A Review of Security Threats, Solutions and Trust Management in VANETs

B. G. PREMASUDHA
Siddaganga Institute of Technology
V. RAVI RAM
Sri Siddhartha Institute of Technology
J. MILLER
Florida International University
and
R. SUMA
Sri Siddhartha Institute of Technology

The real time implementation of Vehicular Ad-Hoc Network (VANET) applications is challenging unless their security and privacy requirements are strongly addressed. Thus many researchers attention is directed towards providing security solutions that mitigate threats to VANET environments. In this paper we give readers an overview of the VANET environment, Intelligent Transport System (ITS) communication configurations and wireless access standards used in VANETs. We have described a general VANET model, the VANET Communication Evaluation Model (VCEM) with two of its communication environments Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) in the context of security, privacy and trust. The roles and relationships of several participating entities in these communication environments along with a few important communication patterns, critical to VANETs are also discussed. The typical security requirements for VANETs are discussed and the categorization of several security threats to these requirements is made. A description on the relevance of these threats for VANETs with illustrations is also made. We have discussed the general working of two types of security schemes, one based on Public Key Infrastructure (PKI) and the other on ID-based cryptosystems. We have outlined the features of various PKI based security schemes and their drawbacks in general. We have focused on several ID based cryptosystems and briefly outlined their merits and demerits with a comparison on performance. In this paper, we have also discussed an important VANET issue, trust among peers. Various types of trust management models in VANETs and the related research efforts have been summarized. The significant properties of an efficient trust management model are discussed and a comparative study of few of the existing trust management schemes is made. Finally the challenges in developing secured VANET applications are presented.

Keywords: VANET, security, threats, PKI, ID-based cryptosystems, trust management.

1. INTRODUCTION

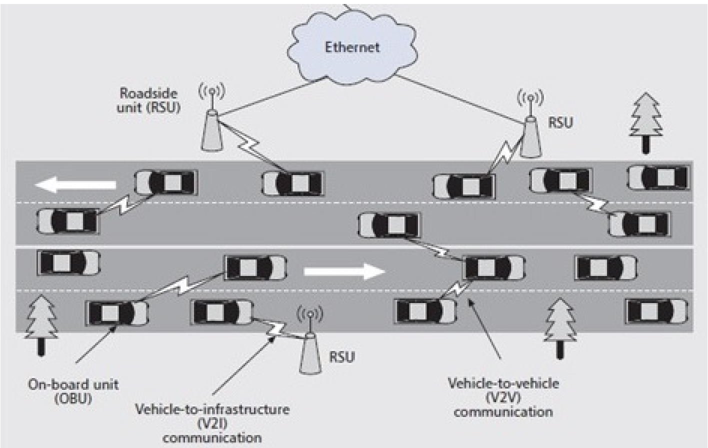
Vehicular Ad-hoc Network (VANET) is a specialized form of Mobile Ad-hoc Network (MANET) and is a key component of Intelligent Transport System (ITS). VANETs consist of vehicles (nodes) equipped with wireless communication devices such as On Board Units (OBU), Global Positioning System (GPS), digital maps, and additional sensors for reporting the condition of the vehicle. In order to exchange information, vehicles communicate among themselves as well as with the access points within their radio range. To propagate information, VANETs either use Ad-hoc or infrastructure based wireless networks. The vehicles in VANET acts as ordinary nodes as well as wireless routers to establish an ad-hoc network in a range of approximately 100 to 500 meters. As specified by authors Raya et al. [2006], the rapid growth in the number of wireless devices in the

Authors' addresses: Dr. B. G. Premasudha, Department of MCA, Siddaganga Institute of Technology, Tumkur, Karnataka, India, bgpremasudha@gmail.com; V. Ravi Ram, Department of MCA, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India, raviramv@gmail.com; J. Miller, School of Computing and Information Sciences, Florida International University, Miami, Florida, USA, Jerryf.miller@yahoo.com; R. Suma, Department of MCA, Sri Siddhartha Institute of Technology, Tumkur, Karnataka, India, sumaraviram@gmail.com

market has a direct influence on the growth of VANET applications and has led to huge demand for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication. As mentioned by authors Harsch et al. [2007], VANETs supports a number of safety and non-safety applications that cater to several needs such as providing safety for vehicles, efficient traffic administration, automation of toll collection, improved vehicle and route navigation, aid in finding amenities such as fuel stations, hotels, restaurants, hospitals and internet hotspots.

The authors Samara et al. [2010] have specified that VANET requirements such as low latency, security and privacy demands novel communication architectures for future vehicular applications. Characteristics like dynamic topology, frequently disconnected network, high mobility, potentially large scaled and partitioned network, communication environment, hard delay constraints and the security and privacy requirements of authenticity, confidentiality, availability makes research in VANETs more challenging. Most of the research efforts that were made all these years focused mainly on the investigation of various issues related to V2V and V2I communication. This clearly indicates that V2V and V2I communications plays significant role in ITS.

The possible communication configurations in ITS include vehicle to vehicle,vehicle to infrastructure, and routing-based communications as proposed by Jinyuan et al. [2007]. Vehicle to vehicle communication configuration uses either multicast or broadcast mechanism over multiple nodes to transmit data to a group of vehicles. Vehicle to infrastructure communication configuration adopts broadcast of data in a single hop, where a roadside unit sends a broadcast message to all its one hop neighbour vehicles. Routing-based communication configuration supports unicast of messages in multiple hops till the target vehicle is reached. The efficiency of these communications solely depends on the accuracy of the available information of the neighbouring vehicles. The basic VANET Communication configurations described by authors Wasef et al. [2010] are shown in Figure 1. As mentioned by authors Zeadally et al. [2012], several wireless access standards are available for VANETs and they include communication protocols, security specifications, routing and addressing services, and interoperability protocols. The details of wireless access standards for VANET are discussed in Section 2.


Ethernet
Roadside unit (RSU)
RSU
RSU
On-board unit (OBU)
Vehicle-to-infrastructure (V2I) communication
Vehicle-to-vehicle (V2V) communication

. Figure. 1: VANET communication configurations

Based upon current, ongoing research in the ITS environment, we developed a VANET Communication Evaluation Model (VCEM), to identify the critical factors to be met by researchers engaged in ITS activities and conducted a review of ongoing research efforts on security threats, solutions and trust management in VANETs. Basically a VANET model can be constructed by logically bifurcating into two communication environments 1) Infrastructure Environment and 2) Ad-hoc Environment. A third communication environment, sensor-to-sensor aboard a single vehicle, is also a critical component of the two principal communication environments, but can be considered either independently, or as a part of the two principal communications environments. For purposes of this paper, we consider sensor-to-sensor communications as part of the two larger environments.

Security, privacy, and trust considerations are central components to each environment. Security is the broader term which addresses how to protect the usability, reliability, integrity, and safety of your network and data. Privacy on the other hand, is in fact the most difficult and complex issue to address. Privacy assures that the data on the network, as well as the vectors of the data, or indications of where the information is coming from and going to is not accessible to those not authorized to obtain the information. Trust provides authenticity guarantees so each node can communicate safely to every other node with assurance that each node is part of the actual network, and authorized to receive/send data and not acting maliciously.

In order to perform basic communication operations in VANETs, the participation of several communication entities is required along with the vehicles. To better understand the security issues related to the VANET environment, one must understand the roles of these entities and their relationships.

The VANET communication patterns that comprise the VCEM and the participating entities with their roles and relationships are discussed in section 3. There are several communication patterns for VANETs, however from the security point of view V2V and V2I communication patterns are some of the most challenging in an ad-hoc network and need special focus. Thus few of the communication patterns that fall under this category are discussed in Section 3.

