specialized CAs offer questionable security against dedicated attackers trying to obtain a certificate for another institution/entity. Second, vehicles from different states or different countries may not be able to authenticate each other unless vehicles trust all CAs, which reduces security. Finally, certificate based key establishment has the danger of violating driver privacy, as the vehicle’s identity is revealed during each key establishment.

Incentives

Successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers, and the government, and reconciling their often conflicting interests will prove challenging. For example, law-enforcement agencies would quickly embrace a system in which speed-limit signs broadcast the mandated speed and vehicles automatically reported any violations. Obviously, consumers would reject such intrusive monitoring, giving vehicle manufacturers little incentive to include such a feature. Conversely, consumers might appreciate an application that provides an early warning of a police speed trap. Manufacturers might be willing to meet this demand, but law-enforcement is likely to object.

Bootstrap

Initially, only a small percentage of vehicles will be equipped with DSRC radios and little infrastructure will exist

to support them. Thus, in developing applications for vehicular networks, we can only assume that a few other vehicles are able to receive our communications, and the applications must provide benefits even under these limited conditions (with increasing benefits as the number of DSRC-equipped vehicles increases).

Related Work

The VANET challenges must be examined carefully and different technologies must be applied to improve system security. Few researchers have examined the problem of security in vehicular networks. Zarki et al. present the DAHNI (Driver Ad Hoc Networking Infrastructure) system for providing driver assistance. They show how they can use a vehicular network to track nearby vehicles and report potential hazards to the driver. In contrast to their work, we argue that privacy and key establishment are two vital issues that require additional work before vehicular networks can be securely deployed. Hubaux et al. describe some of the attacks vehicular networks may face and propose a mechanism for providing secure positioning; they also suggest the congestion detection application discussed in this work. In another work, Raya and Hubaux consider the issues involved with key management for vehicular networks, as well as the use of anonymous public keys. They also analyze the feasibility of using a PKI to support the security requirements of vehicular networks. The different methods must be used to solve the challenges. And new techniques must be applied to face VANET challenges.

To Resolve VANET Challenges

In this section, we present the methods to solve the considerations of security when the LTE is used in VANET. To provide VANET communication, the cost and time for constructing the infrastructure will be needed. Thus, the using of LTE in VANET is anticipated that the commercialization of VANET is activated more quickly. The Table I shows the solution in LTE for the unresolved issues of the security in VANET.

