13

Security and Privacy of Intelligent VANETs

Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi
Khalifa University of Science, Technology and Research
United Arab Emirates (UAE)

1. Introduction

The rapid advancement and pervasiveness of wireless communications and information technologies are revolutionizing many aspects of the human lifestyle. The convergence of these technologies is enabling the delivery of a wide range of services and applications of personnel as well as public nature. An application area which is expected to benefit greatly from this is advanced vehicle safety. Car manufacturers have started incorporating some of the wireless information communication technologies (ICT) in their cars with applications covering safety, traffic efficiency, driver assistance, and infotainment. They are utilizing the dedicated short range communication (DSRC) to deliver these applications (Eichler, 2007). The goal is to have fully integrated Intelligent Transportation Systems (ITS) that increase the overall safety and efficiency of transportation in the future.

Smart vehicles with the appropriate wireless ICT will in the near future be able to communicate with each other as well as road-side units (RSUs) located at key points on the road, such as junctions. This enables the formation of self-organized networks connecting the vehicles and RSUs. The RSUs can also be connected to a backbone network if needed. This new form of networks is called VANETs (Vehicular Ad-hoc NETworks). In VANETs, the vehicles or RSUs nodes act both as end points and routers. Due to their ad-hoc mobile nature VANETs support context awareness and are emerging as the first viable commercial implementation of MANETs (mobile ad-hoc networks) (Lin et al., 2008; Raya et al., 2006)

VANET is a relatively new technology that enables vehicular communication. A number of companies have managed to introduce products that enable vehicle Internet access. An example of this is the TracNet system, by Microsoft and KVH Industries, which turns the vehicle to a Wi-Fi hotspot with connection to the Internet. The interest by the automotive manufacturers in the technology has gathered momentum in recent years to the point where new standards called the IEEE 1609 WAVE (wireless access in vehicular environment) have started to emerge. The standards basically include enhancements to the IEEE 802.11 in order to support wireless communication among vehicles as well as road side units (Lin et al., 2008; Jiang et al., 2006). However, most of the work done until recently has tended to concentrate on the development of an appropriate MAC (medium access control) layer as well as applications and services.

VANETs are expected to offer tremendous benefits. However, such networks have a number of novel problems that need to be resolved before they get implemented in a practical setting and people have the confidence to use them. Most of the problems are

associated with the security and privacy of VANETs. The major challenges to solve these problems are due to the infrastructureless and high dynamic nature of VANETs. A lot of effort has been put recently to resolve these issues in an efficient and robust manner.
This chapter discusses the security and privacy challenges associated with intelligent VANETs, along with some possible solutions. Following this introduction, Section 2 presents the characteristics of VANETs. Next, VANET security threats and challenges are described. Then Section 4 discusses possible VANET security schemes and their underlying concepts. Next, Section 5 describes an efficient light weight identity based cryptosystem (IDBCS) for VANETs. Furthermore, Section 6 describes a complete system that implements the proposed IDBCS. Finally, Section 7 presents the conclusions of this chapter.

2. VANETs Characteristics

A pervasive (or ubiquitous) network (PN) is a term that refers to a relatively newly emerging technology. It signifies the ability of users to obtain the services and applications of several distinct networks regardless of their location or time. In other words, users can choose to communicate with **A**nyone, **A**ny organization, **A**nytime, **A**nywhere through **A**ny network using **A**ny type of device (A6), if such networks are deployed (Yeun et al., 2005; Theng & Duh, 2008). Figure 1 illustrates the basic concept of pervasive networks.

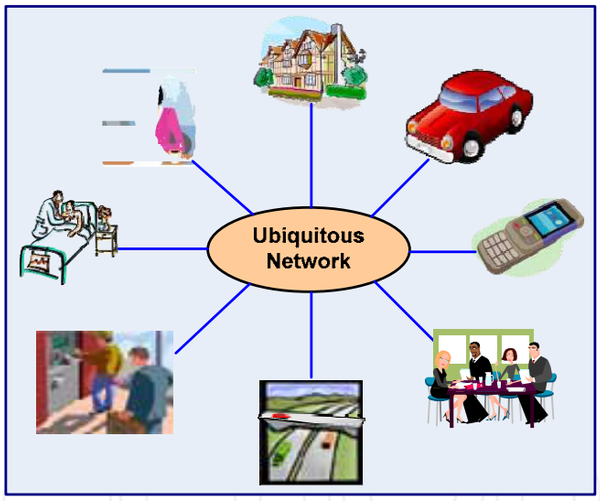


Fig. 1. Pervasive networks

This would provide users with many advantages, such as the ease of communication and the aptitude of linking diverse services into single access points. Due to such desirable features; a lot of effort is being conducted to provide the services for pervasive networks. However, a key issue that needs to be considered is the security of these networks. Currently, there are many security challenges facing PN; how secure such networks are and what are the best methods of delivering such services still remain open problems that need to be addressed (Yeun et al., 2005; Want & Pering, 2005; Connelly et al., 2008).
There are many forms of pervasive networks; most commonly the so-called Wireless Ad-hoc Networks (WANETs). As such networks are based on wireless communication, they provide ease of access but in many instances they are considered less secure than other

communication systems. 'Ad hoc' means that, in such networks, users or 'nodes' are constantly communicating with each other. In other words, these networks are based on node-to-node communication. A node can either be a user who desires certain features or dedicated equipment to manage the service.
Based on the fundamental concepts of WANETs, many other categories have emerged. The most common are: wireless mesh networks, wireless sensor networks and Mobile Ad-hoc Networks (MANETs). The former two categories proved to be useful and are used in some fields like mobile devices' communication and weather monitoring, respectively. Whereas MANETs are those networks that offer high levels of mobility for users and take many forms. One of the most useful forms of MANETs is VANETs, which are also considered the first commercial application of MANETs (Yu & Chong, 2005; Kiess & Mauve, 2007). Figure 2 shows the general breakdown of wireless ad-hoc networks.

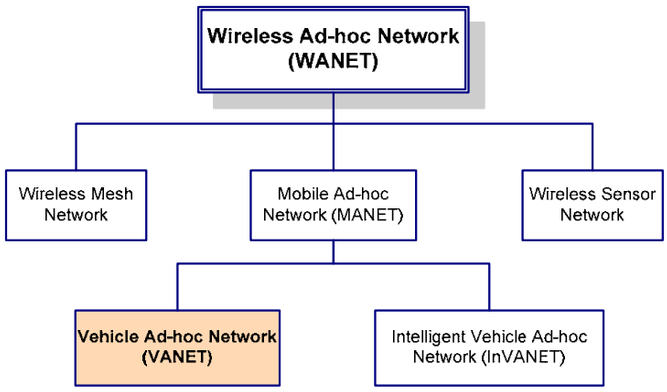


Fig. 2. Hierarchy of wireless ad-hoc networks

VANETs are wireless ad-hoc networks where the nodes, be it vehicles or RSU, can communicate and exchange data for purposes of information inquiry or distribution. The ultimate goal of VANETs is to enhance the driving experience and increase the level of safety for drivers. This can be achieved by allowing nodes within certain ranges (typically 5-10 Km) to connect with each other in order to exchange information (Raya et al., 2006; Nadeem et al. 2005; Dornbush & Joshi, 2007; Schoch, 2008). Figure 3 shows a general view of VANETs structure.

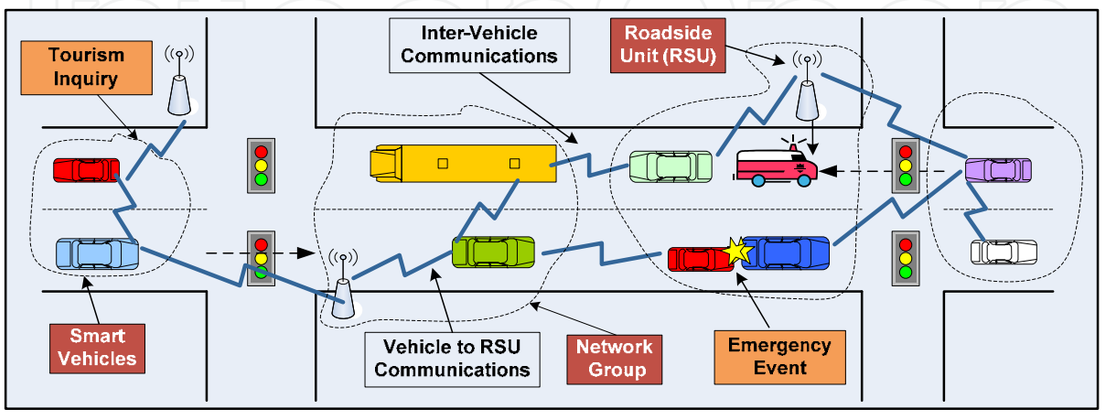


Fig. 3. The basic structure of VANETs

VANETs have a number of distinctive properties that need to be taken into consideration when designing systems to secure them. Those properties include:

- **The nature of communication**: VANETs are based on node-to-node communication; where nodes establish connections with other nodes in order to exchange information of different nature. This topology is referred to as a 'distributed' network; however in some cases, VANETs can be of a 'centralized' nature where a single authority has higher level of control. Moreover, nodes can rely on other nodes to make decisions about route selections for example. Communication can take many forms, for example a node can specifically request some information from another node, or RSU can exchange information with nodes as they pass by for database updates and so on. Obviously, this nature of communication raises many security issues which will be discussed later. Furthermore, a node in VANETs can either act as a host requesting data or a router distributing data.
- **Mobility & Dynamic-nature**: since VANETs are one form of MANETs, the 'mobility' feature is expected to be inherited. In VANETs, nodes are constantly changing their locations (except RSUs) with different speeds and directions, which make the network very dynamic in nature. For instance, a number of nodes can communicate once a group is set up. But the group can rapidly change its structure if a node leaves the group or another join it, as shown in Figure 4. This, in turn, makes it challenging to establish security protocols for a group of nodes or even to guarantee that communication is successful.
- **Frequent exchange of information***:* because nodes are very mobile in VANETs, it is expected that nodes are continuously exchanging information with any number of other nodes.
- **Real time processing & self-organizing***:* because of the properties mentioned above, VANET communication requires fast processing of information that does not take time in order to correctly exchange information. Furthermore, since nodes are mobile, the network is organized in different 'topologies' each time.