Providing safety and comfort to drivers and passengers is a major concern in VANETs as human lives and their commuting times are precious. Thus the vital information propagated by safety applications shall not be altered or dropped during transit and their timely delivery shall be guaranteed. Any unfair activity of malicious users especially on life- critical safety information could turn fatal for other users as mentioned by the authors Ram and Premasudha [2014]. Thus in VANETs, it is highly required to safeguard critical information from attackers. The need for VANET security and the inherent challenges are discussed in Section 4. VANET security has to satisfy several security requirements such as authenticity and integrity, availability, non- repudiation, access control, message confidentiality, privacy and anonymity. Each of these requirements is also discussed in Section 4. There are several threats to VANET security requirements. A classification of security threats and a description on relevance of those threats to VANETs is made in Section 5.

Several researchers have put in their efforts to mitigate security threats in VANET environment, and those efforts have been broadly categorized as Public Key Infrastructure (PKI) security architectures and ID-based cryptosystems.

PKI is comprised of several software and hardware components governed by certain policies and procedures to manage and distribute digital certificates. The general working of PKI security systems, various PKI based security architectures with their key features and drawbacks are summarized in Section 6.

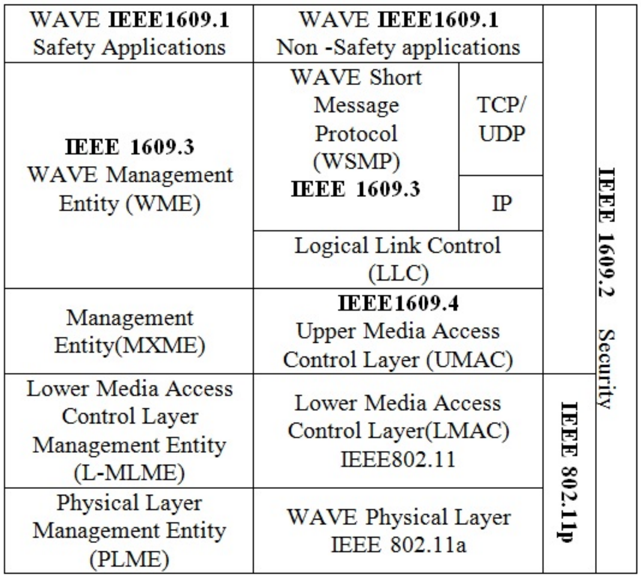
ID-based cryptosystem uses the identity of the vehicle or the driver as a public key and the corresponding private key is generated by the Private Key Generator (PKG). Any trusted third party can act as the PKG. The working of ID-based cryptosystems in general and few ID based security architectures with their key features are discussed and compared in Section 6.

In addition to security and privacy, one more inherent issue that arises in the VANET environment is the opinion of trust among peers. It is desirous that each peer in a VANET detects dishonest peers and the malicious data sent by them. The categories of trust management models with a summary of related work and the significant properties of a typical trust management model are presented in Section 7. A comparative study on the properties of few existing trust models is also made in Section 7. Finally, the future challenges for secured VANET application development are presented in Section 8.

2. WIRELESS ACCESS STANDARDS FOR VANETS

The authors Zeadally et al. [2012] have specified that there are several wireless access standards for VANETs and they cater to communication protocols, security specifications, routing and addressing services, and interoperability protocols. Dedicated Short Range Communications (DSRC) service facilitates both vehicle-to-vehicle and vehicle-to-roadside communications to cover a wide range of safety and non-safety VANET applications. The sole purpose of DSRC is to facilitate high data transmissions with low latency in a small communication range. DSRC is based on the IEEE 802.11a physical layer and 802.11 MAC layer. The access to DSRC spectrum is free but it is licensed in terms of its restricted usage.

The United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum at 5.9 MHz to be used by DSRC. Due to typical and dynamic characteristics of VANETs, conventional IEEE 802.11 Media Access Control (MAC) operations under-perform when used in vehicular environment. To improvise the performance of IEEE MAC operations, the American Society for Testing and Materials (ASTM 2313) working group had migrated to the IEEE 802.11 standard group. The improvised version of DSRC is renamed as IEEE 802.11p Wireless Access in Vehicular Environments (WAVE). The top layers of IEEE 1609 standards handle the operational complexities of DSRC. The management activities specified in IEEE 1609.1, the security protocols defined in IEEE 1609.2, and the network-layer protocol defined in IEEE 1609.3 regulates the functioning of WAVE applications. As IEEE 1609.4 standard lies above IEEE 802.11p, it supports all higher layer operations without involving any of the physical channel access parameters. Any stationary WAVE device that hosts VANT application can act as a service provider. Similarly, any mobile device that runs the peer application can use those services. Figure 2 describes WAVE, IEEE 1609, IEEE 802.11p standards as described the authors Zeadally et al. [2012] and Figure 3 illustrates a typical VANET communication scenario.



. Figure. 2: Wireless Access Standards for VANET

The purpose of various IEEE 1609 standards:

- IEEE 1609 standard specifies VANET architecture and its components such as On Board Unit, Road Side Unit, and WAVE interface. It also specifies physical access for WAVE, security mechanisms and resource management.

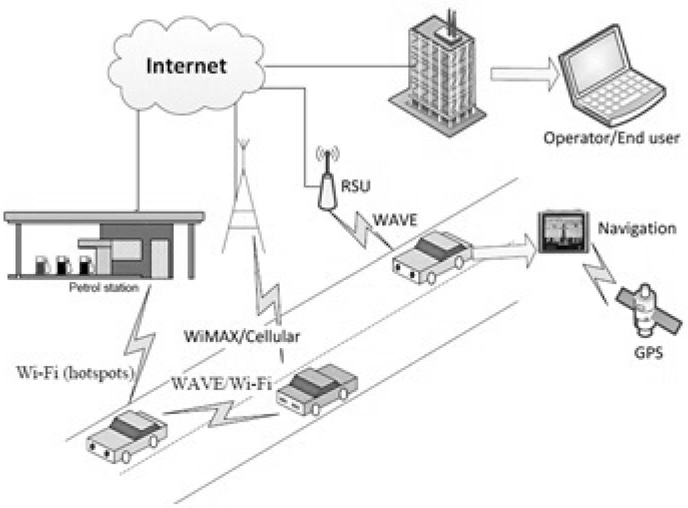
—IEEE 1609.1 (Resource Manager) standard specifies application interoperability, command formats, description on WAVE architecture elements, types of OBU supporting devices.

—IEEE 1609.2 (Security Services for Applications and Management Messages) standard specifies the need for secured messaging and the available security services.

—IEEE 1609.2 (Security Services for Applications and Management Messages) standard specifies the need for secured messaging and the available security services.

—IEEE 1609.3 (Networking Services) standard specifies the possible addressing and routing mechanisms for a secured data transfer. It defines WAVE Short Message Protocol (WSMP) which can be used by WAVE applications as an alternative to internet Protocol (IP).

—IEEE 1609.4 (Multi-Channel Operations) standard specifies the improvements made to the basic 802.11 MAC Layer to suit for WAVE.



. Figure. 3: Typical VANET Communication Scenario

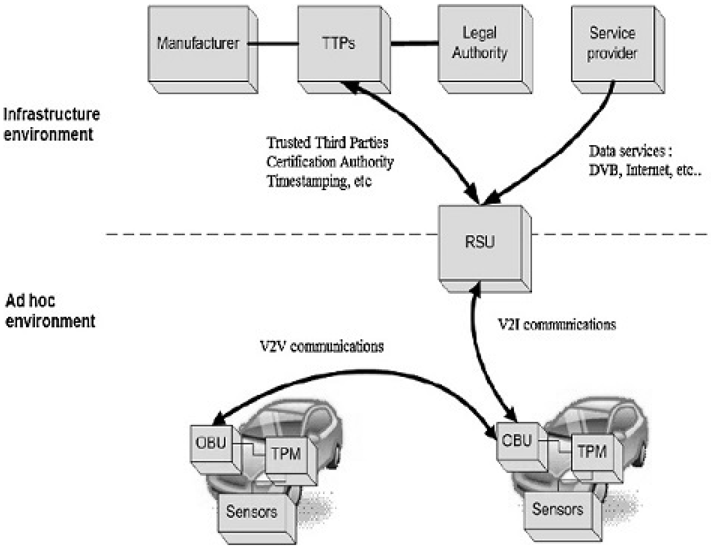
3. OVERVIEW OF VANET MODEL AND COMMUNICATION PATTERNS

In order to perform basic communication operations in VANETs, participation of several communication entities is required along with the vehicles. The most commonly used entities in a VANET communication model are shown in Figure 4 as described by authors Fuentes et al. [2010].

