

# EFFICIENT SECURITY IMPLEMENTATION FOR EMERGING VANETS

**Chan Yeob Yeun, Mahmoud Al-Qutayri, Faisal Al-Hawi**  
Khalifa University of Science Technolgy and Research, UAE  
{cyeun, mqutayri, f.alhawi}@kustar.ac.ae

## ABSTRACT

Vehicle ad-hoc networks (VANETs) are a prominent form of mobile ad-hoc networks. This paper outlines the architecture of VANETs and discusses the security and privacy challenges that need to be overcome to make such networks practically viable. It compares the various security schemes that were suggested for VANETs. It then proposes an efficient implementation of an identity based cryptosystem that is robust and computationally secure.

**Keywords:** VANETs, Security, Privacy, Identity Based Cryptosystem

## 1 INTRODUCTION

Pervasive Networks (PN) are those networks that provide a diversity of services from single access points. One example of such networks is the Mobile Ad-hoc Network (MANET) where nodes are highly mobile hence constantly reforming the topology of the network. An application of these networks is the emerging VANET.

VANETs are wireless ad-hoc networks where the nodes, either vehicles or road side units (RSUs), can communicate and exchange data for purposes of information inquiry or distribution. This can be achieved by allowing nodes to connect within certain ranges (typically 5-10 Km) in order to exchange information about traffic conditions [1]. Figure 1 illustrates a general view of VANETs structure.

VANETs can greatly help in providing safety services and improving the driving experience. For example, the provision of road conditions such as environmental hazards information, traffic conditions and congestions' locations, accident reporting which help the authorities to maintain road status.

Moreover, entertainment options can be provided for customers. An example of such an option is the TracNet system which was introduced by Microsoft and KHV [2] to provide internet access in vehicles. The diversity of applications is driven by the fact that VANETs are ultimately considered a form of ubiquitous networks which intend to provide many services with a single access point.

To date, communication technologies in VANETs are based on existing protocols. An example of such protocols is the IEEE 802.11 (i.e. Wi-Fi) standards [3] with its different enhancements (802.11b/g). Some application of VANETs such as toll payments system used in several countries also rely on Radio Frequency Identification (RFID) which is a type of Dedicated Short Range

Communication (DSRC) standard suit [3]. However, these methods introduce some latency problems which are intolerable in such networks. Therefore, an IEEE project to provide a new enhancement to the 802.11 standard that will improve communication for such network is in progress. The new standard, known as IEEE 802.11p [3], will be based on DSRC but with an addition of Wireless Access for Vehicular Environments (WAVE). This will support both Vehicle-to-Vehicle (V2V) and Vehicle-to-RSU (V2R) communication in VANETs [4], [5].

In order for VANETs to be used in the future they must provide adequate levels of security and privacy to the users. These aspects of the system are of paramount importance as they affect people safety and may compromise their personnel privacy if not properly addressed.

The paper is organized as follows: section two discusses the challenges that are facing VANETs. Section three explores previous related works on VANET security. Section four, provides an example of how Identity-Based Cryptography (IDBC) can be used in VANETs. Then, we present our proposed implementation of IDBC in VANETs. This is followed with analysis about the work achieved in the implementation of IDBC for VANETs.

## 2 VANETS CHALLENGES

The ultimate goal of VANETs is to enhance the driving experience by providing different measures of safety while driving. However, in order to achieve this goal; some challenges must be considered. In this paper, we categorize challenge aspects into two major groups that must be considered: security and privacy. Although privacy aspects will be reviewed and discussed, the paper will focus more on the security aspects that are taken into account in order for users to trust using such networks.

## 2.1 Security Challenges

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.

For example, vehicles cannot access events recorders or other vehicles. Also, integrity of exchanged messages must be provided in order to detect malicious intent such as information alteration and prevent vehicles from spreading false traffic conditions. Additionally, vehicle authentication is important to ensure that all nodes within the network are who they claim to be. Hence preventing impersonation attacks where a vehicle pretends to be an authority or another vehicle.

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) [1, 6]. Some recent works have 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 of confidentiality, integrity and authentication in vehicular networks.