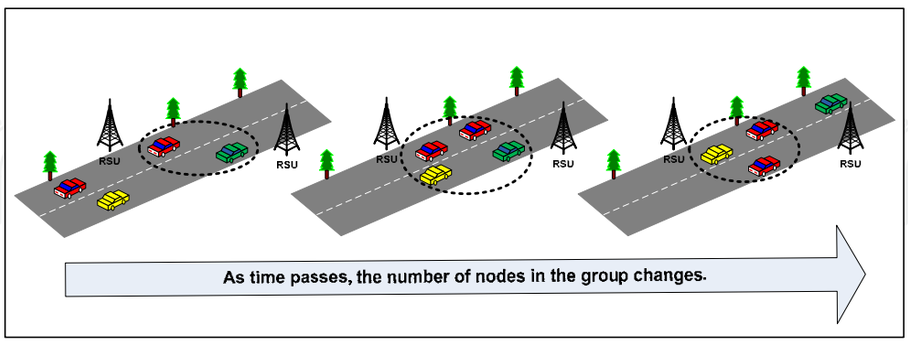


Fig. 4. The dynamic nature of VANETs

- **Infrastructure-less nature***:* nodes are not connected by any sort of physical mediums in VANETs; it is completely based on a wireless 'infrastructure-less' environment. This, as will be discussed later, raises some security concerns in managing VANETs communication.

- **Low volatility***:* obviously, in VANETs nodes are only in range of communication for short period of times. This causes context and data to be changed rapidly because there are many data being exchanged as nodes travel.
- **Data value vs. distance***:* VANETs can provide communication over 5-10 Km ranges. As mentioned previously, nodes form virtual groups to connect and exchange information. However, the value of the information decreases as data travels further from the origin. This is because information is susceptible to various types of attacks which affect its validity (Golle et al., 2004; Zhao & Cao, 2008).
- **Other properties***:* there are other properties that concern the physical and statistical aspects such as: no two nodes may exist in the same location at the same given time or that nodes rarely travel at an average speed greater than 120 Km/h. These properties help in producing more rigid security protocols.

VANETs can provide many applications that are safety or entertainment oriented. Examples include: the provision of road conditions information, traffic conditions, accident reporting which help the authorities to maintain road status, entertainment and internet access and many more (Raya et al., 2006; Boukerche et al., 2008). The diversity of applications is driven by the fact that VANETs are ultimately considered a form of pervasive networks.

Figure 5 illustrates some of these applications as they could occur in VANETs. In scenario 1 after the accident occurs; the vehicles involved in the accident notify RSU 1, which notifies RSU 2 and RUS 3 about the accident. RSU 3 notifies authorities about the location and recommends alternative routes for vehicles headed towards that location. In scenario 2 a new vehicle to the town can communicate with a RSU to provide it with directions to a nearby gas station.

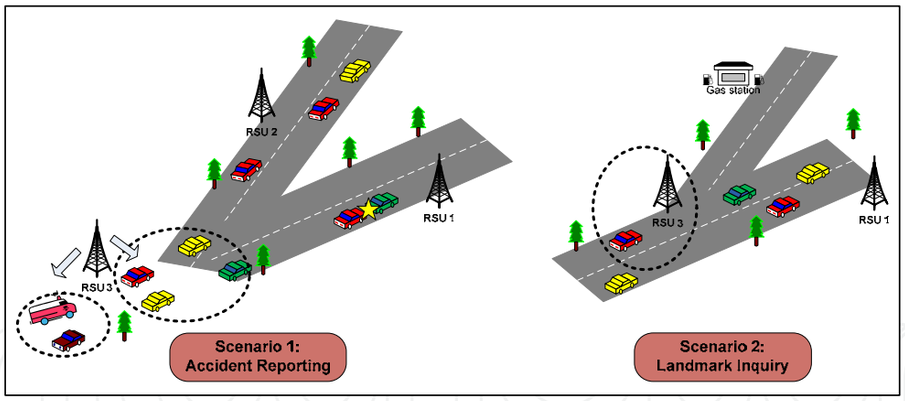


Fig. 5. Some applications of VANETs

Currently, communication in such networks as VANETs is based on the IEEE 802.11 (i.e. Wi-Fi) standards with its different enhancements (802.11b/g). Some applications of VANETs; such as toll payments, also rely on DSRC standard. However, these methods introduce some latency problems which are intolerable in such networks. Therefore, the IEEE is developing a new enhancement to the 802.11 standard that will improve communication for such network. The new standard, known as IEEE 802.11p, will be based on DSRC but with an addition of WAVE. This will support both Vehicle-to-Vehicle (V2V) and Vehicle-to-RSU (V2R) communication in VANETs (Eichler, 2007; Yang & Wang, 2007).

3. VANET Security Threats and Challenges

This section discusses the types of security attacks and network adversaries that can pose a threat for VANETs. It also highlights the major security and privacy challenges facing them.

3.1 Adversaries

Just like any other wireless network, there are many different catastrophic attacks that can occur in a VANET. Before we classify these attacks, it is good to look at how adversaries are categorized. A node is considered 'adversary' if it attempts to inject any type of misbehavior in the network that might cause other nodes (i.e. victims), and ultimately the network, to function improperly (Haubaux et al., 2004; Papadimitratos et al., 2008). Attackers can be of several forms each with different levels of impact on the network, some of these are:

- **Drivers looking only for their best interest:** for example a node might deceive other nodes that a certain route is blocked in order to clear the path to its (adversary's) destination.
- **Users who misuse VANETs:** for example a robber might try to extract data from the network to help him locate places with no cars (i.e. most likely no people), and hence break-in to that place which could be a house.
- **People from within the industry:** this category has a major impact on the security of VANETs since they can access core information about a vehicle (node) as it is manufactured.
- **Malicious attackers:** this is considered the most dangerous category since they can cause severe damage to the network. Possible attacks from this category can be ranged from eavesdropping to terrorism attacks.

3.2 Attacks and Threats

As in other communication networks, there are numerous attacks that can disturb the security of the VANET and the privacy of its nodes. Each type of attack affects some of the security services in the system; termed 'CIA' which stands for Confidentiality, Integrity, and Accountability, and Availability. In general, attacks fall into 4 categories (Maiwald, 2003) as shown in Table 1.

Type of Attack	Definition	Affected Characteristic
Access	An attempt to obtain unauthorized information.	**Confidentiality**; because information is exposed to unauthorized parties.
Modification	An attempt to alter and change information that is unauthorized to change.	**Integrity**; because correctness of information is compromised.
Denial of Service	An attempt to deny usage or access of information for legitimate users.	**Availability**; because the services of a network might not be available for users
Repudiation	An attempt to give incorrect information or deny the occurrence of events.	**Accountability**; because information is no longer liable.

Table 1. Categories of Attacks

Below is a listing of the most common and devastating forms of attacks that a VANET can suffer:

- **Denial of Service (DoS):** a very simple, but yet lethal attack. In this attack a node might continuously send unwanted data across the network so that it enters a grid-lock state where other nodes are unable to communicate due to channel blocking. This attack can either deny access to information or applications or even the whole VANET (Maiwald, 2003; Parno & Perrig, 2005; Raya & Hubaux, 2007).
- **Interception:** where a node plays the 'man-in-the-middle' role so that information exchanged between two nodes passes by the adversary node. Hence, it gains information that is intended to other destinations.
- **Fabrication:** where attackers send incorrect information to other nodes for different purposes. For example, a node sending false data about traffic conditions in certain roads. These types of attacks can be very dangerous because they affect the validity of the data received by nodes (Parno & Perrig, 2005; Raya & Hubaux, 2007).
- **Impersonation:** attackers can pretend to be what they are not in order to gain access to certain information or to aid other attacks by pretending to be a vehicle when in fact it is a stationary adversary (Raya et al., 2006; Raya & Hubaux, 2007).
- **Alteration & suppression of data:** in these types of attacks, adversary nodes can receive valid data, alter it and resend it to other nodes. Moreover, an adversary can prevent communication between two nodes by dropping certain messages between them. These attacks cause false data and confusion to be distributed among the network nodes and hence it affects performance (Golle et al., 2004).
- **The Sybil attack:** a malicious node attempts to make other nodes, which in turn, make other nodes malicious and hence control significant portions of the network and misuse it. This attack is as dangerous as DoS attacks because it can destroy valid communication in the network (Golle et al., 2004; Yan et al., 2008).

3.3 VANET Security and Privacy Challenges

VANETs are considered a relatively new area of research. Many research papers explore the nature of VANETs and how to implement them. However, recently the network security design issues of VANETs are becoming a major area of interest for researches in order to enable assure future users of the robustness of such system (Raya et al., 2006; Lin et al., 2008; Jakubiak & Koucheryavy, 2008).

One of the major challenges of securing VANETs is *communication security*. This aims to provide secure communication between vehicles, which is referred to as Inter-Vehicle Communication (IVC), and between vehicles and Road Side Units (RSU); Vehicle-to-RSU communication (VRC). Any security framework must ensure that basic security services are provided in VANETs. These services include: information confidentiality which aims to prevent unauthorized access to information. Also, integrity of exchanged messages must be provided in order to detect and prevent malicious intent such as information alteration.

Additionally, node authentication is important to ensure that all nodes within the network are who they claim to be and hence prevent impersonation. Other services include: availability of network services for all users at all times and accountability which aims to associate events with particular nodes for future references in order to prevent attempts to provide false claims or reject true ones (i.e. a node claiming that it was not at a certain location; where in fact it was) (Raya et al., 2006; Maiwald, 2003). A lot of work has been done

to achieve security in VANETs; the use of cryptography primitives such as encryption and digital signatures proved to be able to provide security services discussed above (i.e. confidentiality, integrity, authentication, etc.) in vehicular networks.