To better understand the security issues related to VANET environment, it is required to understand the significance of these entities and their relationships. From the Figure 4 it is clear that the VANET model is logically bifurcated into two communication environments 1) Infrastructure Environment and 2) Ad-hoc Environment.

3.1 Role of the entities in infrastructure environment

The participating entities in this environment are permanently interconnected as they come under fixed infrastructure. These entities primarily control traffic and offer several external services to the VANET users. Manufacturer entity is required to be included in this environment as it is responsible for assigning a unique identifier for each vehicle. The Legal authority entity mainly looks after vehicle registration and crime reporting. It is mandatory that every vehicle has to register with the Legal authority and get a license plate. Another class of entities called Trusted Third Parties (TTPs) plays a major role in this environment as they are responsible for



. Figure. 4: A simplified Model for VANET

providing services like time stamping and certificate management. Vehicle manufactures as well as legal authorities communicate with the TTPs to get electronic credentials. One more entity called Service Provider is required to cater data services like Internet, Digital Video Broadcasting (DVB) etc..

3.2 Role of the entities in ad-hoc environment

In this environment ad-hoc communication is established among the vehicles. Each vehicle is equipped with an On Board Unit (OBU) to facilitate V2V and V2I communications. In addition to this, optional sensors are used to measure the status of the vehicle (e.g. fuel consumption) as well as its environment (e.g. safety distance, road condition). Certain data related road safety can be shared among the neighbouring vehicles. One more important entity that is installed in each vehicle is the Trusted Platform Module (TPM) for reliable storage, computation and analysis. TPMs maintain an internal clock to generate timestamps of events and are reliable as they are tamper resistant. The sensitive information such as vehicle / user credentials, pre-crash event log stored in the TPMs provide important evidences during investigation of crimes and accidents.

As per the Dedicate Short Range Communications (DSRC) standard, communication entities such as Road Side Units (RSUs) act as gateways between the infrastructure environment and the ad-hoc environment.

3.3 Communication Patterns

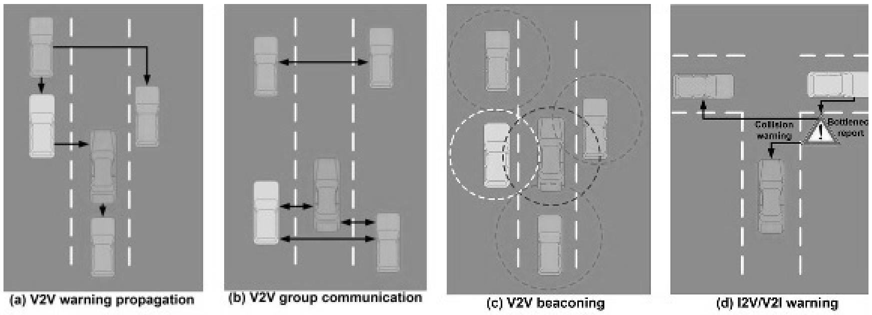
There are several communication patterns for VANET. However, from the security point of view V2V and V2I communication patterns are challenging and need special focus. Few of the communication patterns that fall under this category as described by the authors Fuentes et al. [2010] are discussed below:

Warning message propagation among vehicles (Figure 5a): In VANETs it is required to send messages to a particular vehicle or to a group of vehicles. As an example when an accident occurs, a warning message has to be sent to all the arriving vehicles in order to enhance traffic safety. Similarly when an emergency vehicle needs lane clearance then a warning message has to be sent to all the preceding vehicles. In these situations an efficient routing protocol is required to forward the warning message.

Group Communication among vehicles (Figure 5b): This communication pattern is required in place to facilitate group communication among a set of vehicles with static predefined travel objectives or among vehicles that dynamically participate in group communication over a time frame.

Beaconing among vehicles (Figure 5c): A vehicle sends beacon messages periodically to all nearby vehicles. These beacons contain the property values that reflect the current state of the vehicle such as acceleration, breaking, heading etc. Beacons are sent to only one hop neighbours. These beacons are of great value for finding the best neighbour to route a message.

Warnings between infrastructure and vehicles (Figure 5d): In order to increase road safety, warning messages are sent by infrastructure (RSU) to all the vehicles in its range when a potential danger is detected or expected. As an example, all the vehicles approaching an intersection may be warned regarding the possibility of vehicle collisions.



(a) V2V warning propagation (b) V2V group communication (c) V2V beaconing (d) I2V/V2I warning

. Figure. 5: VANET Communication patterns

4. SECURITY IN VANETS

4.1 Need for VANET security and its challenges

Providing safety and comfort to drivers and passengers is a major concern in VANETs as human lives and their commuting times are precious. Thus the vital information propagated by safety applications shall not be altered or dropped during transit and their timely delivery shall be guaranteed. Any unfair activity of malicious users especially on life critical safety information could turn fatal for other users. Thus in VANETs, it is highly required to safeguard critical information from attackers. Similarly the liability of the drivers is required to be established while preserving the privacy of the commuters. It is difficult to resolve the security attacks in VANET environment due to its typical and dynamic characteristics such as high speed, varied density and short term connectivity of the vehicles. These dynamic characteristics demand novel communication patterns, security and privacy preserving approaches and wireless communication systems that effectively utilize the existing infrastructure. In addition to its inherent dynamic characteristics, the use of wireless media for vehicular communication makes VANETs more prone to various kinds of security attacks.

4.2 Security requirements for VANETs

VANET security has to satisfy several requirements such as authenticity and integrity, availability, non -repudiation, access control, message confidentiality, privacy and anonymity. Each of these requirements is described below.

Authenticity and Integrity: Primarily VANET security must ensure message authenticity which ascertains the correctness of received information and entity authenticity which ascertains that the source is who he claims to be. If authentication requirement is not considered seriously, malicious users may randomly transmit a huge number of safety-related messages from non-existing nodes. In order to control the authorization level of the entities, a source vehicle assigns its private key along with its certificate to all the messages it sends. And at the receiving end, the vehicle first checks the key and certificate and then verifies the message.

Availability: This requirement ensures authorized parties access to required resources when needed. Most of the safety related applications are time sensitive and a delay in seconds in message delivery may be devastating. The VANET applications must be robust enough to operate even in the presence of malicious behaviour of the attackers.

Non-Repudiation: This requirement ensures that a vehicle which sends a message cannot disagree that the message has originated from it. With the help of the information stored in Tamper Proof Devices (TPD) installed in vehicles, it is possible for regulatory authorities to detect malicious behaviour of the attackers and make them liable for their ill behaviour.