Another salient challenge that faces the security of VANETs is the process of 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.

An important category is the process of key revocation which is the process of discarding suspected key or keys that are bound to malicious nodes. Traditional methods such as Certificate Revocation Lists (CRLs) are not suitable for VANETs because of large scale of the network (i.e. millions of vehicles) [7] which make these lists huge and increase the overhead of the revocation process.

A second category is the process of group key management since VANETs inherit the characteristic of mobility from Mobile Ad-hoc Networks (MANETs). What makes this issue a problem is the fact that vehicles rarely form groups in VANETs since two vehicles may only be in close range for short amounts of time. Therefore, the security framework must resolve this issue to prevent malicious vehicles from compromising the security of the network.

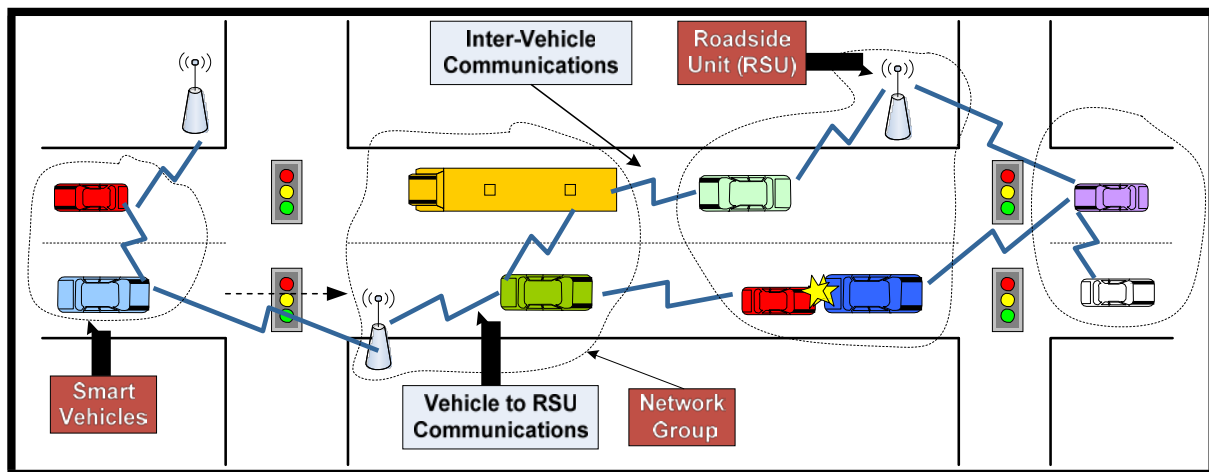


Figure 1: The basic structure of VANETs

## 2.2 Privacy Challenges

The privacy issue is concerned with protecting personal information of drivers; such as name, location and plate number, within the network. This may seem easy at first, however the network protocol has to be designed in such 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 [7] and that could be 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 in [7, 8].

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) [7]. 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.

### 3 RELEATED WORKS

This section examines major previous works that is related to the field of vehicular communication and VANET security. It highlights the researches carried out to resolve the security challenges facing VANETs. Each subsection focuses on some security aspects and the proposed schemes to resolve them.

#### 3.1 Public-Key Approaches for Security and Privacy

Hubaux *et al.* [8] have drawn the attention to security and privacy issues in vehicular communication which they believe was overlooked by the research community. 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 (PKC) 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. 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.

In [1], a 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 does 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.

#### 3.2 Certificate Revocation

Raya *et al.* [1] proposed a security architecture for vehicular communication that aims to provide security services for such networks. 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.

In [7], a novel method for certificate revocation in VANETs is proposed; termed RSU-aided Certificate Revocation (RCR). In this method, the Third Trusted Party (TTP) (i.e. CA) 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 how silent attacks (i.e. where a node disables message broadcasting feature in order to be camouflaged from the RSU) can be prevented using the RCR.

#### 3.3 Privacy Preservation in VANETs

In [1], 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.

The article in [7] addresses the 'conditional' privacy preservation in VANETs. 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, CRLs become very difficult to manage.

