A Survey of Security in Vehicle to Vehicle Communications

S. Christal Anand
Faculty, Lord Jegannath College of Engineering and Technology, Tamilnadu, India
christalanands@gmail.com

Abstract—Vehicular Ad hoc networks are latest research area in the Network filed. This Vehicular Network work with higher level mobility vehicles that is used for secured communication among these vehicles.As the number of vehicles grows the trust between them should also be maintained for the flexible communication. Consequently Security is a forebear to any protected communications in these networks. In this paper, Survey of VANETs Security has different types of security scheme that has been discussed. In addition providing a survey of related several open security problems.

Keywords— VANETs, Authentication, Public Key infrastructure, Location Privacy, Encryption, Safety

I. INTRODUCTION

Vehicular ad hoc networks (VANET) are the most widely used realization of mobile ad hoc networks (MANET). VANET have wide applications in Automobile Industry including Intelligent Transportation System (ITS) to avoid collision and route vehicles efficiently to improve safety. VANET includes vehicle to vehicle (V2V) communication and vehicle to road side communication. [2]The road to a successful introduction of vehicularcommunications has to pass through the analysis of potentialsecurity threats and the design of a robust security architectureabilities to cope with these threats. [3]

V2V communication technologiesamong the variety of wireless technologies for ITS applications, DSRC (Dedicated Short Range Communications, aka IEEE 802.11p) and IEEE 1609 (aka WAVE:Wireless Access in Vehicular Environments) are the emergingones for direct V2V communications.Direct V2V communications bring stringent requirementsforthehigher level network protocols, such as highly ad hocconnectivity, scaling to a large number of vehicles, and independently from infrastructure support. Unfortunately as we will explain in Section II-A, the current TCP/IP implementations are a poor fit to such direct V2V communications. [4]

VANET have received increased attention as the potential technology to enhance active and preventive safety on the road, as well as travel comfort. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Generally, attacks cause anomalies to the network functionality. A secure VANET system, while exchanging information should protect the system against unauthorized message injection, message alteration, eavesdropping. Authentication schemes that are used to reduce the overhead in authentication, when roaming - proxy re-encryption scheme and new proxy re encryption scheme is reviewed in detail. A comparison between the two schemes is done, which shows that the privacy can be maintained better by using new proxy re encryption. [5]

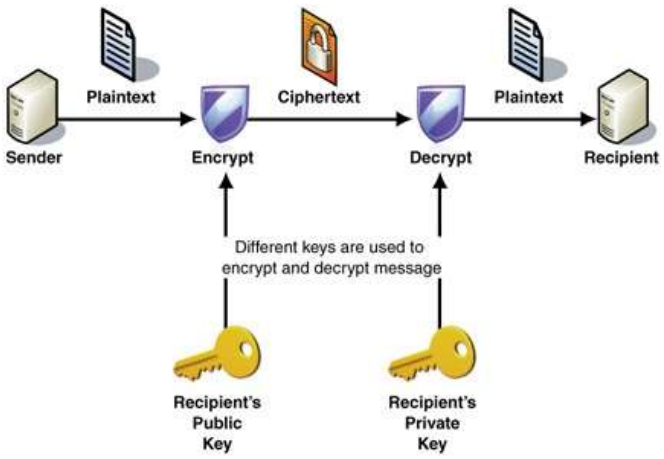
Vehicular networks are organized with high-mobility vehicles, which are a challenge to key agreement and secured communicationbetween vehicles; hence, efficient cryptography schemes for lightweight ciphers are essential. Many security schemes for vehicular networks particularly take the secure propagation of traffic-related information into account. Group communication is desirable in vehicular networks, while groups of friends drive the vehicles to travel together. [1]

Vehicular ad hoc networking is an important component of Intelligent Transportation Systems. The main benefit of vehicular ad hoc network (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. Dedicated Short Range Communications (DSRC) are a key enabling technology for VANET applications and services. There are many challenges that must be addressed before VANETs can be successfully deployed. Among these challenges is designing of security mechanisms to secure VANETs against abuse, and designing of efficient medium access control (MAC) protocols so that safety related and other application messages can be timely and reliable disseminated through VANETs. [7] Vehicular ad hoc networking is a promising Vehicular communication technology for improving highway safety and information services. [7] In this paper, we discuss about existing security schemes and their needs of the improvement of VANETs.