Another salient challenge that faces the security of VANETs is *key management*. The key in the security domain is the number sequence that is used to encrypt and decrypt information. The issue of key management has many categories that must be resolved when designing security protocols for such networks. One category is key revocation which is the process of discarding suspected key or keys that are bound to malicious nodes. Traditional methods of revocation such as Certificate Revocation Lists (CRLs) are not suitable for VANETs due to the large scale of the network (Lin et al., 2008). A second category of this challenge is group key management since VANETs inherit the characteristic of mobility from MANETs.

Furthermore, *detection of malicious nodes and intentions* is considered the most challenging issue in VANETs so far. The reason for that is because it is easy to access data in the network and hence data validity is compromised. Consequently, it becomes much more difficult to distinguish valid data from malicious data. What makes this even worse is that in VANETs there are no guarantees that previously honest nodes do not turn to malicious nodes in the future. Furthermore, in such networks it became desired to prevent the attack before it occurs which really calls for strong security algorithms (Yan et al., 2008; Li & Joshi, 2009).

Location verification is another challenge for VANET security. Currently in VANETs, position coordinates can be verified using either a GPS unit, a RSU, or via inter-vehicle communication (IVC). All of these methods are considered weak since an attacker can easily fool a GPS unit or manipulate RSUs or even forge data via IVC. Position verification plays a vital role to prevent many attacks like impersonation. It also helps in the data validation process. Therefore, a solid method to verify nodes positions' is required to help improving the security of VANETs (Haubaux, 2005; Golle et al., 2004; Yan et al., 2008).

These two challenges are quite significant because they intervene with the privacy of the node, i.e. drivers are not willing to reveal their routes and driving habits to be exposed by others. Consequently, they lead to another major challenge in securing VANETs which is *privacy preservation* (Rahman & Hengartner, 2007; Raya & Hubaux, 2007; Wang et al., 2008).

The privacy issue is concerned with protecting personal information of drivers (name, location, plate number, etc.) within the network. The network protocol has to be designed in a way that hides this information from other nodes; but allows it to be extracted by authorities in cases of accidents or malicious intent as a mean of auditing for authority usage. Hence, achieving 'conditional' privacy is desirable for VANETs rather than unconditional privacy which is a major challenge. Moreover, the tradeoff between robustness measures, such as the inclusion of personal information during communication which makes the task of malicious node detection easier, and the protection of drivers' information makes the issues of privacy more challenging (Lin et al., 2008; Yan et al., 2008).

The *trade-off between robustness and the level of privacy* a protocol grants is also a key challenge facing VANETs. Any proposed security algorithm must take into consideration the impact on the users and how well will the public accept it because their privacy is involved in such matters. This becomes a problem when an algorithm mainly depends on personal data as unique identifiers, in order to be robust enough, that can be traced back to a specific user. For example, the public might consider it intrusive if the algorithm requires the use and exposure of their biometric data. Hence, proposing a security protocol that is robust enough

to secure VANETs communication, yet be well-accepted by the public is still an open problem (Raya & Hubaux, 2007).
Other challenges facing VANETs include *time sensitivity* and *network scale*. The time required to process information in such networks is vital because as mentioned previously, nodes are only within the communication range for short period of time. This forces communication methods to be of real-time processing nature because nodes need to exchange, verify and prevent attacks as they are travelling at high speeds. So, we need security methods that take this issue into consideration. It is also clear how the issue of network scale can turn to a challenge when talking about such dense networks as VANETs. Huge number of vehicle, of different origins and manufactures, makes it really difficult to manage communication and security in the network (Raya et al., 2006).
The eventual goal of VANET security protocols is to provide a vehicular communication network that is able to resist malicious activities and attacks and provide the highest possible level of node privacy. This is very challenging due to some of the unique features of VANETs such as the high mobility and the large network scale (i.e. millions of vehicles). Such features make it more difficult to design protocols that will provide secure communication and prevent many types of security attacks, as well as protect all personal information of drivers unless it is absolutely required.

4. VANET Security Schemes & Concepts

This section presents a literature review for the security of VANETs and classifies the approaches used to overcome security challenges. The section also includes an explanation of the Identity Based Cryptography as it is the center of the system developed in the chapter. Then it explains in details important cryptographic concepts that are related to this chapter.

4.1 Symmetric Key Approaches

Symmetric Key systems were the first type of cryptosystems used to secure information. In these systems, nodes can only communicate after sharing and agreeing on a secret key that is used to process communication messages. As stated previously, VANETs are a relatively new research area and the security for such networks is only starting to be a major research topic. Hence, there are not many papers that propose the use of such systems for VANET security as the attention is more directed towards Public Key and Identity Based systems. Nevertheless, this section discusses existing proposals of using Symmetric Key systems for VANET security.
In (Burmester & Chrissikopoulos, 2008) a hybrid system that uses both Symmetric and Public Key operations is proposed to provide security for VANETs. The hybrid system provides authentication, confidentiality and privacy preservation. To achieve this it defines two types of communication within VANETs: pair-wise and group communication. The former type occurs when two nodes require exchanging messages, whereas the latter is established when more than two nodes require communication. They propose the use of symmetric keys when pair-wise communication occurs in order to avoid introducing overhead of using a key pair (i.e. public key systems). However, they point out that symmetric keys should not be used in the authentication process since it might prevent non-repudiation. The symmetric key generation process is explained in (Burmester & Chrissikopoulos, 2008) and the key size is 1024 bits and they suggest the use of the

Advanced Encryption Standard (AES) (a symmetric key scheme) for the encryption process (Daemen & Rijmen, 2002; Stallings, 2002).

4.2 Public Key Approaches

Public key schemes were most widely used prior to the introduction of ID-based ones. In Public Key frameworks, each node is granted a pair of keys: a secret key and a public key. These are used in security operations when communicating with other nodes. Is it very important to note that in order to implement this framework; a Public Key Infrastructure (PKI) is required to handle key management operations. Based on such frameworks, the security protocol can also offer desirable features such as certificate revocation and privacy of nodes. Related works in these two fields are discussed in this section.

In (Hubaux et al., 2004) security and privacy issues in vehicular communication are addressed. They highlighted how privacy concerns arose due to the fact that the license plates were replaced with electronic identities as a method of tracking vehicles used by authorities. They proposed the use of public key cryptography in vehicular communication in order to allow authorities and vehicles to certify identities of other vehicles; using 'Electronic License Plates' (ELP).

They also suggest desirable privacy protocols that preserve drivers' personal information and mention some applications that could use the ELP. Solutions are also proposed for some types of attacks like impersonation. To ensure privacy preservation, they point out that privacy protocols must be based on anonymity schemes that hide the relationship between drivers' information and some random identifier. The article also addresses the problem of location verification in vehicular networks. It argues that GPS-based systems have more weaknesses that strengths and hence proposed the use of distance bounding protocols for the purpose of location verification in vehicular networks.

In (Raya et al., 2006), another new architecture is proposed where vehicles have two extra hardware units; the Event Data Recorder (EDR) to record all events and the Tamper-Proof Hardware (TPH) that is capable of performing cryptographic processing. The article argues that the proposed architecture provides authentication, authorization and accountability. They suggest the use of public key cryptography with a manageable and robust PKI since symmetric key cryptography do not support accountability. Authentication is performed by digital signatures of communicated messages; they proposed the use of Elliptic Curve Cryptography (EEC) since it reduces the processing requirements.

4.2.1 Certificate Revocation

In (Raya et al., 2006) a security architecture for vehicular communication that aims to provide security services for such networks is proposed. They highlight the salient challenges facing vehicular networks such as: the network scale, the privacy issues and the real-time requirements. They also describe the types of security threats and attacks that such network are susceptible to such as: impersonation, information forgery and tempering with traffic. They also proposed a novel certificate revocation technique through three protocols: the Revocation protocol of Tamper-Proof Device (RTPD), Distributed Revocation Protocol (DRP) and Revocation protocol using Compressed Certificate Revocation Lists (RCCRL). These protocols are introduced since they argue that standard methods of revocation such

as Certificate Revocation Lists (CRLs) causes substantial amount of overhead and requires pervasive infrastructure.
Furthermore, (Lin et al., 2008) discussed the current standards for providing security in vehicular communication. They described how the IEEE 1609 WAVE standards (i.e. DSRC) supports security for IVC and VRS. The IEEE 1609.2 standard provides security measures that require the use of public key cryptography with ECC support for some applications. However, drivers' privacy preservation issues are not addressed in these standards. The Vehicle Safety Communication (VSC) project by the US Department of Transportation resolves the privacy issues through the use of CRL.
The articles explains the disadvantages that prevent such methods of being suitable for vehicular environments; such as the network scale which is substantial in VANETs and causes the CRL to grow rapidly and hence increase processing requirements when revocation is required. Furthermore, it is highlighted the CRL are considered centralized approaches which do not suit VANETs because of the property of high mobility.
A novel certificate revocation scheme termed RSU-aided Certificate Revocation (RCR) is proposed by (Lin et al., 2008). In this method, the TTP grants secret keys for each RSU which enables it to sign all messages communicated within its range. Whenever a certificate is detected to be invalid; the CA issues a warning message to all RSUs which in turn use broadcast messages to all vehicles in respective ranges in order to revoke the particular certificate and stop all communication with that node. They also explain silent attacks (i.e. where a node disables message broadcasting feature in order to be camouflaged from the RSU). Figure 6 is adopted from (Lin et al., 2008) and illustrates the novel RCR method.