#### 3.4 Identity Based Approaches for VANETs

In [9], an ID-based framework that could achieve privacy and non-repudiation is introduced. The work in [9] also explained 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. They suggest the use of

‘distributed control’ where a single authority is unable to reveal drivers’ personal information. Instead, they proposed having multiple authorities to 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 [1] 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. They 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 acquire the use of public or symmetric key cryptography for further communication once mutual authentication has been established between nodes in VANETs. They proposed a method based on ID-based threshold signatures to provide non-repudiation services for authorities in VANETs [9].

Another contribution in the field of IDBC in VANET security is proposed in [10] by P. Kamat *et*

*al.* They point out that VANETs nodes (i.e. vehicles and RSU) should be able to mutually authenticate with other nodes; but protect the identity of themselves in order to grant privacy services. It is explained why traditional cryptography techniques cannot be used in VANETs environments and why IDBC is possibly the ‘best’ solution to resolve VANET security issues.

#### 4 AN IMPLEMENTATION OF IDBC FOR VANETS

This paper proposes the use of identity-based cryptosystem (IDBC) for VANETs as it has a number of distinguished features. Firstly, the TTP has to perform a single task of generating the private key for users after an authentication process is performed. Hence, it does not keep any records binding keys to users and once the keys are distributed which reduces the overhead on the TTP.

This is also coincides with the infrastructure-less nature of VANETs since there is no need for Certificate Authorities (CA) or Key Distribution Centers (KDC). Secondly, all security activities (i.e. encryption, decryption, signing and verifying) are performed by nodes without intervention of the TTP which reduces the communication delays and overhead. This will ensure real-time responses for VANET communication as it is a major requirement in such networks.

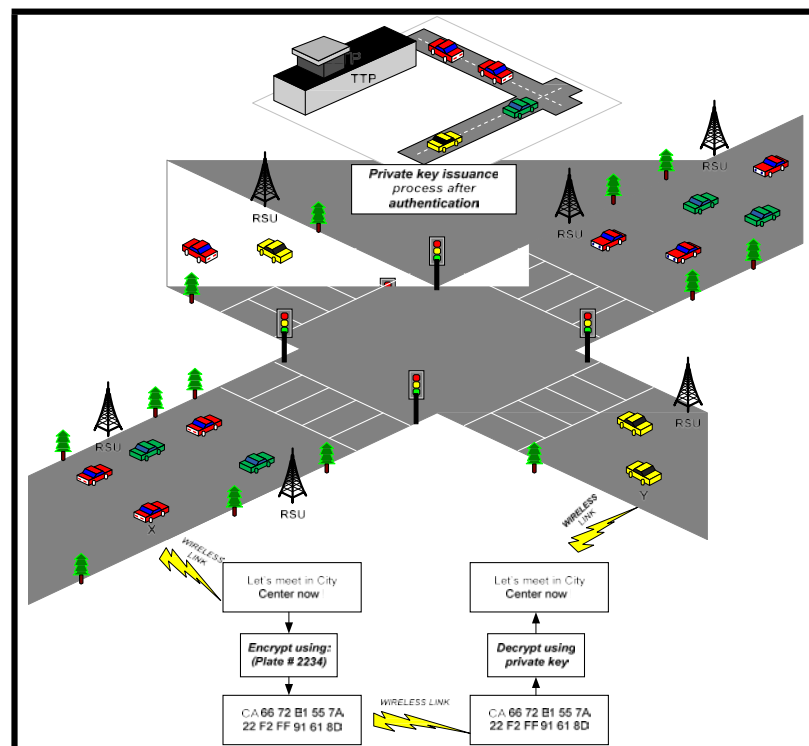


Figure 2: How IDBC can deploy in VANETs

personal information about a particular vehicle will not be exposed unless absolutely required by authorities (e.g. in case of accident investigation); which ensure that conditional privacy is provided. Figure 2 illustrates deploying Identity-Based Encryption (IDBE) in a VANET. The public key of a node can be a combination of its plate number and license registration number (e.g.,  $X^{public} = plate\ number \parallel license\ registration\ number$ ). The TTP can be any governmental organization (e.g. the Road & Transportation Authority; RTA), and it should handle the process of issuing private keys for nodes (i.e. vehicles) after they have been authenticated. The process of authentication of vehicles can be similar to the methods used by authorities today; i.e. presenting identification documents to prove that you are the owner of the vehicle. The underlying security framework uses IDBC as a security measure.

the figure, the sender X uses the public key of the recipient Y to encrypt the message and send it via the communication protocols in use. Upon receiving the encrypted message, the recipient uses its private key (which was previously extracted from the TTP) to decrypt the message and obtain the original plaintext.