II. Security On Vehicular Ad Hoc Networks

A. Public-key infrastructure

Public-key infrastructure (PKI) can protect vehicular communication using the public key cryptography. [1] Vehicles have to apply for a valid key pair, certificated by trusted third party such as Certificate Authorities (CA). In the V2I mode, vehicles connect to the PKI services through roadside RSUs, since RSUs have always supported wireless and wired techniques. Basically, one participantrepresented as a mobile vehicle or a fixed RSU should have an individual public/private key pair with the certificate for authentication, communication confidentiality and integrity in VANETs. [1] The asymmetric cryptography is not suitable to secure group communication, while one vehicle wants to transmit confidentially huge amount of data such as digital map-based information and multimedia to other vehicles in a group. Additionally, unstable V2V links cannot endure long periods of group communication. With the aid of RSUs in the V2Imode, the scattered vehicles can keep connections during a group communication session. Using a symmetric key to secured group communication improves the performance of delivering confidential data by comparing the data protected by all individual asymmetric-based keys of all participants. [1]



Advantages of the PKI Approach

1. PKI is a standards-based technology.
2. It allows the choice of trust provider.
3. It is highly scalable. Users maintain their own certificates, and certificate authentication involves the exchange of data between client and server only. This means that no third party authentication server needs to be online. There is thus no limit to the number of users who can be supported using PKI.

4. PKI allows delegated trust. That is, a user who has obtained a certificate from a recognized and trusted certificate authority can authenticate himself to a server the very first time he connects to that server, without having previously been registered with the system.
5. Although PKI is not notably a single sign-on service, it can be implemented in such a way as to enable single sign-on.

Components of a Public Key Infrastructure

PKI Component	Explanation
Digital certificates	Digital "identities" issued by trusted third parties that identify users and machines. They may be securely stored in wallets or in directories.
Public and private keys	PKI for secure communications, based on a secret private key and a mathematically related public key
Secure sockets layer (SSL)	An Internet-standard security protocol
Certificate Authority (CA)	Acts as a trusted, independent provider of digital certificates

There are types of secure Credentials

- Certificate based Authentication in PKI
- Storing secure credentials with PKI
- Single Sign-On using PKI
- Network Security Using PKI

Certificate based Authentication in PKI

Establishing user identity is of primary concern in distributed environments; otherwise, there can be little confidence in limiting privileges by user. Passwords are the most common authentication method in use, but for particularly sensitive data, you need to employ stronger authentication services. This section describes:

Certificate Authorities:

A certificate authority (CA) is a trusted third party that certifies that other entities--users, databases, administrators, clients. When it certifies a user, the certificate authority verifies the user's identity and grants a certificate, signing it with the certificate authority's private key. The certificate authority has its own certificate and public key, which it publishes, as well as a private key, which is securely maintained. Servers and clients use the CA's root certificate to verify signatures that the certificate authority has made.

Certificate

A certificate is like an electronic passport that proves the identity of a user or device that seeks to access the network. The certificate ensures that the entity's information is correct and that the public key actually belongs to that entity. A certificate is created when an entity's public key is signed by a trusted identity (a certificate authority)

Digital Signatures and Hashing Algorithms

Digital signatures and hashing algorithms accomplish two of the four PKI goals. They ensure the integrity of the information being sent, and they solve the nonrepudiationproblem by not allowing the sender to dispute that he was the originator of the sent message. In order to understand how digital signatures and hashing algorithms accomplish these goals, the following figure shows how they work.