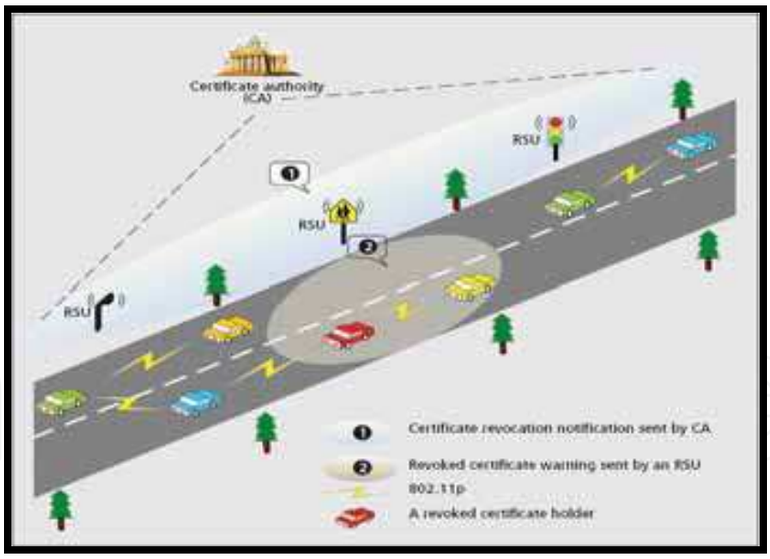


Fig. 6. RSU-aided certificate revocation

4.2.2 Pseudonym Based Approaches for Privacy

In (Raya, et al., 2006) a novel approach for privacy preservation is proposed by using of a set of anonymous keys, which have short life-times, that is previously stored in the TPD for a certain amount of time, i.e. a year or several months. Once a key is used it is declared void and cannot be used again and all key distribution and management is performed by the CA

of the network. However, they stress on the point that these keys have to be traceable to the driver only in case of emergencies or authority requirements.
In (Lin et al., 2008) the 'conditional' privacy preservation in VANETs is addressed. This is a desirable characteristic for VANET because it ensures that recipients are not able to extract senders' personal information; however, authorities are able to do so in cases of accidents or network misuse. They explain why the pseudonym-based approaches are not suitable for VANETs since at each revocation process, the CA is requires to search exhaustively a large database. Moreover, as the network scale grows larger, CRL become very difficult to manage. They explain the previously proposed scheme for conditional privacy in (Lin et al., 2007); the Group Signature and Identity-based Signature (GSIS).
The scheme categorizes the process into two groups: On Board Units (OBS) to OBU and RSU to OBU; which ultimately refers to IVC and RVC. The first group uses short-group signature schemes to ensure the anonymity of communicating nodes, and IBS are used in the second group where all RSU messages are signed and the overall cryptographic overhead is reduced since it is an identity-based approach. GSIS also prevents what's called the 'RSU replication attack where a compromised RSU is relocated in order to misuse the network and spread malicious data.

4.3 Identity-Based Cryptography

Recently, this approach became the mainstream for VANET security frameworks as it is considered a viable choice due to the properties of VANETs. As mentioned previously, earlier proposed security schemes relied on the use of public key cryptography (PKC) and/or symmetric key cryptography (SKC). However, recent researches discovered that such cryptography methods are not the 'best' choice for security in VANETs. One important characteristic of VANETs is that they are of infrastructure-less nature; hence the use of PKC is not suitable since it requires a Public Key Infrastructure (PKI) which deals with issues of key distribution and management. Moreover, sizes of the keys and certificates pose a constraint on the use of PKC in such networks since the bandwidth is limited in such dynamic wireless environments. Also, because VANETs require real-time responses and cannot tolerate delays in communication; SKC is also not considered a good choice (Kamat et al., 2006). Therefore, IDBC is currently considered a viable choice to provide security in VANETs.

4.3.1 Identity-Based Signature

The basic idea of identity-based signature (Shamir, 1984) is to provide secure communication without the requirement of a public/private key pair. IDBC is based on an underlying public key cryptosystem. However, instead of generating a key pair, an arbitrary string that uniquely identifies the user can be used as his public key. The private key is then generated by a Third Trusted Party (TTP) and issued to the user (Shamir, 1984). However, (Shamir, 1984) was only able to propose a functional Identity-Based Signature (IBS) scheme but not an encryption scheme.
As stated previously; IDBC requires an underlying public key cryptosystem, but Identity-Based Encryption (IBE) scheme requires two additional requirements: the ability of easily computing private keys from a random seed and the intractability of the process of computing this seed if a public/private key pair is known. At that time, the proposal used

RSA (Shamir, 1984) as the underlying public key cryptosystem which did not satisfy the two additional requirements for an IBE scheme, and hence it was an open problem. Figure 7 below illustrates a general view of the proposed IBS scheme by (Shamir, 1984).

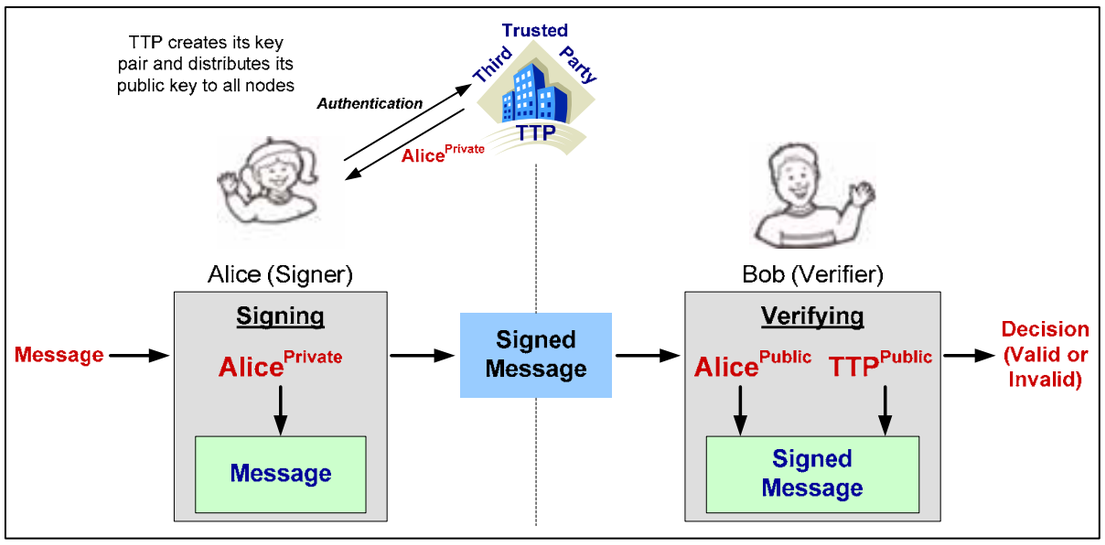


Fig. 7. A General Identity-Based Signature Scheme

The signing/verifying process is performed in 4 steps (Baek et al., 2004):

- **Setup:** TTP creates its own pair of public and private key (master secret) and distributes its public key to all parties within the network.
- **Extraction:** the signer of the message (Alice) authenticates herself to the TTP and requests her private key ($Alice^{pri}$), which is generated by the TTP and issued to Alice.
- **Signing:** the signer (Alice) uses her private key ($Alice^{pri}$) to sign the message and send it to Bob.
- **Verifying:** Upon receiving the signed message, the verifier (Bob) uses the public key of Alice ($Alice^{pub}$) and the public key of the TTP (TTP^{pub}) to make a decision whether the signature is valid or invalid.

4.3.2 Identity-Based Encryption

The IBE open problem was solved by (Boneh & Franklin, 2001) with a fully functional scheme based on the Weil Pairing (Stinson, 2005). The strength of the scheme they proposed was based on the intractability of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which will be discussed in the later.

The encryption process shown in Figure 8 is performed in 4 steps (Baek et al., 2004):

- **Setup:** TTP creates its own pair of public and private key (master secret) and distributes its public key to all parties within the network.
- **Extraction:** the recipient (Bob) authenticates himself to the TTP and requests his private key (Bob^{pri}), which is generated by the TTP and issued to Bob.

- **Encryption:** the sender (Alice) uses the Bob's public key which is the arbitrary string (Bob^{ID}) and the public key of the TTP (TTP^{pub}) to encrypt the message and send it to Bob.
- **Decryption:** Upon receiving the encrypted message, Bob uses his private key (Bob^{pri}) to obtain the original message.

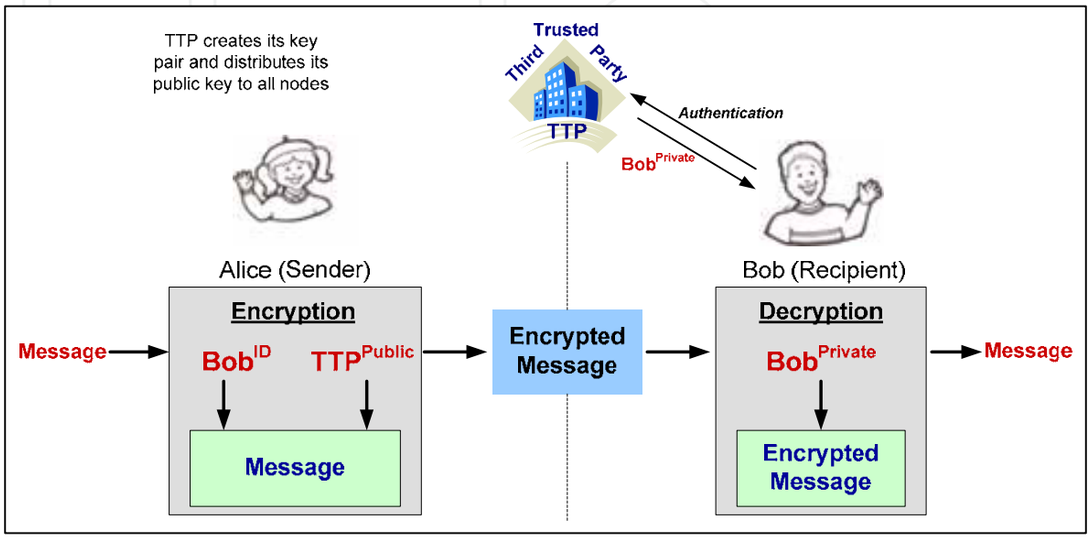


Fig. 8. A General Identity-Based Encryption Scheme

The strength of the security offered by IDBC is based on four key points as stated in (Shamir, 1984):

1. The strength of the underlying public key cryptosystem.
2. The level of secrecy of all information acquired and stored in the TTP.
3. The strength of the authentication methods performed prior to private key issuance.
4. The methods and precautions by which private keys are guaranteed not to be leaked.