Figure2: Pictorial VANET Information

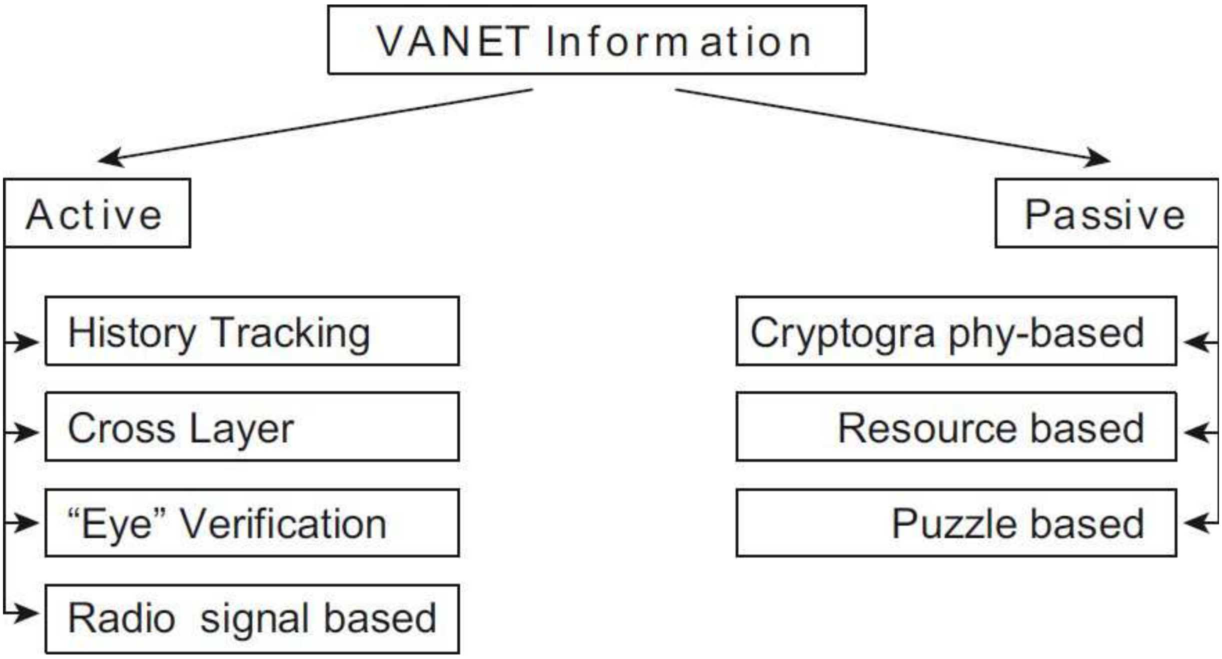

Table I

The Solutions to Resolve the Security Considerations of VANET Through The LTE

Sr. No.	Consideration of the VANET Security	Solution in the LTE
1	When the RSU is not sufficiently installed	The HSS sends the IMSI and LTE key to MME when the device is connected in LTE
2	protection by the exposure of ID	Alternates the IMSI by generating the GUTI that the temporary ID

1) According to existing studies about VANET, the key can be generated by RSU. However, the key generation cannot be provided by RSU because the density of RSU placement has not yet been determined. Therefore, if the LTE is used, this problem will be solved through the Authentication and Key Agreement (AKA) protocol. The authentication protocol performs an authentication of device through the key information sent from Home Subscriber Server (HSS). The HSS has the International Mobile Subscriber Identity (IMSI) and the master key of the EPS called LTE key. It sends the key information to Mobility Management Entity (MME) for authentication of the users' device. Even though the RSU is not installed, the key generation is able to make use through an allowed key exchange mechanism that the AKA. Therefore, the LTE is anticipated that it is a suitable for VANET by generating the key through the AKA authentication protocol.

2) In LTE, the identifier is used to GUTI (Globally Unique Temporary Identifier) instead of the IMSI for solving the problem of privacy protection. When the device initially connects, it requests the registration as IMSI. And the GUTI is allocated from the MME. After this, if the device re-connects in other networks it can be solved the problem of privacy protection by using the GUTI.

Conclusion

The Protocols which are used to face VANET challenges must be secure and powerful. To make vehicular networks viable and acceptable to consumers, we need to establish secure protocols that satisfy the stringent requirements of this application space. Designing secure protocols is complicated by the seemingly conflicting requirements of consumers, automobile manufacturers, and government, particularly when trying to provide strong vehicle identification while protecting driver privacy. Fortunately, the properties of vehicular networks provide new approaches for these challenges, allowing us to develop new primitives based on, for example, the entanglement of vehicle trajectories and the use of simple reanonymizers. We anticipate that the challenges outlined in this paper and the new opportunities for solutions in vehicular networks will encourage other researchers to start studying this important and exciting research area.

References

[1] Zang Li, Wade Trappe, Yanyong Zhang, and Badri Nath. Robust statistical methods for securing wireless localization in sensor networks. In Proc. of IPSN, April 2005.

[2] Donggang Liu, Peng Ning, and Wenliang Kevin Du. Attack-resistant location estimation in sensor networks. In
Proc. of IPSN, April 2005.

[3] PKI Forum. Verisign fraudulent certificates. http://www.pkiforum.com/resources/ verisigncerts.html, Accessed on January 2005.

[4] Bartosz Przydatek, Dawn Song, and Adrian Perrig. SIA: Secure information aggregation in sensor networks. In Proc. of ACM Conference on Embedded Networked Sensor Systems (SenSys), 2003.

[5] Maxim Raya and Jean-Pierre Hubaux. The security of vehicular ad hoc networks. In Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 2005.

[6] Arvind Seshadri, Adrian Perrig, Leendert van Doorn, and Pradeep Khosla. SWATT: Software-based attestation for embedded devices. In Proc. of IEEE Symposium on Security and Privacy, May 2004.

[7] Trusted Computing Group. Trusted platform module main specification, Part 1:design principles, Part 2: TPM structures, Part 3: Commands.
http://www.trustedcomputinggroup.org, October 2003. Version 1.2, Revision 62

[8] U.S. Department of Transportation, Bureau of Transportation Statistics. Transportation Statistics Annual Report, 2003.

[9] Jijun Yin, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty.
Performance evaluation of safety applications over DSRC vehicular ad hoc networks In Proc. of ACM workshop on Vehicular Ad Hoc Networks (VANET), 2004 [23] Magda El Zarki, Sharad Mehrotra, Gene Tsudik

[10] Jan Camenisch and Anna Lysyanskaya. Efficient non-transferable anonymous multi-show credential systemwith optional anonymity revocation. In Proc. of Advances in Cryptology - Eurocrypt, 2001.