Figure 3 describes the process of the proposed IDBC. There are 4 stages for the system: The *setup* stage where all system parameters are initialized and then the public/private key pair of the TTP is computed. Next is the *extract* stage where the user's private key is computed. Then, at the *encryption* stage the encryption key is used to encrypt the plaintext message using the Blowfish scheme that uses maximum key size of 448-bits [11]. Moreover, in the *decryption* stage, the cipher is decrypted using the Blowfish decryption scheme.

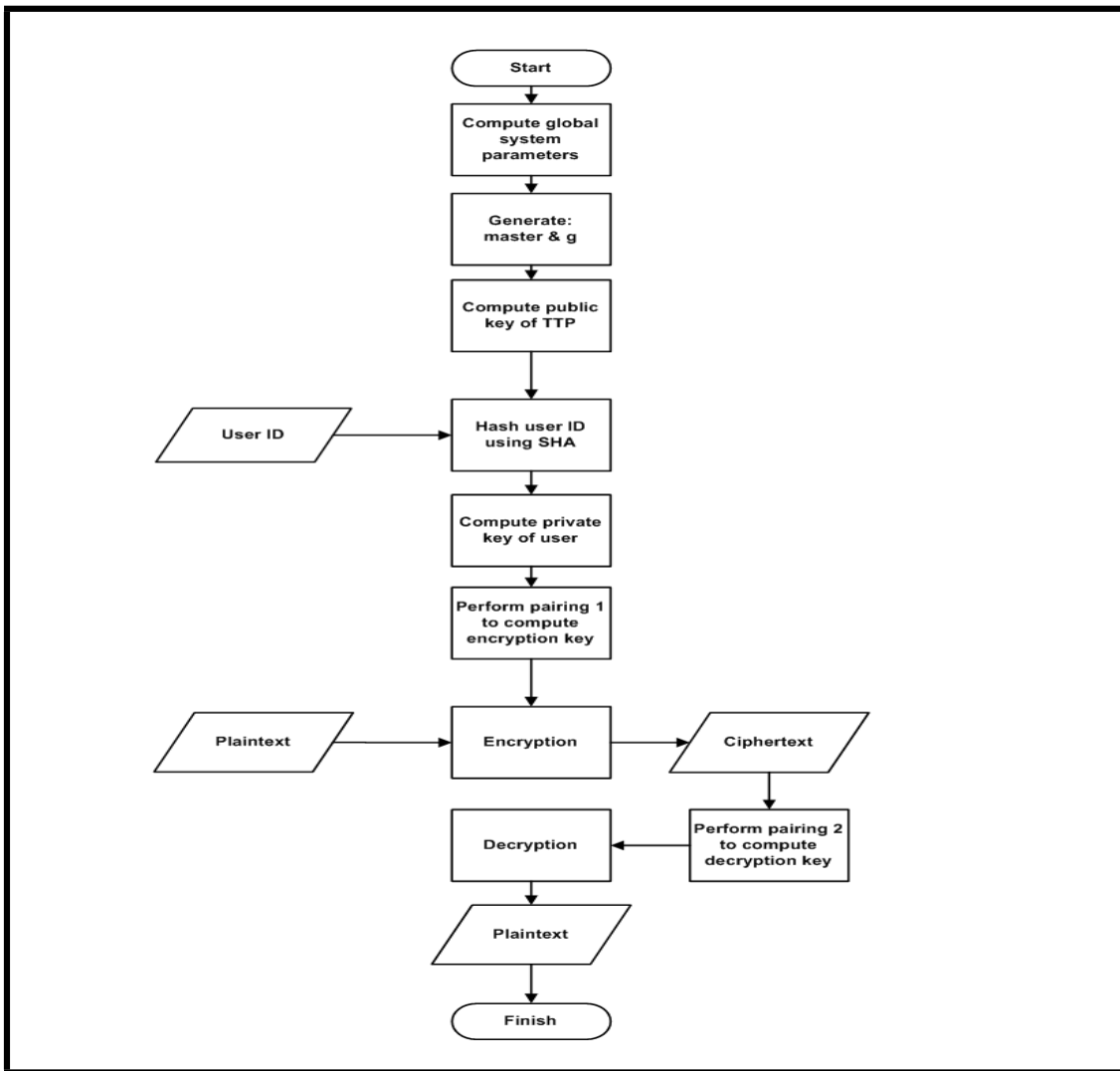


Figure 3: The functionality of IDBC system

The implementations of IDBC modules are briefly explained as follows:

- *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 [12, 13].
- *PKG Setup*: this function generates all the key elements associated with the Third Trusted Party 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. Note that these keys are 160 bits that is equivalent to RSA 1024 bits.
- *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.
- *Driver/Vehicle Registration & Authentication*: in order for users to communicate messages with other users using the system; one should first go through a registration process. This function is responsible for acquiring driver information, validating input data and creating specific files that will hold all his/her personal, vehicle and system information such as name, date of birth, vehicle model, registration number and license plate number.
- *Message Communication*: this function performs the core functionalities of the message communication between two drivers. The system checks if both vehicles are registered in the system or not. If both are registered, the message communication function is called. This function takes as input the sender's vehicle plate number and the destination's vehicle plate number.
  1. 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

updates the files that are created for each user by these messages sent/received. Firstly, this function opens corresponding files to read the receiver's private and public keys for encryption and decryption respectively. Then, it generates a random element  $r$ , computes a timestamp, and then computes the first half of the encryption data which is an extra value  $E = g^r$  which is required for the decryption process.

2. Next, it applies a pairing function between the PKG public key and the user's public key and stores it in  $C = e(PKG^{public}, User^{public})$ .  $C$  is converted to bytes which then represent the encryption key. After that, the user is asked to enter the message he/she wishes to send and that message is hashed using SHA-1 [14] that produces digest of 160 bits in 80 rounds (for the digital signature process) and mapped to an element. Then the Blowfish encryption occurs with the encryption point and the plaintext message (discussed in the next section).
3. For the decryption process to occur successfully, the function applies a pairing function between the extra value and the receiver's private key and stores it in  $P = e(E, User^{private})$ .  $P$  is also converted to bytes which then represent the decryption key. A checking process is also performed to make sure that the encryption and decryption keys are identical. Then the Blowfish decryption occurs with the decryption key and the cipher which is produced from the encryption process.
4. Next, the function opens corresponding files to read the sender's private signature key and the receiver's public verifying key for the digital signature process. After that the BLS signature/verification process occurs. During the processes of the message communication function the medium and map files are updated as well as sender's and receiver's files with.

In brief, the message communication 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. Figure 4 shows the flowchart of the message communication function.

- *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

- to the communication process.
- *System Reset*: this function flushes all PBC and system elements previously generated and

function will disable all functionalities of the system unless setup is performed again.

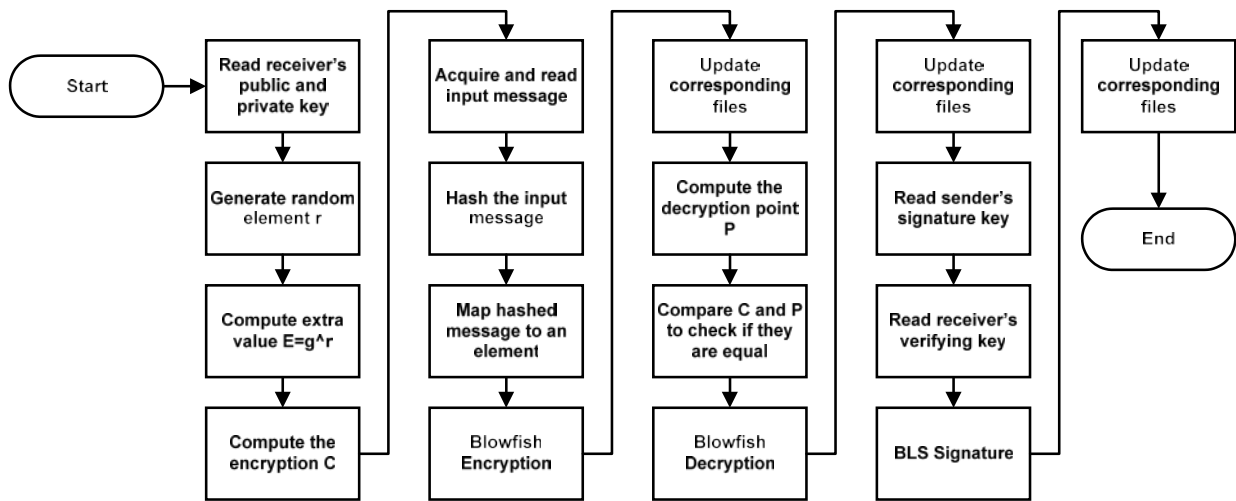


Figure 4: Message Communication Function Flowchart

## 5 ANALYSIS

The most critical part of testing is analysis, where our implementation of IDBC in VANETs is compared to other system according to certain criteria. Analysis is done in three stages in the following subsections: the security analysis of the system and comparison to other system, and the system performance.

### 5.1 Security Analysis

There are many methods of evaluating the security of a cryptosystems. One of these methods is referred to as computation security which signifies that a given cryptosystem requires a very large number of operations to be broken. In other words, the underlying problem of the cryptosystem is intractable and computationally infeasible. The IDBCS implements several cryptography primitives each having a source of security behind it.

The security of the Boneh-Franklin scheme [13] is based on the infeasibility of the Computational Diffie-Hellman Problem (CDHP) [15]. Furthermore, since the system is based on the Pairing Based Cryptography, other variants of the Diffie-Hellman problems are also considered a source of strength in the system. Moreover, the IDBC is also based on Elliptic Curves which means that another source of its strength is the intractability of the Scalar Multiplication Problem of Elliptic Curves, i.e. Elliptic Curve Diffie-Hellman Problem (ECDHP) [12].

Thus, as long as the variant of Diffie-Hellman problems and the ECDH are intractable, the IDBC is

considered computationally secure. Furthermore, a cryptosystem should provide security services that facilitate secure communication. Consequently, our implementation of IDBC provides four of these services:

- *Confidentiality*: is provided through the use of encryption schemes which effectively hide the information from all but those people authorized to reveal it. The IDBC implements Boneh-Franklin Identity Based Encryption framework using the Blowfish encryption scheme, hence confidentiality is guaranteed.
- *Integrity*: is to ensure that the information being communicated has not been altered in the communication channel. For cryptosystem to provide this feature, Modification Detection Codes (MDCs) should be used. Hashing functions is a type of MDC which ensures that even a slight modification in the message will significantly alter the digest. The IDBCS uses SHA-1 as its hashing function, hence it provides data integrity.
- *Non-repudiation*: is a security services which keeps track of operation in the system so that no entity can claim false actions or deny true ones. This feature is provided by the use of digital signatures. The IDBCS implement the BLS signature scheme [16] which ensures that no node can deny a message it sent or claim to be the source of a message.
- *Authentication*: is provided by the IDBCS as all users who wish to communicate using the system are required to go through a registration

process which validates their identities before issuing them system parameters. Note that in actual VANET system, the authentication process might be similar to a passport checking process at airport where an agent validates identities.

## 5.2 Comparisons to Other Systems

IDBC is proving to be the most suitable scheme for VANET security. The reason is because the scheme matches the security requirements in such networks; which depend on the properties of VANETs. Firstly, if we compare IDBC to Public Key Cryptography [17]; we can note that the TTP in an IDBC has to perform a single task of generating the private key for users after an authentication process is performed. Hence, it does not keep any records binding keys to users and once the keys are distributed which reduces the overhead on the TTP.

Unlike the TTP in Public Key systems which requires the existence of a Public Key Infrastructure (PKI) [18] to manage all key operation and this introduces significant processing burden on the TTP. The elimination of the PKI in IDBC also coincides with the infrastructure-less nature of VANETs since there is no need for Certificate Authorities or Key Distribution Center (KDC).

Furthermore, all security activities (encryption, decryption, signing and verifying) are performed by nodes without intervention of the TTP unlike the case in Public Key systems where a digital signature requires a node to acquire a certificate from the TTP. Therefore, using an Identity Based system will reduce the communication delays and ensure real-time responses for VANET communication as it is a major requirement in such networks.

Also, since the public key in such networks could be a unique arbitrary string such as the license plate number; there is bound to be less processing delays compared to Symmetric Key systems. If a Symmetric Key system is deployed in a VANET, it would mean that nodes should agree on a shared key each time a communication channel is established which requires extensive processing requirements given the fact that VANETs are very dense (i.e. huge number of nodes in the networks).

The matter worsens if we look at the dynamic and mobility feature of VANETs. Since groups might be formed constantly, it might not be suitable to use a Symmetric Key system since each time a node joins/leaves a group, another shared key is required to be generated and agreed between the nodes.

Moreover, assuming that the TTP is fully-trusted, personal information about a particular vehicle will not be exposed unless absolutely required by authorities (e.g. in case of accident investigation);

which ensure that conditional privacy is provided. However, unconditional trust is rarely provided and it could be a disadvantage in such networks.

The strongest argument against Identity Based systems is the immaturity of the field compared to the very mature areas of public and symmetric key systems. However, IDBC is becoming a mainstream for security systems especially for infrastructureless networks with dynamic features such as those of VANETs.

## 5.3 Performance Testing

The metric used to measure the performance of the IDBC is time-oriented. The time required to complete the major functions (setup, extraction, encryption and decryption) of the system were measured for 10 trials. This was done by measuring the time at the beginning and the end of the function using time variables from the PBC library. Then, the average time required was calculated for each of these functions.

Note that the time required to perform some functions such as registration and message communication depend on the user and hence they were excluded from this performance metric to avoid inaccurate data. The results for the time metric of the IDBCS functions are shown below:

- *Setup Stage:* Table 1 shows the time required to perform this function for 10 trials. As can be seen, the time required for the setup stage is quite small and the margin between trials is not significant. The average time required for the setup process is = 0.064285 seconds.
- *Extraction Stage:* Table 2 shows the time required to perform this function for 10 trials for hashing user public key and generating signature. Similarly, the time required for the extraction stage is small and the margin between trials is not significant. The average time required for the setup process is = 0.067783 seconds.
- *Encryption Stage:* Table 3 shows the time required to perform this function for 10 trials. We can see that the time required for the encryption segment of the message communication stage is small and the margin between trials is not significant. The average time required for the setup process is = 0.029125 seconds.
- *Decryption Stage:* Table 4 shows the time required to perform this function for 10 trials. Similarly, the time required for the decryption segment of the message communication function stage is even smaller and the margin between trials is not significant. The average time required for the setup process is = 0.013826 seconds.

## 6 CONCLUSION

This paper surveyed VANETs and their applications and highlighted the major challenges facing such networks. It also reviewed previous schemes proposed in order to provide security and privacy for VANETs. It subsequently introduced our practical implementation of IDBC in VANETs. This paper showed that Identity Based Cryptography is considered the most viable choice to provide security for such networks. This is primarily due to the lightweight 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.

Our practical implementation was concerned with developing a novel implementation of IDBC that demonstrates how this scheme could be used for VANETs security. The system was designed and implemented in C language and it is based on Pairing Based Cryptography and Elliptic Curve Cryptography. 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 IDBC proved that the system is computationally secure since it implements algorithms which require a very large number of operations to break.

In conclusion, 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.

## 7 ACKNOWLEDGEMENT

The brief sketch of the paper was presented in the 4<sup>th</sup> International Conference on Information Technology (ICIT'09), 3-5 June 2009. The full implementation, security analysis, comparisons to other systems and performance testing are added in this paper.

## 8 REFERENCES

- [1] M. Raya, P. Papadimitratos and J. Hubaux: Securing vehicular communication, IEEE Wireless Communication, Vol. 13, pp. 8-15, October (2006).
- [2] TracNet System: <http://www.kvh.com/> as of March 9<sup>th</sup> (2009).
- [3] Standard Documentation of Dedicated Short Range Communication (DSRC): [http://www.standards.its.dot.gov/Documents/advisories/dsrc\\_advisory.htm](http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm), as of March 9<sup>th</sup> (2009).
- [4] K. Bilstrup: A Survey regarding wireless communication standards intended for high-speed vehicle environment, School of Information Science, Computer and Electrical Engineering, Halmstad, Sweden, SE-30118, <https://dSPACE.HH.se/dSPACE/handle/2082/2391> as of 28th March (2009).
- [5] IEEE Projects Time-line: [http://grouper.ieee.org/groups/802/11/Reports/802.11\\_Timelines.htm](http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm), last modified: September (2008).
- [6] E. Maiwald: Fundamentals of Network Security, Illinois: McGraw Hill (2004).
- [7] P. Golle, D. Greene and J. Staddon: Detecting and correcting malicious data in VANETs, in Proceedings of First ACM Workshop on Vehicular Ad-hoc Networks, pp. 29-37 (2004).
- [8] J. Haubaux, S. Capkun and J. Luo: The security and privacy of smart vehicles, IEEE Security & Privacy, Vol. 2, pp. 49-55, May-June (2004).
- [9] J. Sun, C. Zhang and Y. Fang: An identity-based framework achieving privacy and non-repudiation in vehicular ad hoc network, Military Communication Conference, Florida, USA (2007).
- [10] P. Kamat, A. Baliga and W. Trappe: An Identity-based security framework for VANETs, in Proceedings of 3<sup>rd</sup> international workshop on Vehicular ad hoc networks, pp. 94-95 (2006).
- [11] B. Schneier: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), in Proceedings of Fast Software Encryption, Springer-Verlag, pp. 191-204 (1994).
- [12] L.C. Washington: Elliptic Curves Number Theory and Cryptography, 1<sup>st</sup> edition, CRC Press (2007).
- [13] D. Boneh and M. Franklin: Identity-based encryption from the Weil pairing, in Proceedings of Crypto 2001, Vol. 2139 of LNCS, pp.213-229, Springer-Verlag (2001).
- [14] Federal Information Processing Standards Publication 180-1: Secure Hash Standard, Arpl 17 (1995).
- [15] F. Bae, R. Deng and H. Zhu: Variations of Diffie-Hellman Problem, in Proceedings of ICIC 2003, LNCS 2836, pp. 301-312 (2003).
- [16] D. Boneh, B. Lynn and H. Shacham: Short signatures from the Weil pairings, Journal of Cryptology, Vol. 17, No. 4, pp. 297-319 (2004).
- [17] R.L. Rivest, A. Shamir and L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communication of the ACM, Vol. 21, pp. 120-126 (1978).
- [18] X. 509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certification frameworks, ITU-T, August (2005).

**Table 1:** Setup Function Trials' Times

Trial	1	2	3	4	5	6	7	8	9	10
Time (s)	0.042247	0.064371	0.074538	0.068026	0.066744	0.064829	0.065089	0.064299	0.064071	0.068638

**Table 2:** Extraction Function Trials' Times

Trial	1	2	3	4	5	6	7	8	9	10
Time (s)	0.082902	0.066	0.059721	0.081693	0.052748	0.081411	0.082691	0.051732	0.060304	0.058632

**Table 3:** Encryption Segment Trials' Times

Trial	1	2	3	4	5	6	7	8	9	10
Time (s)	0.035525	0.028737	0.02039	0.035553	0.033755	0.02088	0.013377	0.036296	0.030004	0.036737

**Table 4:** Decryption Segment Trials' Times

Trial	1	2	3	4	5	6	7	8	9	10
Time (s)	0.010079	0.011627	0.010586	0.009969	0.009965	0.010585	0.010533	0.02732	0.010316	0.027281