4.3.4 Identity-Based Approaches

Few researchers proposed the use of IDBC for VANET security. In (Sun et al., 2007) an ID-based framework is presented that could achieve privacy and non-repudiation; along with the fundamental security features, in VANETs. The importance of having privacy preserved in such network is highlighted as a key issue to attract vehicles to join such vehicular networks. The proposed framework includes a justification as to why previously proposed ID-based solutions to achieve privacy; such as ring signatures, do not suit VANET environments since it results in 'unconditional privacy'. The latter term refers to the inability to reveal the identity of vehicles under all circumstances; which should not be the case in VANETs. This is resolved by (Sun et al., 2007) through the use of 'distributed control', where a single authority is unable to reveal drivers' personal information. Instead, multiple authorities can participate in a collaborative process in case an identity needs to be revealed for legal reasons.

The framework relies on the pseudonym-based approach to achieve non-repudiation in VANETs. This approach was introduced previously in (Raya et al., 2006) and it involves

preloading vehicles with a set of short-lived keys that cannot be used more than one time, hence other vehicles are unable to track the identity of particular vehicles. They proposed the addition of a Pseudonym Lookup Table (PLT) that can be used to associate random identifiers (pseudonyms) with the real identity of the vehicle.
In (Sun et al., 2007) the authors also suggest the use of existing wireless infrastructure to perform key revocation processes since there does not exist a dedicated vehicular communication infrastructure. However, the proposed framework assumes the use of Tamper-proof Hardware (TPH) which ensures that the master secret of the TTP is never disclosed. Although the proposed framework is based on IDBC; they also require the use of public or symmetric key cryptography for further communication once mutual authentication has been established between nodes in VANETs. The proposal suggests a method based on ID-based threshold signatures to provide non-repudiation services for authorities in VANETs.
In (Kamat et al., 2006) another IDBC is proposed for VANET security. It stressed on the indispensability of security and privacy in VANETs in order for them to be well-accepted by the public. They point out that VANET nodes should be able to mutually authenticate with other nodes; but protect the identity of themselves in order to grant privacy services. It explains why traditional cryptography techniques cannot be used in VANETs environments and why IDBC is possibly the 'best' solution to resolve VANET security issues.
The paper also proposes the use of 'signcryption' (Baek et al., 2007) which have considerable advantages over standard encryption and signature methods. Such advantages include reduced cipher sizes but they argue that VANET nodes are not computational-power restricted and can perform complex processes of Tate pairings. Their proposal suggests that the base station is the only party that will require storing CRLs, hence preserving a substantial amount of storage space in vehicles. Moreover, the issue of non-repudiation is also addressed and explained in details in (Kamat et al., 2006).

4.4 Cryptographic Mathematical Concepts

The field of cryptography is very much based on the number theory and other mathematical concepts (Stinson, 2006; Washington, 2007; Menezes et al., 1997). There are several mathematical terms that are used in cryptography; this section explains the most important ones. Most of the notations used in this section will be reused later in this chapter.

- **Roots of Unity:** all complex number that yield the value of 1 when raised to a given power n. Also referred to as de Moivre numbers (Conway & Guy, 1995); they can be represented on the unit circle of the complex plane. Mathematically, n^{th} root of unity is defined as a complex number that satisfies:

$$Z^n = 1; \quad n = 1, 2, 3 \ldots$$

- **Cyclic Groups:** a group **G** of elements is called 'cyclic' if a generator '**g**' element exist such that all the elements of the group can be represented as a power of **g** (the multiplicative representation) or a multiple of **g** (the additive representation) (Joseph, 1998). It is defined as:

$$G = < g > = \{ g^n \mid n : \text{int} \, eger \}$$

For example; suppose that $G = \{g^0, g^1, g^2, g^3, g^4\}$ is a cyclic, then $g^5 = g^0$, $g^6 = g^1$ and so on.

- **Group Generator:** a subset **S** of a group **G** is referred to as the 'generating set of **G**' if every element in the group **G** can be expressed as a product of a finite number of elements in the subset **S** (Arfken & Weber, 2005). If $G =< S >$ then it is said that **S** generates **G** and the elements of **S** are called generators of **G.**
- **Group Order:** the order of a group **G** is defined mathematically as the number of elements in the group (i.e. the group's cardinality) (Arfken & Wber, 2005). For example, if $G = \{1,2,4,7\}$ then the order of **G** is denoted as:

$$|G| = 4 \quad OR \quad ord(G) = 4$$

- **Abelian Groups:** a group is called 'Abelian' if operations on elements within the group do not depend on their respective orders. These groups are characterized as commutative and associative. Moreover, an inverse element exist for each element in an Abelian group and the group posses the identity element (Finch, 2003). Generally, these groups can be represented in two ways: additive and multiplicative notation. Table 2 below defined the convention for each representation.

Convention	Operation	Identity	Powers	Inverse
Addition	$x + y$	**0**	Nx	$-x$
Multiplication	x * y	e or 1	x^n	x^{-1}

Table 2. Abelian Groups' Conventions

- **Torsion Group:** a group **G** is called 'Torsion' or periodic if all elements within the group have finite orders. The order of an element **x** in **G** is defined as the smallest integer '**n**' such that:

$$x^n = e; \quad e \, is \, the \, identity \, element \, of \, G$$

If no **n** exist such that the above equation is satisfied; then the element is said to have an infinite order (Armitage & Eberlein, 2006).

- **Bilinear Maps:** are defined as mathematical functions that map the product of 2 linear elements to a third element; all within the same group (Boneh et al., 2003). For example, let **X** and **Y** be linear elements of **G**, then the bilinear map is defined as:

$$F : X * Y \rightarrow Z \text{ ; Z is a third element in G}$$

An example of a bilinear map is the multiplication (i.e. a mathematical function) of elements in the integer group **N**. For instance

$$2, 3 \; \varepsilon \; N \; and$$
$$2, 3 = 6 \; \varepsilon \; N$$

Hence integer multiplication is a bilinear map.

4.5 Strength of Cryptosystems

It is a well-known fact that there does not exist a security algorithm that is mathematically proven to be secure (Stinson, 2006; Menezes et al., 1997). The core of any cryptosystem is a computationally infeasible problem; which is not proven to be 'unbreakable' but assumed to be computationally hard. Hence, such problems allow the use of cryptosystems that are based on the intractability of these problems. This section explains these mathematical problems.

4.5.1 The Discrete Logarithm Problem

This is considered the base mathematical problem that allows cryptosystems to be considered secure. As long as the Discrete Logarithm Problem (DLP) is computationally infeasible and cannot be solved; cryptosystems based on these problems are considered secure (Stinson, 2006). For instance, the famous ElGamal Cryptosystem is based on the assumed hardness of the DLP. The DLP is described below:

Given a group G, $\alpha \in G$ *with order n and* $\beta \in <\alpha>$
find the unique integer ***a*** *such that:*
$$a^{\alpha} = \beta w$$
where ***a*** *is called the discrete logarithm of* β

4.5.2 The Diffie-Hellman Problems

When the Diffie-Hellman key agreement protocol was introduced; its strength was associated with the difficulty of solving the Diffie-Hellman Problem (DHP) which is described below (Diffie & Hellman, 1976):

Given a group $*$ *generator g and some random integers* α, β
if g^{α} *and* g^{β} *are known*
find $g^{\alpha\beta}$

As this problem became very important in the field of cryptography; several variants of the problem were introduced, namely: the Computational Diffie-Hellman Problem (CDHP) and the Decisional Diffie-Hellman Problem (DDHP) which are explained below:

- **The Computational Diffie-Hellman Problem (CDHP):**
  The setting of this problem is similar to the DLP problem (Stinson, 2006).

Given a group G, $\alpha \in G$ *with order n and* $\beta, \gamma \in <\alpha>$
find the unique integer ***a*** *such that:*
$$\log_{\alpha} a \equiv \log_{\alpha} \beta \, x \log_{\alpha} \gamma (\mathrm{mod}\, n)$$
or more clearly, given α^{x} *and* α^{y}*, find* g^{xy}
where x and y are integers

- **The Decisional Diffie-Hellman Problem (DDHP):**
  The setting of this problem is similar to the CDHP, and the problem is to make a decision whether it is the case that the CDHP holds or not (Stinson, 2006). Equivalently, it can be described as:

$$\textit{Given } \alpha^x, \alpha^y \textit{ and } \alpha^z$$
$$\textit{Make a decision whether the following condition holds or not}$$
$$z \equiv xy (\mathrm{mod}\, n)$$

4.6 Elliptic Curves Cryptography

Elliptic Curve Cryptography (ECC) is considered a public key approach for cryptography that is based on algebraic (Abelian) elliptic curve groups over finite fields. The ECC approach allowed many existing protocols and cryptographic schemes to use it in order to have a variant of the original protocol. For example, ECC can be used to construct the Elliptic Curve Diffie-Hellman (ECDH) key agreement scheme where elliptic curves are used to agree a shared key between two parties (Hankerson et al., 2004; Washington, 2008).
As stated previously, the strength of any cryptosystem is based on a computationally infeasible problem. In the case of ECC, this computationally difficult problem is termed the Elliptic Curve Discrete Logarithm Problem (ECDLP). The source of the problem is known as the Scalar Multiplication (SM) of Elliptic Curves. The SM problem is described below:
Suppose that P is an elliptic curve point

$$\textit{Find the result (R) of doubling P several times (K time), such that:}$$
$$P \cdot K = R$$

The difficulty of this problem relies on the infeasible computation of the value **K** where; this is referred to as the intractability of the 'scalar multiplication' of the point **P.** In practical cryptosystems, the value of **K** is very large such that it is computationally infeasible to compute its value using successive doubling operation of the elliptic curve point (i.e. $P \rightarrow 2P \rightarrow 2P + P = 3P \ldots \rightarrow KP$) (Hankerson et al., 2004; Washington, 2008).

4.7 Pairing Based Cryptography

IDBC can be achieved through two main methods: *quadratic residues*; which is a variant of integer factorization and *admissible bilinear pairings* (Baek et al., 2004). The former is proved to be inefficient since it relies on bit-by-bit encryption processes which results in huge cipher-texts (Baek et al., 2004; Stinson, 2006). The scheme proposed by (Boneh & Franklin, 2001) is based on admissible bilinear pairings; which is more accepted and used in the field of IDBC due to its efficiency.
The main concept of PBC is constructing a mapping between two suitable cryptographic groups (e.g. elliptic curve groups) and then being able to reduce the complexity of a problem in one group to be simpler in the other group; hence producing sufficient cryptographic schemes (Galbraith & Paterson, 2008). For instance, the DDHP and the DLP can be easily solved using these mappings (i.e. pairings).