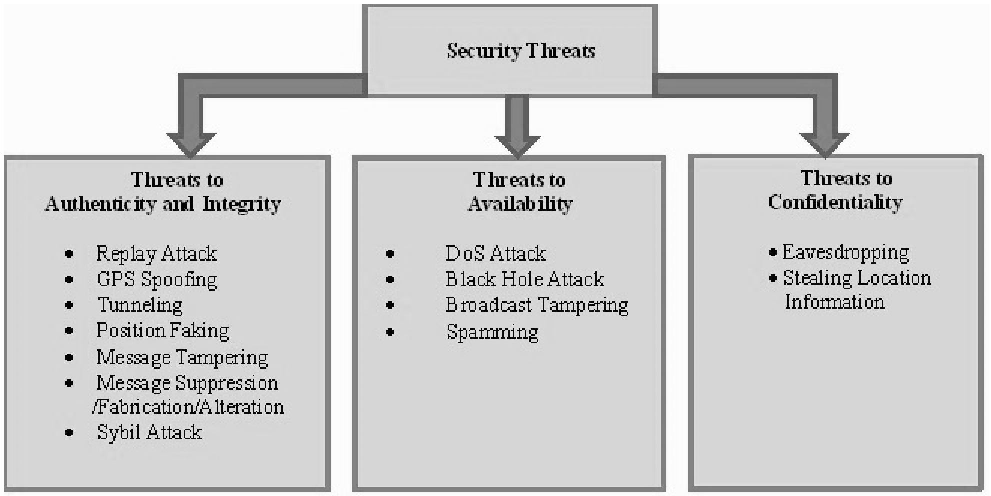
Access Control: This requirement sets stringent policies on access to specific services provided in the VANET environment thereby delineating the service levels among the participating vehicles in the network.

Message Confidentiality: This requirement limits information access to authorized users and protects information from stealing by unauthorized users.

Privacy and Anonymity: This requirement safeguards identity of sender from tracking. The privacy of the user has to be safeguarded in the sense that the user's data such as name of the driver, the vehicles license information, speed, location and travelling route has to be kept undisclosed from other users. However this information must be available to the regulatory authorities to identify the suspicious vehicles and the drivers during crime investigation.

5. VANET SECURITY THREATS

There are several kinds of threats to VANET security requirements. Figure 6 classifies the security threats under the security requirements such as Authenticity, Integrity, Availability and Confidentiality.



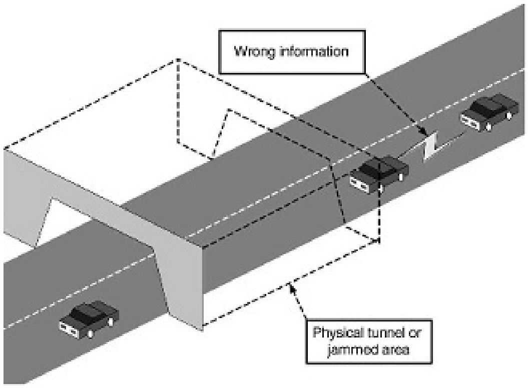
. Figure. 6: Classification of few VANET Security Threats

5.1 Threats to Authenticity and Integrity

Replay Attack: Continuous re-injection of beacons and previously received messages back on to the network are instances of replay attacks. This attack happens easily in VANETs, as message sequence numbers and time stamps are not maintained. Using this attack it is very easy for an attacker to confuse the traffic authorities possibly preventing them to identify the vehicles in incidents like theft and hit and run cases. Thus there is a need for maintaining timestamps of messages and authentication of individual packets before decryption.

Global Positioning System (GPS) Spoofing: The attacker generates virtual GPS signals stronger than the original signals generated by the trusted satellites. Thus unknowingly a legitimate user receives false position information.

Tunnelling: When a vehicle passes through a tunnel it cannot access position information through GPS services. As mentioned by the authors Raya and Hubaux [2007], this is a boon to the attacker to inject fake position information on to the on board devices of the vehicles well before the vehicle again receives authenticated position information .



. Figure. 7: Tunnel attack

Position Faking: In VANETs, a vehicle is held responsible for providing its accurate position information. As mentioned by the authors Zeadally et al. [2012], attackers may report modified or misrepresented position information to other vehicles in the network .

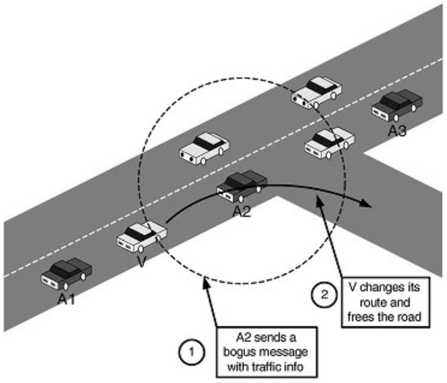
Message Tampering: It is possible for an attacker to tamper request and response messages exchanged among vehicles there by destructing the integrity of transaction. This attack corrupts or meaningfully manipulates safety messages and critical traffic notifications as specified by authors Leinmuller et al. [2006].

Message Suppression/Fabrication/Alteration: An attacker selectively drops important packets while in transit and uses them at a later stage. The attacker suppresses the congestion warnings so that other vehicles could not receive those warnings, finally putting the vehicles into a traffic jam . An attacker can fabricate messages, vehicle identities, certificates and critical warnings as mentioned by authors Raya et al. [2006]. An attacker can alter the original data to be transmitted such as altering the road congestion notifications.

Sybil Attack: An attacker creates and sends several wrong messages with fabricated source identity. As mentioned by the authors Raya and Hubaux [2007] several instances the attacker uses this mechanism to create an illusion of a traffic jam among other vehicles so that they deviate to alternative routes, there by leaving the road for the attacker itself.

5.2 Threats to Availability

Denial of Service Attack (DoS): This attack is possible when the resources of a vehicle are overridden or when the control channel used for communication is jammed. These attackers can be insiders or outsiders and the attack may be centralized or distributed. DoS attack flattens the node's resources by making the node busy all the time in verifying surplus artificial messages that are received, there by not giving room for the node to carry out important jobs. As an


A3
A2
V
A1
2 V changes its route and frees the road
1 A2 sends a bogus message with traffic info

. Figure. 8: Sybil Attack

example, an attacker can make an intentional accident and may prevent the crash notification reaching oncoming vehicles by employing a DoS attack Raya et al. [2006].

Black Hole Attack: This happens as a result of drop out or refusal of a node to participate in the VANET communication. These broken paths results in loss of transmitted messages. Finding multiple routes to the destination is an expensive solution in VANETs due to high speed of vehicles. Another solution is to keep track of the sequence number embedded in the packet header as mentioned by authors Shurman et al. [2004].

Broadcast Tampering: As mentioned by author Sabahi [2011], false safety messages injected into the network by insiders may severely cause damages such as accidents due to suppression of traffic warnings or misleading information which changes the traffic flow.

Spamming: Spam messages increases transmission latency and are difficult to regulate since VANETs lack infrastructure and centralized administration as mentioned by the authors Zeadally et al. [2012].

5.3 Threats to Confidentiality

Eavesdropping: An attacker collects information of drivers without their knowledge and uses that information at later stages for their personal benefit as explained by the authors Zeadally et al. [2012].

Stealing Location Information: As mentioned by the authors Fussler et al. [2007], an attacker steals location information of vehicles from the broadcasting messages. Thus location privacy and anonymity are required to protect confidentiality.

6. VANET SECURITY SOLUTIONS

Network security solutions have long employed cryptographic architectures as a method of securing the network and data. Several VANET researchers have also put in their efforts to mitigate security threats in the VANET environment using cryptographic architectures. These efforts have been broadly categorized as Public Key Infrastructure (PKI) security architectures and ID-based cryptosystems.

6.1 Public Key Infrastructure (PKI) based Security Architectures

In VANETs, the security requirements such as message authentication and non-repudiation can be accomplished with the use of digital signatures. This is possible by using asymmetric cryptography where each vehicle has a public/private key pair. Any vehicle can generate a digital signature for its outgoing messages using its unique private key. On the other hand the receiver of the message verifies the digital signature using the sender's public key. This digital signature verification ensures message authentication as well as non-repudiation. For entity authentication of a vehicle, its public key must be authentic to all other vehicles in the network. Thus PKI is required for securing VANETs.