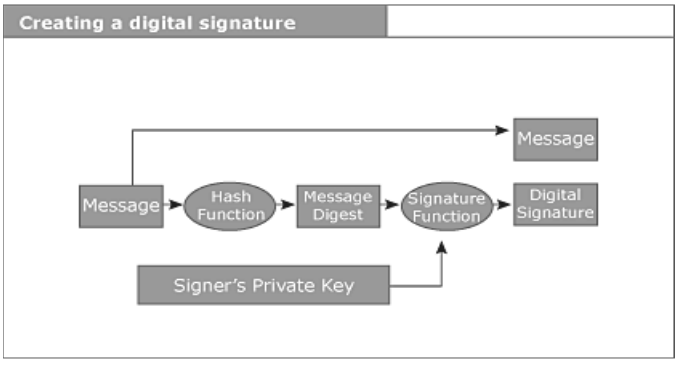


Fig: 1 Creating a Digital Signature. Taken fromhttp://www.digsigtrust.com/images/pki_2.gif

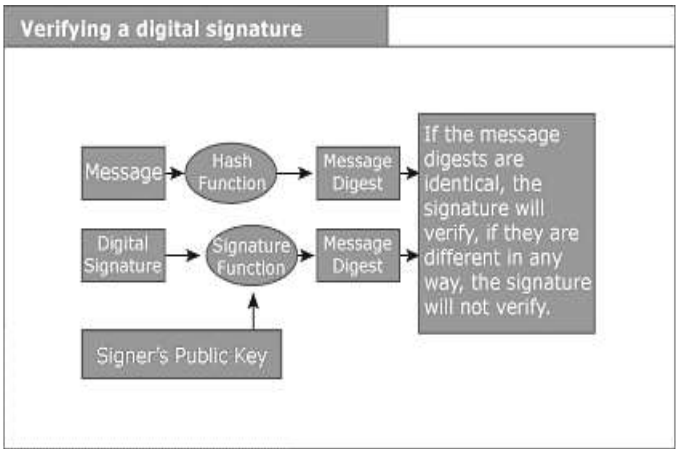


Fig: 2 Verifying a Digital Signature. Taken from http://www.digsigtrust.com/images/pki_3.gif

B. Malware Detection Techniques

Malware Detection Techniques used for malware detection can be broadly classified into two categories: anomaly-based detection and signature-based detection. An anomaly based detection technique uses the knowledge of what is considered as normal to find out what actually is malicious .A special type of anomaly based detection is specified baseddetectionspecification based detection makes use of a certain rule set of what is considered as normal in order to decide the maliciousness of the program violating the predefined rule set. Thus programs violating the rule set are considered as a malicious program. Signature based detection uses the knowledge of what is considered as malicious to find out the maliciousness of the program under inspection. [6]

Categories of the malware

- Viruses
- Worms
- Spyware
- Adware
- Trojans

The following Malware detection techniques

- Signature-Based Malware Detection Techniques
- Specification-based Detection
- Behavior -based Detection

Signature-Based Malware Detection Techniques

Commercial antivirus scanners look for signatures which are typically a sequence of bytes within the malware code to declare that the program scanned is malicious in nature. Basically there are three kinds of malware: basic, polymorphic, metamorphic malware. In basic malware the program entry point is changed such that the control is transferred to malicious payload. Detection is relatively if the signature can be found in the viral code [5]. The following basic malware

ENTRY → ORIGINALCODE → MALICIOUS CODE

The signature based detection method is as follows:

- Signature extraction and distribution is a complex task.
- The signature generation involves manual intervention and requires strict code analysis.
- The signatures can be easily bypassed as and when new signatures are created.
- The size of signature repository keeps on growing at an alarming rate.

Specification-based Detection:

Specification-based intrusion detection, where manually specified program behavioral specifications are used as a basis to detect attacks.Limitation of specification-based approaches have been the difficulty of verifying that the specifications are correct and that they cover the threat model. Important efforts this issue by applying a formal verification framework.Additional background information about this framework is provided. This framework to verify the monitoring operations for theC12.22 standard protocol.