In mathematics, pairings refer to bilinear maps which maps elements of one group to elements of another group and satisfy three conditions: bi-linearity, non-degeneracy and efficient computability. Pairings are explained below (Stinson, 2006; Washington, 2008):

Suppose two groups G1 and G2 (which can be additive or multiplicative)
of the same prime order q
P and Q are generators of G1
We consider a mapping function e: G1 x G1 $\rightarrow$ G2 that satisfies 3 conditions:

Bilinearity:

$$\forall P, Q \in G1 \; and \; x, y \in Z_q^*$$

$$e(xP, yQ) = e(P, Q)^{xy}$$

Non-degeneracy:

$\forall P \in G1$ *and P is a generator of G1*
Then $e(P, P)$ *is a generator of G2*

Efficient Computability:

There exists an efficient algorithm to compute $e \forall P, Q \in G1$

Examples of such pairings include the Weil Pairings and the Tate Pairing (Galbraith & Paterson, 2008). In both cases; one of the two groups is an elliptic curve group and the other is algebraic group of finite field. The strength of current IDBCSs relies on a third variant of the DHP; namely the 'Bilinear Diffie-Hellman Problem' (BDHP) which is explained below (Stinson, 2006).

Given G, q, e, P, aP, bP, and cP
where a, b and c are random elements $\in Z_q^*$
computing $e(P, P)^{abc}$ *is assumed to be hard*

It is important to note that the cryptosystem designed and implemented in this chapter is based on bilinear pairings using the Weil pairing on elliptic curve groups (Boneh & Franklin, 2001).

5. Identity Based Cryptosystem for VANETs

This section explains the specifications of the Identity Based Cryptosystem (IDBCS) developed for VANETs security. It explains the system architecture through the functional, behavioral and data models of the system.

5.1 Functional Model

The main goal of the system developed in this chapter is to demonstrate how VANET security could be achieved using Identity Based Cryptography. The system consists of the main 4 functions of Identity Based Cryptography: setup, extraction, encryption and

decryption; in addition to other functions that are required to construct a complete cryptosystem. Figure 9 shows the *functional decomposition* of the IDBCS.

The IDBCS can be decomposed into the following main modules:

- **System Setup:** this function is responsible for initializing all the parameters that will be used in the system. Parameters refer to: Pairing Based Cryptography elements, elliptic curves and pairing functions.
- **PKG Setup:** this function generates all the key elements associated with the TTP or what is referred to as Private Key Generator (PKG) in IDBC since it is responsible for generating private keys for users. Five keys are associated with the PKG: master secret, system generator, public key, secret signature key and public verifier key. This function also creates three system record files: the medium file which holds all data communicated within the system, the map file which maps messages to random numbers and the status file which stores registered users.
- **User Parameter Extraction:** this function is responsible for generating all key elements associated with the user of the system. These keys will be used in order to complete operations within the system such as: encryption or digital signatures. Similarly, four keys are generated for each user: public, private, signature and verifying key.
- **PBC Elements Management:** the system is designed to hold all secret and/or public keys of users and the PKG in respective files. This function manages the read, write, convert, extract and update operations of all elements and files.
- **User Registration & Authentication:** in order for users to communicate messages with other users using the system; they should first go through a registration process. This function is responsible for acquiring user information, validating input data and creating specific files that will hold all the elements required for the user to use the system.
- **Message Communication:** this function performs the core functionalities of the message communication between two users. It is responsible for extracting the required parameters in order to encrypt the input message, digitally sign it in the sender's side and decrypt the message and verify the signature in the receiver's side. Moreover, it updates the files that are created for each user by these messages sent/received.
- **Check User Status:** this function simply checks if the user is registered in the system or not. If the user is not registered, it passed him to the registration process; otherwise the user is passed to the communication process.
- **System Reset:** this function flushes all PBC and system elements previously generated and deletes all record files created. Performing this function will disable all functionalities of the system unless setup is performed again.

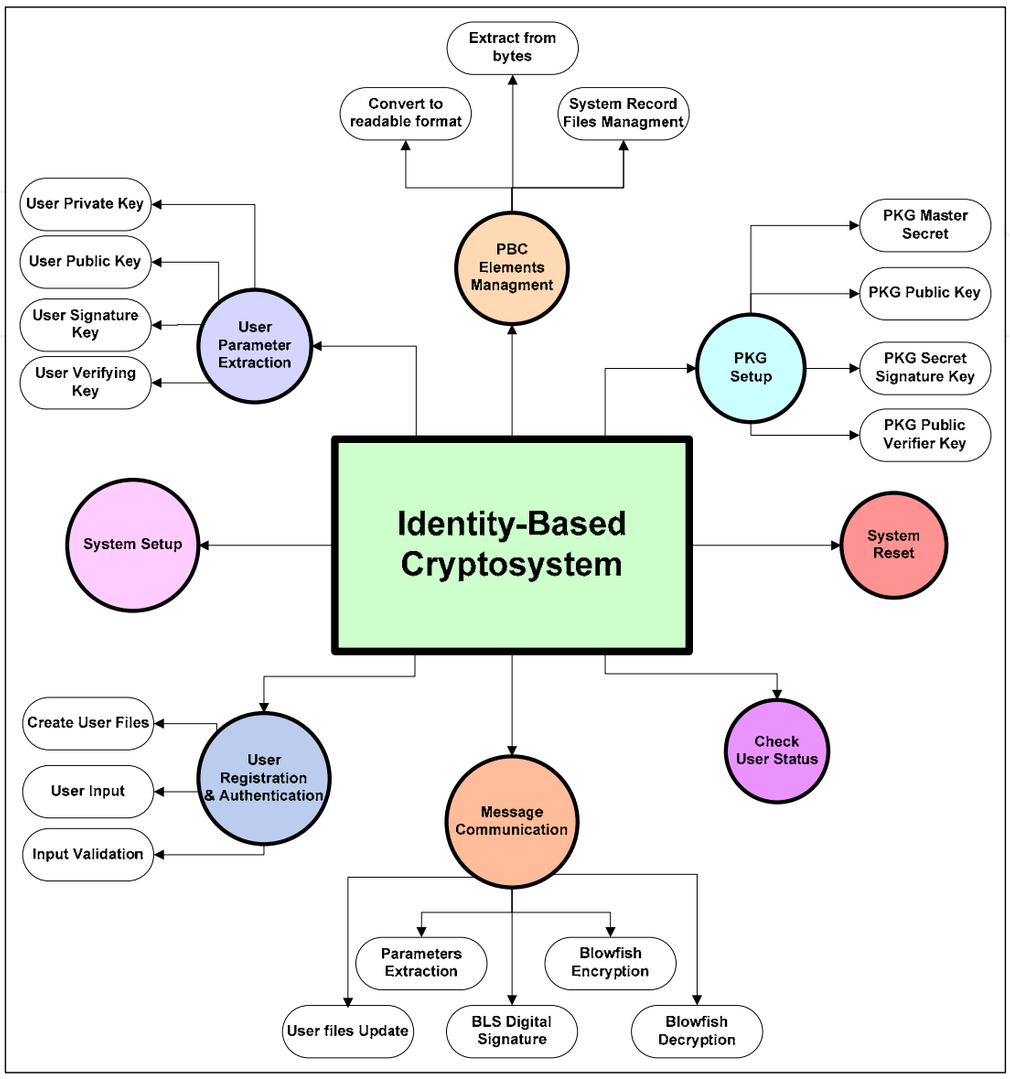


Fig. 9. The IDBCS functional decomposition

5.2 Data Model

The modules that make up IDBCS as depicted in Figure 9 communicate numerous data between them. These communication operations are critical in order for the IDBCS to operate correctly. Figure 10 shows the data flow diagram of the IDBCS.

As can be seen from Figure 10, the system requires data inputs from the user: name, date of birth, vehicle model, vehicle registration number, source and destination plate numbers and the input message the user wishes to send. Moreover, the system requires the parameters from the system setup function in order to produce correct output data for other modules. Additionally, an input is required to choose the function required to be performed.

The outputs produced by the system are directed to different modules which perform certain operation with these data. Below is an explanation of which output data are directed to which modules:

- The function choice determines which function to perform. For each function, specific messages depending on the flow of the system are displayed for the user.
- The PKG and user keys are directed to PKG and user files respectively. Some user information along with timestamp is directed to the users' status update module which adds users to the status file.
- System parameters and the encrypted and signed message are directed to the system record file update module which adds these data to respective files.
- The input message or the decrypted message, a timestamp and source/destination plate numbers are directed to the user message database module which updates the files created for the user with these data.