PKI is a collection of software and hardware components governed by certain policies and procedures for the management and distribution of digital certificates. PKI based security architectures uses cryptography wherein a Certification Authority (CA) binds public keys with user identities. In PKI systems, digital signatures are issued and verified by CA whereas users' identities are verified by registration authority such as Regional Transportation Authority (RTA). By restricting the possible actions that can be made by users on the attributes of the certificates it is possible to attain access control. Similarly PKI based security schemes demands revocation of issued certificates when the certificate encryption keys are compromised and also when there is a change in the status of encryption peers that possess the certificate. A Certificate Revocation List (CRL) is a collection of certificates that are issued and subsequently withdrawn by the CA. Prior to the verification of a message, the receiver checks whether the sender is in the CRL. Conditional Privacy can be achieved by using anonymous certificates as they do not carry any personal identity of the certificate holder. Thus the privacy of the sender is preserved while authenticating any vehicle. However, the RTA can know the real identity of the vehicle from its anonymous certificate.

PKI has some limitations in securing VANETs. Even though anonymous certificates in PKI achieve identity privacy, they lack capacity in providing location privacy. An attacker is capable of tracking the vehicle in his observation area even though the vehicle changes its anonymous certificate. Revocation of certificates is also sensitive in VANETs as it sometimes may lead to revocation of certificates belonging to innocent vehicles due to unintentional broadcast of a disputed message. Hence fair revocation of certificates is required in VANETs. According to DSRC standard, once in every 300 ms time a vehicle has to broadcast its speed, current position and other information. Meanwhile each vehicle receives a number of signed messages and it is cumbersome for the vehicle to check CRL before verifying those messages. To do this in a timely manner is a big challenge in VANETs.

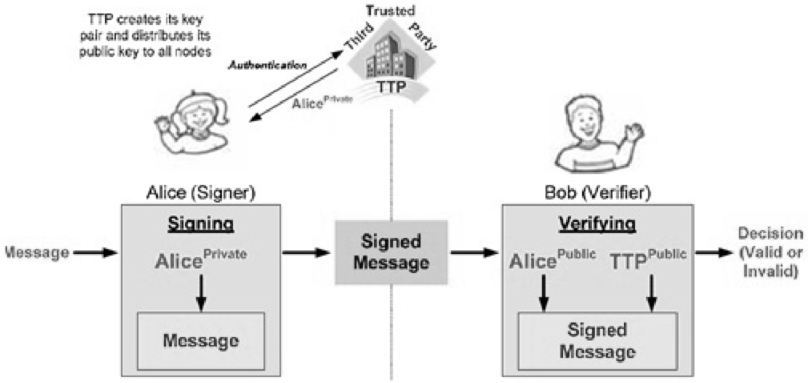
Related research efforts: Several authors have put in research efforts to develop PKI based security schemes. Authors Raya and Hubaux [2005] have addressed the privacy issue based on pseudonyms by using anonymous public key and PKI and have shown that PKI is appropriate for VANETs. Authors Raya et al. [2006] have proposed certificate revocation protocol for Tamper-Proof Devices and revocation protocols that use certification compression and distribution. Authors Plobl et al. [2006] have proposed a three layered security architecture covering basic, single-hop and multi-hop-security features. A security architecture which represents a holistic method to substantiate the requirements of a complete security system was proposed by author Eichler [2007]. Authors Wang et al. [2008] have proposed pairwise and group distribution of authenticated session key suitable for non-safety applications, thereby enhancing the security provided by the scheme proposed by authors Raya and Hubaux [2005]. This scheme offers both confidentiality and non-repudiation services. An efficient security structure using both asymmetric and symmetric-cryptosystem and tamper proof hardware was proposed by authors Plobl et al. [2006]. However, all the PKI based security architectures discussed above are infeasible for availability due to extra communication requirements incurred in managing the CRLs.

6.2 ID-based cryptosystems

VANETs are infrastructure-less by nature, this characteristic limits the use of Public Key Cryptosystems as they rely upon PKI which uses key distribution as well as key management. Dynamic wireless networks have limited bandwidth, thus the size of keys and certificates becomes a bottleneck while using PKI in VANETs. Similarly, Symmetric Key Cryptography is also not best suited for VANETs as the environment cannot tolerate communication delays and demand real time responses. Thus, instead of using certificates, author Shamir [1984] introduced the concept of ID-based cryptography by using unique identities of users as public key to authenticate and encrypt messages, there by simplifying the certificate management procedure.

ID-based cryptosystem uses the identity of the vehicle or the driver as a public key and the corresponding private key is generated by the Private Key Generator (PKG). Any Trusted Third Party (TTP) can act as the PKG. The PKG makes only the master public key available to the users. An authorized user generates his public key which is a combination of his ID and the master public key. In contrast, the user has to depend on the PKG to get his private key generated which is a combination of his ID and the master private key.

The general ID-based signature scheme as proposed by Al-Qutayri et al. [2010] is described in Figure 9. Here the signing and verifying process is carried out in four steps:
1)Setup: TTP generates its public and private key pair (master keys) and shares its public key with all the users in the network.
2)Extraction: The signer of the message (Alice) authenticates herself to the TTP and requests for her private key, in response the TTP generates a private key ($Alice^{pri}$) and sends it to Alice.
3)Signing: The signer uses her private key ($Alice^{pri}$)sign the message.
4)Verifying: On the other side the verifier (Bob) uses the public key of the signer ($Alice^{pub}$) as well as the public key of the Trusted Third Party (TTP^{pri}) to validate the signature.

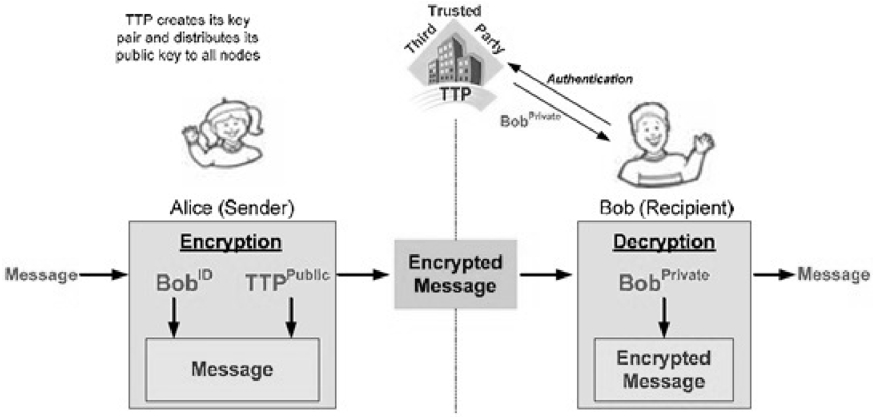


. Figure. 9: General ID-based Signature scheme

The general ID- based Encryption scheme as proposed by Al-Qutayri et al. [2010] is described in Figure 10. Here the encryption process is carried out in four steps.
1)Setup: TTP generates its public and private key pair (master keys) and shares its public key with all the users in the network.
2)Extraction: The recipient(Bob) authenticates himself to the TTP and requests for his private key, in response the TTP generates a private key (Bob^{pri}) and sends it to Bob.
3)Encryption: The sender (Alice) encrypts the message using the public key of Bob (Bob^{ID}) as well as the public key of the Trusted Third Party (TTP^{Pub}) and sends the encrypted message to the recipient Bob.
4)Decryption: The recipient Bob upon receiving the encrypted message uses its private key (Bob^{Pri}) to decrypt it.

Author Shamir [1984] had identified four important points to be considered for strengthening any ID- based cryptosystem. 1)The strength of Public Key Cryptosystem (PKC). 2)The level of protection for the data acquired and stored by the Trusted Third Party. 3)The level of authentication performed before the issue of private key. 4)The policies that safeguard private keys from leakage.