Advanced Metering Infrastructure

Advanced metering infrastructure (AMI) is an architecture for automated, two-way communication between a smart utility meter with an IP address and a utility company. The goal of an AMI is to provide utility companies with real-time data about power consumption and allow customers to make informed

choices about energy usage based on the price at the time of use. The security of Advanced Metering Infrastructures (AMIs) is of critical importance. The use of security protocols and the enforcement of strong security properties have the potential to prevent vulnerabilities from being exploited and from having costly consequences. However, as learned from experiences in IT security, prevention is one aspect of a comprehensive approach that must also include the development of a complete monitoring solution. This technology addresses the practical needs for monitoring and intrusion detection through a thorough analysis of the different threats targeting an AMI.AMI Solution Features and Benefits Are part of a platform that can evolve as your needs change. From handheld and mobile collection to a fully-featured AMI fixed network, you can rest assured knowing that the technology you deploy today can adapt to capitalize on the opportunities of tomorrow.

C. Secure Mac Protocol

The secure [1] MAC protocol will use part of the IEEE 1609.2 security infrastructure including PKI and ECC, the secure communication message format for VANETs, and the priority based channel access according to the QoSrequirements of the applications [1]. The secure MAC protocol. There are two scenarios of the VANETs: V2R based VANETs, and V2V based VANETs. In V2R based VANETs, we assume that the vehicular communication is controlled by RSUs. Each RSU acts as an access point that broadcasts all the messages received from one vehicle to all others in the range. In V2R based VANETs, on the other hand, we assume there is no RSU infrastructure exist, each OBU on a vehicle has to rely on its own for communications. It has to broadcast messages to all the nearby nodes. There is no acknowledgement in the V2V based VANET, unlike in the V2R based VANET where acknowledgement is created by the RSU.

Function Performed

- Receive/transmit normal frames
- Half-duplex retransmission and backup functions
- Append/check FCS (frame check sequence)
- Interframe gap enforcement
- Discard malformed frames
- Append /removepreamble, SFD (start frame delimiter), and padding
- Half-duplex compatibility: append/removeMAC address

Addressing mechanism

The local network addresses used in IEEE 802 networks and FDDI networks are called MAC addresses; they are based on the addressing scheme used in early Ethernet implementations. A MAC address is a unique serial number. Once a MAC address has been assigned to a particular network interface (typically at the time of manufacture), that device should be uniquely identifiable amongst all other network devices in the world. This guarantees that each device in a network will have a different MAC address. This makes it possible for data packets to be delivered to a destination within a subnetwork, i.e. Hosts interconnected by some combination of repeaters, hubs, bridges and switches, but not by network layer routers. Thus, for example, when an IP packet reaches its destination (sub) network, the destination IP address is resolved with the Address Resolution Protocol for IPv4, or by Neighbor Discovery Protocol (IPv6) into the MAC address of the destination host.

Channel access control mechanism

The channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. The multiple access protocol may detect or avoid data packet collisions.

If packet mode contention based channel access method is used, or reserve resources to establish a

logical channel if a circuit switched or channelization based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

A Secure MAC Protocolfor DSRCApplications [1]

A secureMAC protocol in consideration of the Dedicated Short Range Communication channel structuresand to accommodate the Dedicated Short Range Communication applications that providingadequate security for VANETs [1]. The proposed secure MAC protocol will use part of the IEEE 1609.2 security infrastructure including PKI and ECC the secure communication message format for VANET and thepriority based channel access according to the QoS requirements of the applications.

Secure Protocol

VANET security [1] requires message authentication and integrity, message non-repudiation, entity authentication, access control,message confidentiality, availability, privacy and anonymity, and liability identification for the safety related applications.
OBU on a vehicle has a secure database, which stores allcryptography components used for signing and verifying each message. Each vehicle has to have a valid certificate usually issued by a central trusted party called Certificate Authority (CA). PKI will be used for certificates issued by a CA. In the privacy of a vehicle, such as identity andtravel route, a set of anonymous keys can be used to sign each message that will be changed periodically. These keys can be preloaded in the secure database of the OBU for a long period of time, e.g., for one year until next yearly license plate registration. Each key is certified by the issuing CA and has a short lifetime. In case of an accident or other law investigation, the authority can track back to the real identity of the vehicle, using Electronic License Plate (ELP) [1]. This can also help to prevent non-repudiation in case ofaccidents.