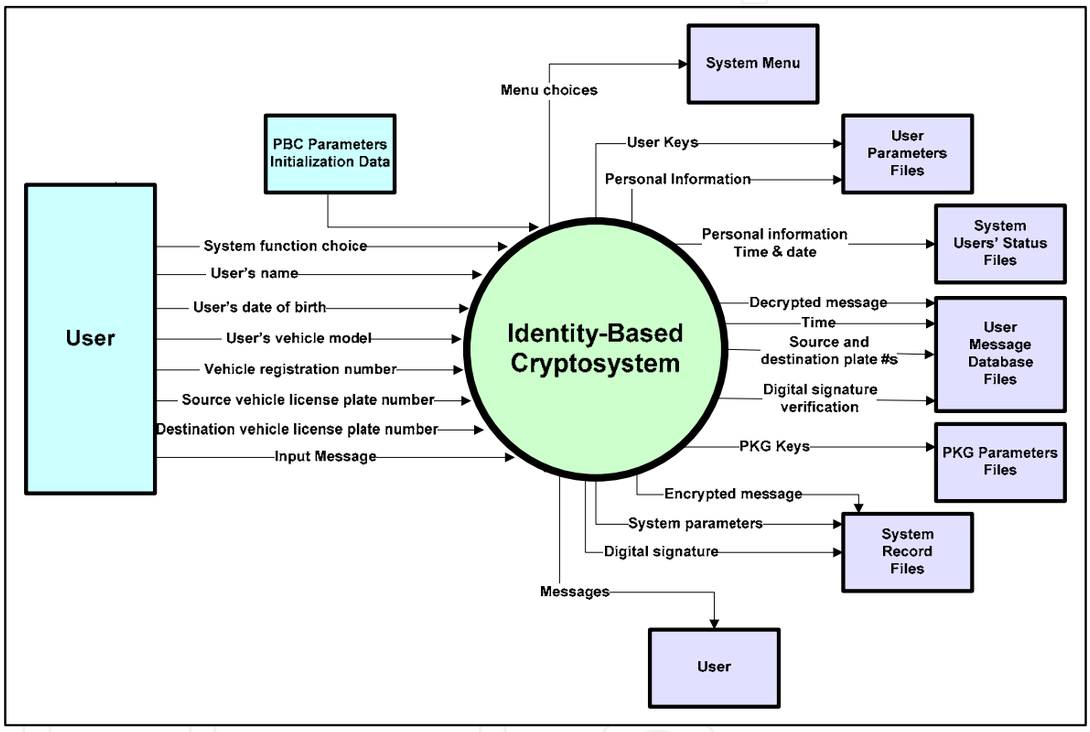


Fig. 10. The IDBCS data flow diagram

5.3 Behavioral Model

The behavior of the IDBCS is shown in Figure 11 which illustrates the State Transition Diagram of the IDBCS. As can be seen from the figure, the initialization occurs when the system is started and then it waits for choice input from the user. Depending on this choice, the system performs the corresponding function. There are 5 choices which the user could choose from:

- PKG Setup
- Registration
- Send Messages
- System Reset
- Exit.

At each choice, the corresponding function(s) is performed and then the user is directed back to the main screen for the next input (except when the choice is Exit).

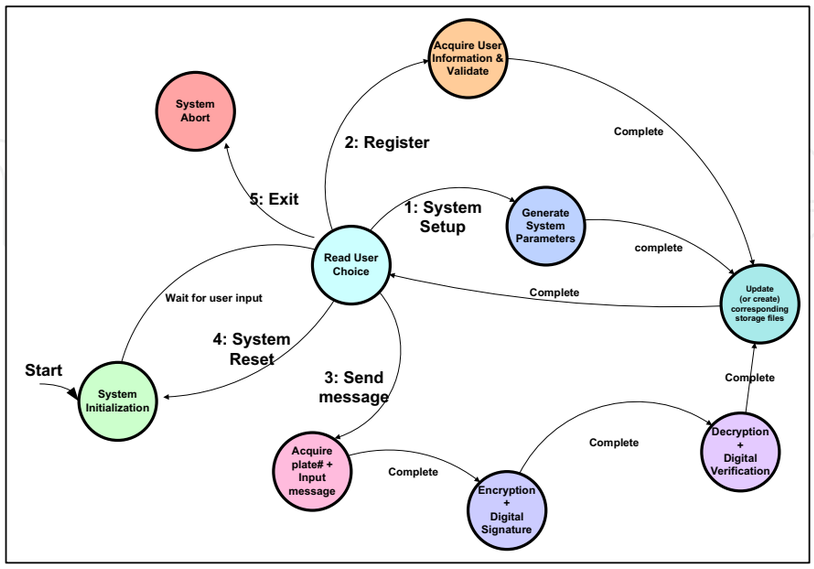


Fig. 11. The IDBCS state transition diagram

6. Complete IDBCS for VANETs

This section outlines the proposed IDBCS for VANETs as a complete system and describes its implementation. The first step in the IDBCS is the initialization of all elements and pairing functions. When that is done, the main screen is printed to the user with 5 possible functions to choose from: system setup, registration, send messages, system reset and exit. When the user chooses an option, the system calls the corresponding function, prints status messages to the user and then returns to the main screen for the next choice (except for exit).

If the user chooses system setup, the system checks if there are any PKG files existing, if there are PKG files then the system only reads the keys of the PKG so that they can be used in the system. Otherwise, the setup function is called: *setup()* and when that is done a flag is set up to indicate that setup was performed successfully. The system prints a message to the user to indicate whether setup is already performed or was performed successfully now.

If the user chooses registration; the system first checks if setup was performed or not by checking the flag value. If setup was not performed, then the system informs the user that registration cannot be done prior to system setup. If setup was performed, then the system asks the user to enter the car plate number and the check status function is called: *check_status(plate_num)* to check whether the user is registered or not. If the user is registered, the system informs the user that he/she is already registered and can send messages. Otherwise, the registration function is called: *registration()*, and then the extraction function is called: *extraction(plate_num, registration_num, user_file_name)*. After performing these two functions, the system informs the user that he was successfully registered to the system and can now send or receive messages.

If the user chooses message communication, the system asks the user to enter his/her plate number and the check status function is called: *check_status(plate_num)*to check whether the

user is registered or not. If the user is not registered, the system informs him/her that he/she cannot communication unless he is registered. If the user is registered; he/she is asked to enter the plate number of the destination and a similar process is repeated to check if the destination vehicle is registered or not. If both vehicles are registered, message communication function is called: *msg_comm(source_plate_num, destination_plate_num)*.
If the user chooses system reset, the system reset function is called: *system_reset()*. Finally, if the user chooses exit, then the system is aborted. The files created by the IDBCS can be viewed by using the command terminal: *gedit file_name*. Figure 12 shows the flowchart of the IDBCS.

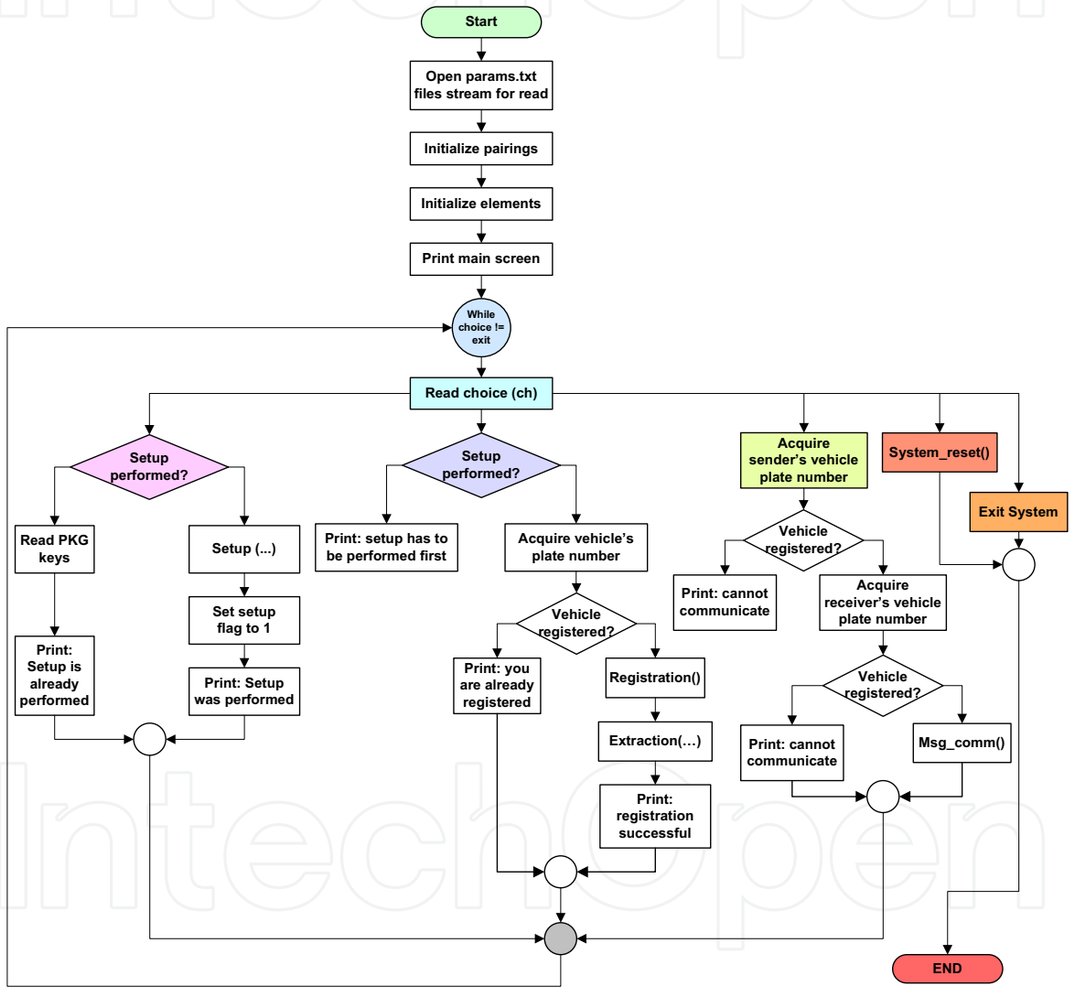


Fig. 12. Flowchart of the IDBCS for VANETs

7. Conclusion

This book chapter presented a study of VANETs. It highlighted their properties and security and privacy challenges such mobile ad hoc networks present. Furthermore, three main cryptography schemes were investigated: public key, symmetric key, and identity based

cryptography as they could be used for the security of the network. The advantages and disadvantages of these schemes were identified and overlapped with the properties of VANETs.

The study showed that identity based cryptography (IDBC) is considered the most viable choice to provide security for such networks. This is primarily due to the light-weight nature of IDBC techniques which align themselves well with the major properties of VANETs which include the infrastructure-less nature and the requirement for high speed real-time response.

In addition to the study of the various security schemes, the book chapter presented a novel implementation of an Identity Based Cryptosystem (IDBCS) that demonstrates how this scheme could be used for VANETs security. The system was designed and implemented and is based on Pairing Based Cryptography (PBC) and Elliptic Curve Cryptography (ECC). Several cryptographic primitives such as encryption and digital signature were implemented in order to provide the fundamental security services of confidentiality, integrity, authentication and non-repudiation.

