International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 2 Issue 7, July-2013, pp: (5-7), Available online at: www.erpublications.com

Data security issues in VANET

Er. Anurag Sharma[1], Dr. Yashpal Singh[2]
[1]Reseach Scholar, Bhagwant University, Ajmer
[2]Head, Dept. of Computer Science, BIET, Jhansi

ABSTRACT: Vehicular Adhoc Network (VANET) is becoming a focusing point in researcher communities. Due to various kinds of applications including safety driving, parking lot finder, real-time route finder, it is becoming popular in recent years. Safety applications based on vehicular network communication are a major aspect of future innovation. VANET provides vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I)[1] communication. These applications are foreseen to improve traffic safety considerably, and to enable innovative infotainment applications and business models. Security is concerned with protection against malicious manipulation of IT systems and plays an important role when designing and implementing such applications. VANET applications need security functionality in order to protect the driver, the manufacturer, component suppliers, and service providers. Safety applications must be protected to avoid malicious manipulation, potentially causing harm to the vehicle driver, and commercial applications must be protected to prevent loss of revenue. In this paper we present Security issues of providing data security in VANET followed by attacker and cryptographic protocols.

Keywords: Adhoc Network, Security issues, V2V, V2I, Vanet.

Introduction

The majority of software and hardware systems in current vehicles are not protected against tampering. One reason for this is that past vehicle IT systems provided little incentive for malicious manipulation, there was little gain in compromising a single vehicle and such a compromise did not affect other vehicles. Additionally, security tends to be an afterthought in any IT system as evidenced by several case studies including the development of the internet. VANET will in most situations not have permanent connections to a fixed infrastructure such as Internet. Therefore, critical issues such as privacy and control of the network need to be handled in a different way from PC-based networks. Further, it might be costly to establish the necessary Internet-like organizational aspects in VANET since these traditional approaches cannot simply be reproduced.

State of the Art

VANET are emerging research area, both in academics and in industry. There are many ongoing projects, while the early projects mainly considered the feasibility of VANET, now the security aspects are also added. The vehicle safety communications consortiums worked on security solutions that strongly influenced the IEEE P1609.2 standard-Consortium (2006); IEEE(2006). Currently the main industrial projects in USA are performed by the vehicle infrastructure integration initiative as well as by the Vehicle safety communications2 consortium in the vehicle safety communications application project. The standard defines the over-the-air message format for VANET and currently suggests attaching an ECDSA (elliptic curve digital signature algorithm) digital signature to each message. Futhermore, either a certificate or a certificate digest needs to be attached to each message .The standard also defines message content encryption as well as the format of certificate revocation lists. A Common approach to security is to apply the IEEE P1609.2 standard regarding message authentication and assume a deployed public key infrastructure. Privacy protection is designed on top by equipping each vehicle with multiple certificates, and changing certificates regularly.

Issues in Data Security

Data security in the personal computer is well researched, although large scale devastating attacks still occur. Security in vehicular networks poses different security threats and also has different requirements.

A. Risk Potential: Due to close coupling with the physical environment, the risk involved in vehicular networks can be much larger than the risk in conventional IT applications. The hacking of an automotive safety-critical application system can have far more immediate physical consequences than hard disk data destroyed by a computer virus.

B. Financial assets: There are a variety of promising applications based on vehicular communication that involve financial aspects, such as digital infotainment content, location based services, and built-in-automotive payment functions (e.g road tolling). Tampering with non-safety applications imposes far less risk of being prosecured than does tampering with safety applications, whereas in the second case, police authorities might heavily pursue any illegal modifications, in the first case, industry needs to defend itself.

C. Cost: In the automotive domain there is little willingness by vehicle buyers to spend money for security. Therefore, security solutions need to be especially cost efficient.

D. Usability: Vehicle driver expects not to deal with electronic issues, and certainly not with a security configuration. If adjustments by external entities are necessary, then they should only be implemented during a workshop visit or by automatic updates via VANET communication channels.

E. Mobility: Contact with other vehicles might be limited to only a few seconds such that establishing a secure channel cannot take too long.furthermore,the communication quality might be affected by the velocity of vehicles, resulting in packet loss.

F. Privacy: Today, almost all movement patterns of an individual can be traced by tracking their vehicle. Further privacy concerns might be involved in financial transactions carried out on VANET. Privacy is both a technical and an organizational matter.

G. Reliability: Unauthorized software updates can lead to serious safety and liability issues, and to financial loss.

H. Market penetration: Vehicles are expected to be equipped with VANET radios over the next decade. However it is expected to take a considerable time until all vehicles are VANET enabled. It is also unclear to what degree or when there will be supporting infrastructure available in the form of roadside units (RSUs). Therefore, potential security solutions should work with a low penetration rate of radio-enabled vehicles and small number of deployed RSUs.

I. Legislation: Legislation might requires both technical solutions and organizational mechanisms for the vehicles and for the supporting infrastructure

Attacher Model

A. Adversaries: Attacker have full access to a generic DSRC radio. Therefore adversaries are able to listen to the channel and read all messages in their reception range. Attachers are able to actively broadcast new messages, replay messages, and tunnel messages over another channel to another location. An attacker might act rationally or purely maliciously but is bound by financial resources and available manpower.

B. Road coverage: The attacker is able to cover a certain percentage of the road network. while a basic attacker has control of a single DSRC radio and covers a range of at most 1000 meters, an organized attacker might deploy a grid of several dozens or hundreds of DSRC radios.

C. Resources: Attackers have a certain limited budget at their disposal. The budget is described in terms of financial and human resources. Furthermore; the adversary needs tools to mount attacks.

Cryptographic Protocols

A. Certificate verification: Vehicles and RSUs exchange certificates before starting secure communication. All protocols require the verification of certificates before continuing. Therefore, a general method of CERT_CHECK to verify certificates. The algorithm requires single signature verification or none at all. We assume that browsing the CRL and storing the certificate requires negligible time.

B. Encryption: It is one of the core security services to provide confidentiality and avoid eavesdropping. Encryption can be provided by both symmetric and asymmetric cryptography.

C. Key agreement: Key agreement allows two parties to agree on a symmetric key by interacting over an insecure channel in such a way that an eavesdropper is not able to derive the key. Therefore, public-key methods are used.

D. Authentication: Authentication is the core security requirement in VANET. Authentication provides message integration in order to avoid message manipulation. Basically, all applications in a VANET require authentication. Authentication comes in different flavors: message authentication versus entity authentication (identification), broadcast, pairwise, and group wise authentication.

E. Identification: Unlike message authentication, identification (or entity authentication) enables a claimer to prove knowledge of a secret that only the claimer knows, thus proving its identity. An identification process needs to include timeliness in order to prove that the claimer definitely has knowledge of the secret.

F. Secure positioning: VANET assume that secure positioning will be provided by GPS, which provides both time and location for all vehicles worldwide. Today vehicles usually have a GPS receiver built in for navigation systems such that it can be concurrently used by VANET at little additional cost. GPS depends on line-of-sight communication with satellite and therefore does not work properly in certain settings such as in tunnels or in an urban canyon like manhattan. Based on these observations, suggest an approach based on RSUs that applies distance bounding. RSUs are assumed to be trustworthy and they determine a vehicles location. Distance bounding determines an upper bound for the distance between verifier and claimant.

G. Identification of misbehaving nodes: Identification of misbehaving nodes and revocation of those nodes is a crucial issue in VANET. Even if there is effective mechanism in place to revoke vehicles, misbehaving vehicles first need to be identified. Vehicles can misbehave in variety of ways. They might malfunction, their sensor input might be manipulated, or their cryptographic keys might be extracted in order to forge messages.

Conclusion

In this paper we have given an overview of challenges for VANET security, and described various security issues of data security and the applications models which describe various requirements for safety and non-safety applications. We expect that there will be only a few VANET worldwide, but each will be country or even continent-wide and will compromise several hundred million nodes. We believe it is infeasible to design, implement, and deploy a security and application system in vehicles that will run for the entire vehicle lifetime without adaptation. Therefore secure updating of application and security software should be included from initial deployment.

Acknowledgement

The Authors are supported by many books and references and journals as mentioned below. Besides this, we are thankful to some faculties' members from different organization.

References

[1]. K. M. Passino, "Biomimicry of bacterial foraging for distributed optimization and control," IEEE Control Syst Mag. USA, vol. 22, pp. 52- 67, June 2002.

[2]. V. Naumov, R. Baumann, and T. Gross, "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," Proc. ACM the 7th ACM MobiHoc' 06, Florence, Italy, May 22-25, 2006.

[3]. N. Wisitpongphan, F. Bai, P. Mudalige, and O. K. Tonguz, "On the routing problem in disconnected vehicular ad hoc networks," IEEE the 26th INFOCOM'07, Anchorage, Alaska, USA, May 6-12, 2007.

[4]. International journal of Network and Mobile Technologies, vol 2 number 1, january-june 2011, ISSN: 2230-8903.

[5]. M. Nekovee, and B. Bjarni Bogason, "Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks," IEEE the 65th VTC'07-spring, Dublin, Ireland, April 22-25, 2007.