Data Aggregation Mechanisms

A MAC layer IEEE 802.11bprotocol limits the size of the payload that is sent on the network channel to a maximum size.The number of records inthe node's validated dataset can be large, making itimpossible to fit all of them in one broadcast message. Inorder to deliver as much information about other vehiclesas possible, data compression/aggregation techniquesshould be applied to the validated records [3]. There is a two method data compression and data aggregation.

Data Compression

Data compression is actually "binary compression" in the sense that it does not base the decisions made on the semantics of the data.Its require a lot of computation resources which is not suitable for most portable devices [3].

Data aggregation

Data aggregation is based on the date semantics. For example, the records from two vehicles can be replaced by a single record with little error if the vehicles are very close to each other, and they are moving with relatively the same speed. The way data aggregation contributes to theTrafficView system is by delivering as many records as possible in one broadcast message. This way, more new records can be delivered in a certain period of time and the overall system performance is improved [3].

D. Secure Key Management scheme

Key distribution is one of the most important security functions of the network. A secure network will designate one special device which other devices trust for the distribution of security keys: the trust center. Ideally, devices will have the trust center address and initial master key preloaded; if a momentary vulnerability is allowed. Typical applications without special security needs will use a network key provided by the trust center (through the initial insecure channel) to

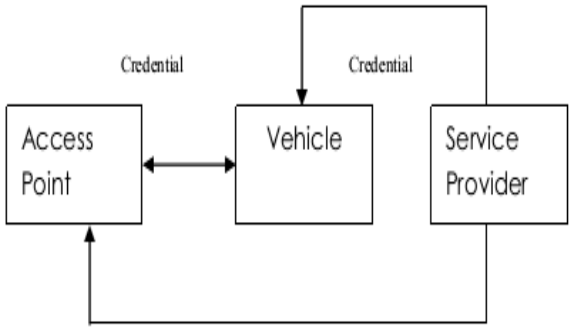
communicate.Thus, the trust center maintains both the network key and provides point-to-point security. Devices will only accept communications originating from a key provided by the trust center, except for the initial master key. The security architecture is distributed among the network layers as follows:

- The MAC sublayer is capable of single-hop reliable communications. The security level it is to use is specified by the upper layers.
- The network layer manages routing, processing received messages and being capable of broadcasting requests. Outgoing frames will use the adequate link key according to the routing, if it is available; otherwise, the network key will be used to protect the payload from external devices.
- The application layer offers key establishment and transport services. It is also responsible for the propagation across the network for changes in devices within it, which may originate in the devices themselves or in the trust manager. It also routes requests from devices to the trust center and network key renewals from the trust center to all devices. Besides this, the ZDO maintains the security policies of the device.

Key Establishment

Cluster Key Establishment: The cluster key is generated between the cluster-head and a node which is obtained by the grouping of the vectors from the node and cluster-head with that of the master key. The cluster-head is selected by means of the estimation of energy consumption with nodes. The main goal of Cluster key establishment is in VANET to decrease system delay and reduce energy consumption.

Station Key Establishment: The station key is a key that is formed between the cluster-head and the Base station. The Base station is nothing but a static node that is assigned a particular vector with the help of which the station key is established.A key management scheme that provides a better security performance with a low memory overhead, the vector key-based cryptosystem facilitates us to design communication and storage efficient schemes, through efficiency analysis, our system is shown to satisfy the predefined security objectives and desirable efficiencies.



Authentication and Key Establishment

E. Risk – Aware Response Mechanism

Risk-aware response mechanism to systematically cope with the identified routing attacks. Risk-aware approach is based on an extended Dempster-Shafer mathematical theory of evidence introducing a notion of importance factors.

F. Security aspects restricted to VANET

- Position verification techniques to thwart position spoofing attacks [6].
- Traceability by trusted network authorities (e.g., Network administrator) for privilege revocation once misbehavior is detected [6].
- Identity and location privacy preserving mechanisms against unlawful tracing and user profiling [6].
- Non-frameability of an honest user who cannot be falsely accused of having misbehaved [6].
- Detecting and correcting malicious data to ensure data consistency [6].
- The system must have light overheads in terms of computational costs and high efficiency [6].

- Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and to damage the security of VANETs [6].
- Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs [6].

G. Privacy Preserving Authentication Scheme

The fundamental security functions in Vehicular Communication will consist in authenticating the origin of a data packet. Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities. In addition, authentication helps also to control the authorization levels of vehicles [8] [6]. To authenticate each other, the vehicles will sign each message with their private key and attach the corresponding certificate.

Threshold Authentication

The initial VANET system setup where a system public/private key pair is assigned to each legitimate user for authentication purpose, before our defense scheme or any other security schemes can be deployed. In general, a VANET user with public/private key pair (PSv;$ v) broadcasts a message m (e.g., Inan accident-avoidance, detour-notification) as follows [2]:

V ! ¤: PSv , m, SIG$v (m k t),

Where SIG denotes the signature scheme for signing message me, and it is the current system time to prevent message replay attack [2] [6].Preserving user privacy, vehicles always use their pseudonyms as public keys for authentication instead of real identities. Here a trust domain is managed by a regional transportation authority (RTA) [2].

III. Conclusion

In this paper the Survey of Security in Vehicle to Vehicle Communications. We analyze about most of the security techniques like Public-key infrastructure, Malware Detection Techniques, Secure Mac Protocol, Secure Key Management scheme, Privacy Preserving Authentication scheme, Risk Aware Response Mechanism etc...These alltechniquesthat could not satisfy all the security issues, everysecurity schemethat satisfies the distinctsolutions,There is a no single technique for solving all the network communication issues. So we need single safety techniques to control all the security issues.

References

[1] Secure protocols for data propagation and group communication in vehicular networks, EURASIP Journal on Wireless Communications and Networking2011

[2] A survey on securing user authentication in vehicular ad hoc networks, Mrs. Arzoo Dahiya, Mr. Vaibhav Sharm, Computer Science & IT Department, Institute of Technology and Management, arzoo@itmindia.edu, shvaibhav@yahoo.com

[3] Securing Vehicular Communications, Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux, Laboratory for computer Communications and Applications (LCA), School of Computer and Communication Sciences.

[4] Data Naming in Vehicle-to-Vehicle Communications, Lucas Wang, Ryuji Wakikawa, Romain Kuntz, Rama Vuyyuru, and Lixia Zhang, Computer Science Department, University of California, Los Angeles, Toyota InfoTechnology Center, USA Mountain View, CA

[5] Security and Privacy in VANET to reduce AuthenticationOverhead for Rapid Roaming Networks, Prof. Alka Jindal, Dept of I.T, PEC University of Technology, Chandigarh, India.

[6] Survey on Malware Detection Methods, Vinod P., Department of Computer Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan, vinod_p22@yahoo.com

[7] A Secure VANET MAC Protocol for dsrc applications, Yi Qian, Kejie Lu, and Nader Moayeri, National Institute of Standards and Technology, University of Puerto Rico, Mayaguez, PR 00681, USA

[8] A Defense Technique Against Misbehavior In VANETsBased On Threshold Authentication, Jinyuan Sun and Yuguang Fang, University of Florida, Gainesville, FL

[9] TrafficView: Traffic Data Dissemination using Car-to-Car Communication, Department of Computer Science, University of Maryland, College Park, MD, USA

[10] A Survey of VANET's Authentication, Department of Computer Science, Islamia College Peshawar (Chartered University) Peshawar, Pakistan

[11] Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, Dept. of ECE, Worcester Polytechnic Institute

[12] Identification of Malicious Vehicle with VANET Environment from DDOS Attack, Ayonija Pathre, Chetan Agrawal, Anurag

Jain, 1Department of Computer Science, RIST, Bhopal, M.P., India

[13] DDoS attacks and defense mechanisms: classification and state-of-the-art, Christos Douligeris, Aikaterini MitrokotsaDepartment of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, 13 October 2003

[14] VITP: An Information Transfer Protocol for Vehicular Computing, Marios D. Dikaiakosy, Dept. of Computer Science, University of Cyprus, Nicosia, CY1678, Cyprus.