Related research efforts: Several authors have put in research efforts to develop ID-based security schemes. The security framework proposed by authors Kamat et al. [2006] uses ID-based



. Figure. 10: General ID-based Encryption scheme

signcryption (signing and encryption) scheme to facilitate message integration, non-repudiation, authentication and confidentiality producing smaller cipher texts. These authors were successful in providing privacy and security by using short-lived pseudonyms. The best part of this scheme is that the pseudonyms are unforgeable and authenticated. In this scheme, a Base-Station (BS) manages CRLs of vehicles and if the vehicle's certificate has not been revoked then the BS issues new pseudonym (RSA encrypted ID and secret key). Key escrow problem persists in this scheme even though RTA has no role in storing vehicle's private key generated by the BS. The pairing operation used for signature verification in this scheme is highly theoretical, computationally expensive and less practical. There is no necessity of secure channel for sending the private key as this scheme uses certificates based on PKI. This scheme uses short-lived replacement for the revocation of private key and resolves the problem faced during ID revocation. The best part of this scheme is that it does not use original ID of the vehicle in generating private key. Moreover, this scheme requires only storing messages consisting of the signature and pseudonyms belonging to source and the destination.

In the security framework proposed by the authors Sun et al. [2007], privacy is achieved by preloaded pseudonym and a signature mechanism using ID based threshold results in non-repudiation. This scheme does not use original ID to create the private key of the vehicle and in turn uses short-lived replacement for the revocation of private key. The drawback of this scheme is that it uses pairing operation for signature and verification which is theoretical and computationally expensive.

The authors Lin et al. [2008] introduced Group Signature and Identity-based Signature (GSIS). In this scheme, group signature is used for Vehicle-to-Vehicle and an ID-based signature for Vehicle-to-Road Side Unit communication. The drawback of this scheme is that it uses pairing operation for signature and verification which is theoretical and computationally expensive.

The authors Li et al. [2008] proposed an efficient secured communication scheme with authenticated key establishment and privacy preserving called SECSPP for Vehicle-to-Vehicle and Vehicle-to-Road Side Unit communication. SECSPP uses blind signature and one way hash chain and is effective if implemented on vehicles but it does not support non-repudiation.

A comparison of ID-based security frameworks discussed is presented Table I. In all these ID-based security schemes, the PKG uses its master private key to generate private keys for the users which lead to key escrow problem. All the schemes discussed above are economical as they avoid the need for PKI and they support a subset of the required security features. All the ID-based cryptosystems unconditionally trust the PKG, as all the cryptography keys are with the PKG.

Table I. Comparison of ID-based security frameworks

	Kamat et.al	Sun et.al	Lin et.al	Li et.al
Key escrow problem	Yes	Yes	Yes	Yes
Problem in the secured key distribution	No	No	Yes	Yes
Problem in the revocation of Private key	No	No	Yes	Yes
Problem in ID revocation	No	No	Yes	Yes
Non-repudiation	Yes	Yes	Yes	No
Conditional Privacy	Yes	Yes	Yes	No

7. TRUST MANAGEMENT MODELS

One more inherent issue that arises in the VANET environment is the opinion of trust among peers. It is desirous that each peer in a VANET detects dishonest peers and the malicious data sent by them. A few models on trust management are discussed here. These models do not fully depend upon static infrastructure and hence they can be implemented easily in real time. In these models, trust relationships are generated based on past communication experience and also from the knowledge gained from the environment.

7.1 Types of Trust Models

Entity-oriented Trust Models

Based on confidence measures and inherent trust, author Gerlach [2007] proposed a sociological trust model and had acknowledged dispositional, situational and system level trust. The architecture proposed by this author could not integrate all forms of trust except location privacy.

Authors Minhas et al. [2010] have proposed a multifaceted trust management model. This scheme uses trust worthiness of peer based on its role and the past experience. The experience based trust acts as an influencing factor in prioritizing entities with in a role category. In this model a vehicle can actively request information from other vehicles regarding the occurrence of an event. The contextual information of an event such as time and location along with the trust of information source collectively determines the advice that can be followed.

Data-oriented Trust Models

Authors Raya et al. [2007] have proposed that data-oriented trust is more promising to use in VANETs. These models decide the trustworthiness of the data received from an entity based on the opinion on the trustworthiness given by other entities. Taking into consideration several trust evaluation parameters, the model evaluates evidences for the occurrence of an event. Finally the trust level assigned with these evidences confirms the occurrence of the event. As data trust is established on per event basis, it is required to build trust relations afresh for each and every event. This model cannot work fine if there is data scarcity in forming evidences regarding occurrence of events.

Authors Golle et al. [2004] came up with a methodology to mitigate the problems in identifying and reforming malicious data in VANETs. Their approach assumes that each node its knowledge about the VANET. All the incoming data is evaluated against this model. If the model agrees the data with high probability then it is readily accepted by the peer. In case of inconsistent data, the peer depends on heuristic explanations which would restore the consistency. The data that matches with the best ranked clarification is considered by the peer. This scheme provides security against adversaries that spread malicious data.

Combined Trust Models

Authors Dotzer et al. [2005] have proposed a distributed reputation model that uses opinion piggybacking. By using the trust worthiness opinions attached to the message by various peers, a node decides its opinion on the trustworthiness of the data it receives. The relative locations of the sender and receiver add dynamism to trust calculation. Situational factors such as familiarity with the area introduce some dynamism in trust building. As this scheme repeatedly uses opinions from various nodes, the earlier nodes opinions have predominant affect than the later ones.

Authors Patwardhan et al. [2006] have proposed an approach using pre-authenticated anchor nodes. The information provided by the anchor nodes is treated as trustworthy. A node can validate its incoming data by an agreement with other nodes or by consulting with the anchor node. If the data received from a node is invalidated by the algorithm then that node is treated as a malicious node. This scheme does not utilize a reputation factor while making several agreements with peers.

Authors Chen et al. [2010] have proposed a trust-based framework where the participating nodes share data regarding road conditions and safety. This trust-based message propagation scheme efficiently receives and propagates participating nodes opinions by dynamically controlling information dissemination in a secured and scalable way. All the peers collaboratively evaluate trustworthiness of information in a distributive manner.

7.2 Significant Properties of Efficient Trust Management Models

The significant properties to be considered while designing an efficient trust management model for VANETs are discussed below.

Decentralization

Due to the highly dynamic and distributed nature of VANETs, it is desirable to decentralize trust management. Some trust models either use one-to-one or one-to-many interactions in determining trustworthiness of a peer in a distributed manner. A few other trust models depend upon the real world role of drivers in building trust in a decentralized fashion. For this to work, the car manufacturers or transportation departments must issue certificates to vehicles during manufacture of the vehicle or upon vehicle registration respectively. For the distributed mutual verification of the roles of the peers, it is required to implement public-private key infrastructure. Authors Mass and Shehory [2001] have proposed a distributed model in which, a peer can execute predefined duties based on its role.

Information scarcity

Due to the dynamic characteristics of VANETs, multiple interactions between the same set of vehicles is not guaranteed. Hence the information gained during first direct interaction should be considered important. Some times the number of peers available to spread information decrease. In such cases, whatever minimum information is received becomes highly valuable. During this time, the weight for the data is raised for trust calculations. The role-based trust models discussed by the authors Minhas et al. [2010] assume predefined trust values and roles for the peers. They were successful in distinguishing trusted peers from untrusted ones even during data scarcity.

Scalability

In dense areas a large number of vehicles pass through the environment. Thus the number of peers that report information will be relatively high. In order to quickly respond to critical conditions, a peer can only communicate with a few trusted peers. This number is always set to a small value and can be relatively updated. If experience is considered for trust calculation, then it is proportional to the number of times the peer interacted. Trust values are updated based on the aggregated past interactions. Only the most recently updated trust values are used for trust calculation to support the scalability of trust management. It is desired to have a trade-off between network scalability and trust establishment. In order to improve the level of confidence of the trustworthy peers, authors Raya et al. [2007] have proposed to frequently consult peers with a higher trust value than the threshold.

Dynamic trust metrics

A trust model shall use certain dynamic metrics such as occurrence of an event/task and the location/time of occurrence. Peers report events such as collisions, traffic jams, weather conditions etc. Event or task specific trust management requires reporting peers trust worthiness in order to respond to the events. Similarly, the messages received from peers that are physically near to the place occurrence of the event are given higher consideration. Also, if the event reporting message is close in time to the occurrence of the event then that message is given higher weight. It is very important to verify whether the location and time information received is real or falsified.

Confidence Measure
In order to record the uncertainty in the trust values of peers it is required to include a confidence value which lies in the range [0, 1]. Several highly reliable metrics are used to measure confidence value. As proposed by authors Chen et al. [2010], it is worth assigning a confidence measure to each one of the reported events.

Security
All the trust building models require an authentication scheme to uniquely identify peers and this requirement demands using PKI. A public key certified by the certification authority is used by the receiver to verify the authenticity of the sender.

Privacy concerns
As trust management demands authentication of senders, it is possible for a receiver to indirectly track personal details of a sender (such as home address) from the log of messages containing the key of the sender. As suggested by the authors Raya and Hubaux [2007], it is possible for a sender to frequently change keys while sending messages to avoid such tracking based on a sender's key. Thus each peer maintains a huge set of keys and certificates.

Robustness
Trust management itself is prone to several attacks such as Sybil Attack, Newcomer Attack, Betrayal Attack and Ballot Stuffing/Bad Mouthing Attack. Thus the robustness of trust management models strongly depends on the defensive mechanisms used against the attacks.

A comparison on the properties of a few VANET trust models is made in Table II. From this it is clear that the trust models mentioned have not captured all the required properties of an efficient trust management model. It is required that the trust models must be robust against various attacks, but robustness was not addressed by the majority of existing trust models.

Table II. Properties of existing trust models

	Kamat et.al	**Gerlach**	**Minhas et.al**	**Raya et.al**	**Golle et.al**
Decentralized	Yes	No	Yes	Yes	Yes
Scarcity	No	Yes	Yes	No	Yes
Scalability	No	No	Yes	No	No
Dynamics	Yes	Yes	Yes	Yes	No
Confidence	No	Yes	Yes	Yes	No
Security	No	Yes	Yes	Yes	Yes
Privacy	Yes	Yes	Yes	No	Yes
Robustness	No	No	No	No	Yes

8. CHALLENGES FOR SECURED VANET APPLICATION DEVELOPMENT

As security is a prominent requirement to be considered while developing VANET applications, it is worthwhile to make a judgement on the status of various security issues and solutions. The urge for providing appropriate level of protection to VANET communications has triggered an active research on security solutions. As rightly pointed out by Elmar Schoch from Volkswagen, it is unfortunate to note that these security solutions typically overload the VANET application thereby decreasing its performance. Thus, any VANET application is expected to balance the trade-off between security and performance. As mentioned by the authors Dressler et al. [2001], while authenticating and preserving integrity of messages, a general agreement was made during the Dagstuhl Seminar on the use of Elliptic Curve Cryptography (ECC) with key pairs and certificates issued by PKI.

The real time deployment of Inter Vehicle Communication takes many more years as it strongly depends on its market penetration. Thus, it is worth considering simple VANET applications that are readily deployable with reasonable delay tolerance and that use simple data dissemination techniques. During the initial deployment of VANET applications, cellular technologies like 3G and Long Term Evolution (LTE) can be used in Vehicles not having Dedicated Short Range Communication (DSRC) Radio support. LTE can also be used for periodic certificate renewal in PKI based security systems. Similarly, ensuring correctness of communicated data strongly requires a cross-validation of data received from several sources that cannot be influenced simultaneously by an attacker.

As mentioned by authors Chen et al. [2009], another key challenge in the deployment of VANET applications lies in the support to multi-channel operations (safety and non-safety communications) by a single radio DSRC on board unit. The basic issues of DSRC Multi-Channel Operations (IEEE 1609.4) such as 1) inefficient channel utilization due to less mature time division channel switching, 2) indiscrimination of distances to the areas of service coverage, 3) lack of migration to multi-radio devices and 4) possibility of synchronized collisions during the start of channel interval obviously limit the performance of secured VANET applications that rely upon safety communications. Additionally, the application researchers are required to state clearly their application requirements that are to be considered comprehensively by the security protocol researchers along with the practical aspects of realistic VANET environments. Thus finding out a correct trade-off between security, privacy and trust management on one hand and efficiency and reduced overhead on other hand is still an open challenge for the researchers.

9. CONCLUSION

VANET requirements such as low latency, security and privacy demands novel communication architectures for future vehicular applications. Providing safety and comfort to drivers and passengers is a major concern in VANETs as human lives and their commuting times are precious. Thus the vital information propagated by safety applications shall not be altered or dropped during transit and their timely delivery shall be guaranteed. Any unfair activity of malicious users especially on life critical safety information could turn fatal for other users. Thus it is highly required to safeguard critical information from attackers. The dynamic characteristics, hard delay constraints, security, privacy and trust requirements make the design and deployment of VANET applications challenging. In this paper we have given readers an overview on the VANET environment, Intelligent Transport System communication configurations and wireless access standards. We have described a general VANET Model with two of its communication environments. The roles and relationships of several participating entities in these communication environments along with a few important communication patterns are also discussed. The typical security requirements for VANETs are discussed and the categorization of several security threats to these requirements is made. A description on the relevance of these threats for VANETs with illustrations is also made. We have discussed the general working of two types of security schemes, one based on Public Key Infrastructure (PKI) and the other on ID-based cryptosystems. We have outlined the features of various PKI based security schemes and their drawbacks in general. All the PKI based security schemes discussed are found infeasible for availability due to the extra communication requirements incurred in managing the CRLs. As an alternative, we have focused on several ID based cryptosystems and briefly outlined their merits and demerits. In the ID based security schemes discussed, the PKG uses its master private key to generate private keys for the users which lead to key escrow problem. Each of the ID based security schemes discussed in this paper addresses a subset of security issues and they unconditionally trust the PKG as all the cryptography keys are with the PKG. In this paper, we have also discussed an important VANET issue called trust among peers. Various types of trust management models in VANETs and the related research efforts have been summarized. The significant properties of an efficient trust management model are discussed along with a comparative study of few of the existing trust management schemes. Finally the challenges for secured VANET application development are also presented. As future VANET applications are required to be evaluated on both application benefits and network properties, it is required to have a better support from evaluation tools that support simulation and modelling of heterogeneous network scenarios.

There is also a need for cross-layer design of application components that cope up with the agile PHY layer conditions. From this comprehensive and comparative study we could convey that still there is a need for design and development of robust security, privacy and trust management schemes for the successful functioning of VANET applications in typical real time scenarios.

REFERENCES

Al-Qutayri, M., Yeun, C., and Al-Hawi, F. 2010. Security and privacy of intelligent vanets. *Computational Intelligence and Modern Heuristics*.

Chen, C., Zhang, J., Cohen, R., and Ho, P. H. 2010. A trust-based message propagation and evaluation framework in vanets. In *Proceedings of International Conference on Information Technology Convergence and Services*.

Chen, Q., Jiang, D., and Delgrossi, L. 2009. Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications. In *Proceedings of IEEE Vehicular Networking Conference (VNC)*. pp.1–8.

Dotzer, F., Fischer, L., and Magiera, P. 2005. Vars: A vehicle ad-hoc network reputation system. In *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*.

Dressler, F., Kargl, F., Ott, J., Tonguz, O., and Wischhof, L. 2001. Reaserch challenges in intervehicular communication: Lessons of the 2010 dagstuhl seminar. *IEEE Communications Magazine*.

Eichler, S. 2007. A security architecture concept for vehicular network nodes. *ICICS*.

Fuentes, J. M. D., Gonzalez, A. I., and Ribagorda, A. 2010. Overview of security issues in vehicular ad-hoc networks. *Handbook of Research on Mobility and Computing*.

Fussler, H., Schnaufer, S., Transier, M., , and Effelsberg, W. 2007. Vehicular ad-hoc networks: From vision to reality and back. *IEEE Wireless on Demand Network Systems and Services*.

Gerlach, M. 2007. Trust for vehicular applications. In *Proceedings of International Symposium on Autonomous Decentralized Systems*.

Golle, P., Greene, D., and Staddon, J. 2004. Detecting and correcting malicious data in vanets. *VANET*.

Harsch, C., Festag, A., and Papadimitratos, P. 2007. Secure position-based routing for vanets. In *Proceedings of IEEE 66th Vehicular Technology Conference*. pp.26–30.

Jinyuan, S., Chi, Z., and Yuguang, F. 2007. An id-based framework achieving privacy and non-repudiation. In *Proceedings of IEEE Vehicular Ad Hoc Networks, Military Communications Conference*. pp.1–7.

Kamat, P., Baliga, A., and Trappe, W. 2006. An identity-based security framework for vanets. *VANET06*.

Leinmuller, T., Schoch, E., and Kargl, F. 2006. Securing vehicular ad hoc networksposition verification approaches for vehicular ad hoc networks. *IEEE Wireless Communications Magazine*.

Li, C. T., Hwang, M. S., and Chu, Y. P. 2008. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Computer Communications 31,* 12.

Lin, X., Lu, R., Zhang, C., Zhu, H., and Ho, P. H. 2008. Security in vehicular ad hoc networks. *IEEE Communication Magazine 46,* 4.

Mass, Y. and Shehory, O. 2001. Distributed trust in open multi-agent systems. *Trust in Cyber-societies Springer-Verlag*.

Minhas, U. F., Zhang, J., Tran, T., and Cohen, R. 2010. Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence Theory and Practice (IJCITP) 5,* 1.

Patwardhan, A., Joshi, A., Finin, T., and Yesha, Y. 2006. A data intensive reputation management scheme for vehicular ad hoc networks. In *Proceedings of 3rd Annual International Conference on Mobile and Ubiquitous Systems*. pp.1–8.

Plobl, K., Nowey, T., and Mletzko, C. 2006. Towards a security architecture for vehicular ad hoc networks. *ARES*.

Ram, V. R. and Premasudha, B. G. 2014. Investigating considerative factors for robust vanet application development. *The Mediterranean Journal of Computers and Networks 10,* 3.

Raya, M. and Hubaux, J. P. 2005. The security of vehicular ad hoc networks. *3rd ACM workshop on Security of ad hoc and sensor networks*.

Raya, M. and Hubaux, P. 2007. Securing vehicular ad hoc networks. *Journal of Computer Security 15.*

Raya, M., Papadimitratos, P., Gligor, V., and Hubaux, J. P. 2007. On data-centric trust establishment in ephemeral ad hoc networks. *LCA-REPORT-2007-003*.

Raya, M., Papadimitratos, P., and Hubaux, J. P. 2006. Securing vehicular communications. *IEEE Wireless Communications Vol.13,* No.5.

Sabahi, F. 2011. The security of vehicular adhoc networks. In *Proceedings of Third International Conference on Computational Intelligence, Communication Systems and Networks*.

Samara, G., Wafaa, A. H., Al-Salihy, and Sures, R. 2010. Security analysis of vehicular ad hoc networks(vanet). In *Proceedings of Second International Conference on Network Applications, Protocols and Services*. pp.55–60.

Shamir, A. 1984. Identity-based cryptosystems and signature schemes. *CRYPTO84*.

Shurman, M. A., Yoo, S. M., and Park, S. 2004. Black hole attack in mobile ad-hoc networks. *ACM Southeast Regional Conference*.

Sun, J., Zhang, C., and Fang, Y. 2007. An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks. *MILCOM*.

Wang, N. W., Huang, Y. M., and Chen, W. M. 2008. A novel secure communication scheme in vehicular ad hoc networks. *Computer Communications 31,* 12.

Wasef, A., Rongxing, Lin, X., and Shen, X. S. 2010. Complementing public key infrastructure to secure vehicular ad hoc networks. *IEEE Wireless Communications*.

Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., and Hassan, A. 2012. Vehicular ad hoc networks (vanets): Status, results, and challenges. *Springer Telecommunication Systems 50,* 4.

Dr. B. G. Premasudha received her B.E. (Electronics) and MCA from Bangalore University, Karnataka, India; M.Tech (CSE) from JNTU, Telangana, India and Ph.D from Dr. M.G.R. Educational and Research Institute, Tamil Nadu, India. At present she is working as Professor in the Department of Master of Computer Applications, Siddaganga Institute of Technology, Tumkur, Karnataka, India. She has 25 years of teaching experience in the area of Computer Science. She had published several journal articles and conference papers at national and international levels. She had received many best paper awards at international conferences and also received AICTE travel grants to attend few international conferences abroad. Dr. B. G. Premasudha to her credit has several funded projects from various funding agencies and she is currently providing research guidance to five PhD scholars under Visvesvaraya Technological University, Karnataka, India. She had delivered several technical talks at various reputed organizations and chaired technical sessions of several national and international conferences. Her areas of interest include spatial analysis, Location Based Services, Mobile Computing, MANETs, VANETs and Sensor Networks.
email:bgpremasudha@gmail.com

V. Ravi Ram received his B.Sc (Applied Sciences) with Computer Science specialization from Andhra University, Andhra Pradesh, India and Master degree in Computer Applications from Visvesvaraya Technological University, Karnataka, India in 1998 and 2001 respectively. He is pursuing his Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University, Karnataka, India. He is having 14 years of teaching experience in Computer Science. He is currently working as Associate Professor in the department of Master of Computer Applications at Sri Siddhartha Institute of Technology, Karnataka, India. His research interests include Routing and Security in Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks.
email: raviramv@gmail.com

J Miller is the Research Coordinator for innovation in the Discovery Lab the undergraduate robotics and autonomous vehicles laboratory and an Adjunct Instructor within the School of Computing and Information Sciences at Florida International University. His current areas of research include cyber security, cloud computing, wireless sensor and ad hoc networks. Mr. Miller is a former Associate Director at Florida International University's Applied Research Center, where he was Principal Investigator and Program Manager for three large research programs; The Western Hemisphere Information Exchange Program conducting renewable energy, water purification and environmental sustainability research The Western Hemisphere Security Analysis Center an initiative designed to address the seven threats in Global Security (Human Security)and the Strategic Culture Initiative integrating Security, Governance and Development Studies, as well as Security Technologies, into transformative and sustainable solutions. He has authored a book on cyber security, written several book chapters, and published a variety of refereed journal articles. He has travelled, organized and presented at multiple international conferences, including IEEE GLOBECOM, in lectured in both Spanish and English. Mr. Miller is a retired USAF Colonel, rescue/special operations helicopter pilot, and former USAF Foreign Area Officer with assignments in Honduras and Uruguay.
email: Jerryf.miller@yahoo.com

R. Suma received her B.Sc (Computer Science)and Master degree in Computer Applications from Bangalore University, Karnataka, India. She is pursuing her Ph.D. in Computer Science and Engineering from Visvesvaraya Technological University, Karnataka, India. She is having 16 years of teaching experience in Computer Science. She is currently working as Associate Professor in the department of Master of Computer Applications at Sri Siddhartha Institute of Technology, Karnataka, India. Her research interests include Routing and Security in Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks.
email:sumaraviram@gmail.com