Security analysis of the implemented IDBCS proved that the system is computationally secure since it implements algorithms which require a very large number of operations to break. The efficiency of the system was also measured and the results indicated that the IDBCS is computationally efficient as most of its functions do not require extensive processing or time.

8. References

Arfken, G. & Weber, H. (2005). Mathematical Methods For Physicists. *Academic Press*

Armitage, J. & Eberlein, W. (2006). Elliptic Functions. *Cambridge University Press*

Baek, J.; Newmarch, J., Safavi-Naini, R. & Susilo, W. (2004). A survey of identity-based Cryptography. *Proceedings of Australian Unix Users Group Annual Conference*.

Baek, J.; Steinfeld, R. & Zheng, Y. (2007). Formal proofs for the security of signcryption. *Journal of Cryptology*, Vol. 20, pp. 203–235

Boneh, D. & Franklin, M. (2001). Identity-based encryption from the Weil pairing, *Proceedings of Crypto 2001,* LNCS, Vol. 2139, pp. 213-229, Springer-Verlag

Boneh, D.; Lynn, B. & Shacham, H. (2001). Short signatures from the Weil pairings, *Proceedings of Advances in Cryptology*, LNCS, Vol. 2248, pp. 514-532, Springer-Verlag.

Boneh, D.; Gentry, C., Lynn, B. & Shacham, H. (2003). Aggregate and Verifiably Encrypted Signatures from Bilinear Maps. *Proceedings of Advances in Cryptology – EUROCRYPT 2003*, LNCS 2656, pp. 416-432

Boukerche, A; Oliveira, H., Nakamura, E. & Loureiro, A. (2008). Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems. Computer Communications, Elsevier, Vol. 31, No. 12, pp. 2838-2849

Burmester, M.; Magkos, E. & Chrissikopoulos, V. (2008). Strengthening privacy protection in VANETs, *Proceedings of IEEE Int. Conference on Wireless & Mobile Computing, Networking & Communication,* pp. 508-513.

Connelly, K.; Siek, K.A., Mulder, I., Neely, S., Stevenson, G. & Kray, C. (2008). Evaluating pervasive and ubiquitous systems. *IEEE Pervasive Computing*. Vol.3, No.7, pp.85-88

Conway, J. & Guy, R. (1995). The book of numbers. *Springer*

Daemen, J. & Rijmen, V. (2002). The design of Rijndael: AES - The advanced encryption standard. *Springer*

Diffie, W. & Hellman, M.E. (1976). New directions in cryptography, *IEEE Transactions on Information Theory*, IT-22, 6, pp.644-654

Dornbush, S. & Joshi, A. (2007). StreetSmart Traffic: Discovering and Disseminating Automobile Congestion Using VANETs. *Proceedings of IEEE Vehicular Technology Conference*, pp.11-15

Eichler, S. (2007). Performance Evaluation of the IEEE 802.11p WAVE Communication Standard. *Proceedings of IEEE Vehicular Technology Conference*, pp. 2199-2203.

Finch, S. (2003). Mathematical Constants. *Cambridge University Press*

Galbraith, S. & Paterson, K. (ed) (2008). Pairing-based cryptography - Pairing 2008. *Springer*

Golle, P.; Greene, D. & Staddon, J. (2004). Detecting and correcting malicious data in VANETs, *Proceedings of First ACM Workshop on Vehicular Ad-hoc Networks,* pp. 29-37

Hankerson, D.; Menezes, A.J. & Vanstone, S. (2004). Guide to elliptic curve cryptography. *Springer*

Hubaux, J.; Capkun, S. & Luo, J. (2004). The security and privacy of smart vehicles. IEEE *Security & Privacy, V*ol. 2, No.3, pp. 49-55

Kamat, P.; Baliga, A. & Trappe, W. (2006). An Identity-based security framework for VANETs, *Proceedings of 3rd Int. Workshop on Vehicular Ad-hoc Networks*, pp. 94-95.

Jakubiak, J. & Koucheryavy, Y. (2008). State of the Art and Research Challenges for VANETs. *Proceedings of IEEE Consumer Communications and Networking Conference – CCNC 2008,* pp. 912-916

Jiang, D.; Taliwal, V., Meier, A., Holfelder, W. & Herrtwich, R. (2006). Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Communications*, Vol. 13, pp.36-43

Kiess, W. & Mauve, M. (2007). A survey on real-world implementations of mobile ad-hoc networks. *Ad Hoc Networks*, Vol. 5, No. 3, pp. 423-339.

Li, W. & Joshi, A. (2009). Outlier detection in ad hoc networks using Dempster-Shafer theory. *Proceedings of Int. Conference on Mobile Data Management, Systems, Services and Middleware – MDM 2009.*

Lin, X.; Sun, X., Ho, P. H. & Shen, X. (2007). GSIS: A secure and privacy preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456

Lin, X.; Lu, R., Zhang, C., Zhu, H., Ho, P. & Shen, X. (2008). Security in vehicular ad hoc networks. *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 88-95

Joseph, G. (1998). Contemporary abstract algebra, 4th ed.. *Houghton Mifflin*, USA

Maiwald, E. (2003). Fundamentals of Network Security, *McGraw Hill*, USA

Menezes, J. A.; Van Oorschot, P. C. & Vanstone, S. A. (1997). *Handbook of Applied Cryptography*, CRC Press

Nadeem, T; Shankar, P. & Iftode, L. (2006). A Comparative Study of Data Dissemination Models for VANETs. *Proceedings of Annual International Conference on Mobile and Ubiquitous Systems (MOBIQUITOUS), San Jose, CA, USA*

Papadimitratos, P.; Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Zhendong Ma, Kargl, F., Kung, A., Hubaux, J. P. (2008). Secure vehicular communication systems: design and architecture. *IEEE Communication Magazine*, Vol. 46, No. 11, pp. 100-109

Parno, B. & Perrig, A. (2005). Challenges in securing vehicular networks, *Proceedings of the Workshop on Hot Topics in Networks (HotNets-IV)*

Rahman, S. & Hengartner, U. (2007). Secure crash reporting in vehicular Ad hoc networks. *Proceedings of Int. Conf. Security and Privacy in Communications Networks - SecureComm 2007*, pp. 443-452.

Raya, M. & Hubaux, J. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, Vol. 15, pp. 39–68

Raya, M; Papadimitratos, P. & Hubaux, J. (2006). Securing vehicular communication. *IEEE Wireless Communication,* Vol.13, No.5, pp. 8-15

Schoch, E.; Kargl, F., Leinmuller, T. & Weber, W. (2008). Communication Patterns in VANETs. *IEEE Communcations Magazine*, Vol.46, No.11, pp.119-125.

Shamir; (1984). Identity-based cryptosystems and signature schemes, *Proceedings of Advances in Cryptology - Crypto' 84,* LNCS, Vol. 196, Springer-Verlag, pp. 47-53.

Stallings, W. (2002). The advanced encryption standard. *Cryptologia*, Taylor & Francis, Vol. 26, No. 3, pp. 165-188.

Stinson, D. R. (2005). *Cryptography Theory and Practice, 3rd ed.,* Chapman & Hall/CRC, USA.

Sun, J.; Zhang, C. & Fang, Y. (2007). An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks, *Proceedings of the IEEE Military Communication Conference-MILCOM'2007*, pp.1-7.

Theng, Y. & Duh, H. (2008). *Ubiquitous Computing: Design, Implementation and Usability*, IGI Global

Wang, N.; Huang, Y. & Chen, W. (2008). A novel secure communication scheme in vehicular ad hoc networks. *Computer Communications,* Vol.31, No. 12, pp. 2827-2837

Want, R. & Pering, T. (2005). System challenges for ubiquitous & pervasive computing, *Proceedings of Int. Conference on Software Engineering – ICSE'05*, pp.9-14

Washington, L. C. (2008). *Elliptic Curves Number Theory and Cryptography, 2nd ed., Chapman & Hall /*CRC Press

Yan, G.; Olariu, S. & Weigle, M. (2008). Providing VANET security through active position detection. *Computer Communications*, Vol. 31, No. 12, pp. 2883-2897

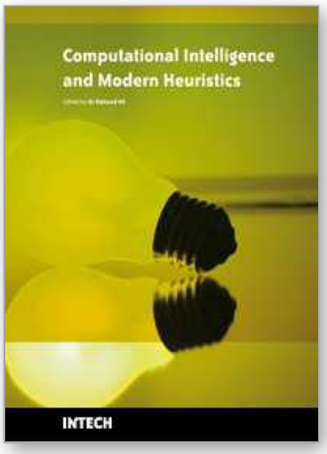
Yang, L. & Wang, F. Y. (2007). Driving into intelligent spaces with pervasive communications. *IEEE Intelligent Systems*, Vol. 22, No. 1, pp. 12-15.

Yeun, C. Y.; Lua, E. K. & Crowcroft, J. (2005). Security for emerging ubiquitous networks, *Proceedings of IEEE Vehicular Technology Conference,* Vol.2, pp. 1242-1248.

Yu, J.Y. & Chong, P.H.J. (2005). A survey of clustering schemes for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, Vol. 7, No.1, pp.32-48

Zhao, J. & Cao , G. (2008). VADD: Vehicle-assisted data delivery in vehicular ad hoc networks. *IEEE Transcations Vehicular Technology*, Vol.57, No.3, pp. 1910-1922.

IntechOpen



Computational Intelligence and Modern Heuristics

Edited by Al-Dahoud Ali

ISBN 978-953-7619-28-2

Hard cover, 348 pages

Publisher InTech

Published online 01, February, 2010

Published in print edition February, 2010

The chapters of this book are collected mainly from the best selected papers that have been published in the 4th International conference on Information Technology ICIT 2009, that has been held in Al-Zaytoonah University, Jordan in the period 3-5/6/2009. The other chapters have been collected as related works to the topics of the book.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi (2010). Security and Privacy of Intelligent VANETs, Computational Intelligence and Modern Heuristics, Al-Dahoud Ali (Ed.), ISBN: 978-953-7619-28-2, InTech, Available from: http://www.intechopen.com/books/computational-intelligence-and-modern-heuristics/security-and-privacy-of-intelligent-vanets

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen