Secured Key Management in Vehicular Ad Hoc Networks
Santosh R Chikkerur1, Ms.Rinki Sharma2, Dr.Ganeshmurthy3
1-Student, M.Sc. (Enng.) MSRSAS, 2-Sr.Lecturer, Communication Engineering Centre, M. S. Ramiah School of Advanced Studies, Bangalore. 3-Industrial Guido-DaimlerChrysler

Abstract
Secure and efficient key management in mobile ad hoc network has been a challenging task for the researchers due to properties of ad hoc network like dynamic topologies, use of wireless media, no fixed infrastructure and low-energy constraint devices. This document describes the research effort carried out securing message communication in Vehicular AdHoc networks (VANETS). VANETs are characterized by nodes with relatively high mobility and various disturbed environments represent a number of remarkable challenges dissimilar to MANETs. Applications of inter-vehicle and vehicle-to-roadside wireless communication that make use of VANETs require reliable communication that provides a guarantee of real-time message transmission.

One of the major challenges is that adhoc networks typically lack a fixed infrastructure both in form of physical infrastructure such as routers, servers and stable communication links and in the form of an organizational or administrative infrastructure. Another difficulty lies in the highly dynamic nature of adhoc networks since new vehicles can join and leave the network at any time. The major problem in providing security services in such infrastructure less networks is how to manage the cryptographic keys that are needed.

In this paper, comparison of relevant technologies in the fields of MANETs is discussed. After the thorough understanding of different methods Identity based Encryption (IBE) proved to be one of the solutions for the intended application for message communication between Vehicles on Highways. IBE can be implemented using Elliptic Curve Cryptography (ECC) as the base arithmetic. ECC allows for faster computations and smaller key sizes for comparable security. A 224-bit ECC signature is equivalent to a 2048-bit RSA signature. The generation of keys and the IBE method with the use of Pairings based cryptography are covered in detail.

Key Words: MANETs, VANETs, ECC, IBE, Weil Pairing

Nomenclature
\( K \) finite field
\( \text{char}(K) \) characteristic of finite field \( K \)
\( GP(p) \) finite field of size \( p \), \( p \) is a prime
\( GP(2n) \) finite field of size \( 2n \)
\( E \) group of points on elliptic curve
\( P, Q \) point on elliptic curve
\( xP, yP \) coordinate of point \( P=(xP, yP) \)
\( O \) point at infinite in elliptic curve group
\( f, g, h \) rational function over elliptic curve
\( \text{div}(f) \) divisor of rational function \( f \)
\( e(P, Q) \) Weil pairing of points \( P \) and \( Q \)
\( E[m] \) group of \( m \)-torsion points on elliptic curve

1. INTRODUCTION

Since the introduction of the safety belt in the 70's, passive safety systems like the airbag have helped to decrease the number of injured or killed passengers, whilst the number of accidents case of Passenger cars have not reduced to negligible figures.

Fig. 1 Cause of Accidents on Germany roads 2006

Consequently, passive safety systems have improved the safety of the passengers during and after an accident, but they have not been effective in reducing these accidents. Today's vehicles already use information about the close environment, collected by the vehicle's onboard sensors. Nevertheless, this information is

Often not enough to warn the driver before an accident. Exchanging information through intervehicle communication (IVC) can help to evaluate the road situation far ahead, and therefore, detect dangerous situations in an adequate amount of time. AdHoc inter-vehicle networks will soon be a reality as cars

Fig. 2 Car-to-Car Communication [2]

become equipped with wireless communication system. One use of an inter-vehicle network is to transmit alerts such as accidents, road conditions, and an ambulance on the way or a pursuit by police vehicles within a region [1-2].

Inter-vehicle communication is a fast growing research topic in the academic sector and industry. In recent years, car manufacturers like BMW, DaimlerChrysler, and Toyota have included global positioning system (GPS), map service, and IEEE 802.11 wireless communication system in their upcoming commercial vehicle designs. Thus the future of an ad-hoc inter-vehicle network will soon be upon manufacturers. From consumers' perspective, these new high-tech additions will be needed in the cars to improve the driving safety and experience. Through this kind of communication, vehicles are able to communicate with each other by using wireless technology like WLAN. As a result, they can be organized in vehicular AdHoc networks (VANETS)

Among the safety applications, Local Danger Warning (LDW) is likely to be one of the most important IV applications in the near future, due to its potential in accident avoidance. Vehicles share information about the current road condition and dangerous situations and are therefore able to warn their drivers of upcoming dangers

Vehicles exchange messages that are processed and interpreted. The messages contain sensor data or information about a special situation (e.g. the presence of a danger at a certain road location). With this information, the vehicles can detect local dangers and inform the driver ahead of time. For the communication and distribution of information by this LDW application, no infrastructure is necessary. Therefore, this system has many advantages compared to an infrastructure-
based approach. [3]
1.1 Security for VANETs
Some specific attacks can be listed in VANETs which warrant for security:
1. Bogus information: Attackers can be Insiders, Rational or Active and diffuse wrong information in the network to affect the behavior of other drivers (e.g., to divert traffic from a given road and thus free it for themselves).
2. Cheating with positioning information: Attackers in this case are also Insiders, Rational or Active, and use this attack to alter their perceived position, speed, direction, etc. In order to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other.
3. ID disclosure of other vehicles in order to track their location. This is the Big Brother scenario, where a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes (e.g., the way some car rental companies track their own Cars) [5-10].
4. Denial of Service: The attacker is Malicious, Active and may want to bring down the VANET or even cause an accident. Example attacks include channel jamming and aggressive injection of dummy messages [11].
5. Masquerade: The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. These are some of the attacks which the VANET security needs to withstand. [12]

2. RELATED WORK
This section outlines the background knowledge on Security in adhoc networking, cryptographic background and the various methods available for key management in mobile adhoc networks. In the end, we pay a close attention to Identity Based Encryption, Pairings and Elliptic Curve Cryptography.

2.1 Basics of Network Security
When discussing network security, three aspects can be covered; the services required, the potential attacks and the security mechanisms. The security services aspect includes the functionality that is required to provide a secure networking environment while the security attacks cover the methods that could be employed to break these security services. Finally, the security mechanisms are the basic building blocks used to provide the security services.

2.2 Security Services to be delivered
In providing a secure networking environment some or all of the following services may be required:
- Confidentiality: Ensures that transmitted information can only be accessed by the intended receivers.
- Authentication: Allows the communicating parties to be assured of the others identity.
- Integrity: Ensures that the data has not been altered during transmission.
- Non-repudiation: Ensures that parties can prove the transmission or reception of information by another party, i.e. a party cannot falsely deny having received or sent certain data.
- Availability: Ensures that the intended network services are available to the intended parties when required. [18]

2.3 Schemes in MANETs
This section briefly about the different techniques available for Key management in MANETs.
Zhou and Haas [1] discuss on Securing Ad Hoc Networks with an overview of the threats an ad hoc network faces and the security goals to be achieved. The paper also highlights Threshold cryptography, to build a highly secure and largely available key management service.
Magda et al. [2] reported the Security issues in a Future Vehicular Network based on infrastructure for vehicular communication on highways. The paper also provides view about several unique security issues and challenges in VANETs.

Chung and Simon[3] present a Secure Group Communications Using Key Graphs where group/multicast key management is used. The average measured processing time per join/leave increases linearly with the logarithm of group size.
Srđjan Capkun, et al. [4] propose a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, their approach does not require any trusted authority, not even in the system initialization phase.

Bechler et al. [5] developed a procedure called Cluster-Based Security Architecture for Ad. Hoc Networks. Since public key infrastructures with a centralized certification authority are hard to deploy they proposed a security concept based on a distributed certification facility. A network is divided into clusters with one special head node each and these cluster head nodes execute administrative functions and hold shares of a network key used for certification.

George et al. [6] designed and developed an innovative KMS which uses a modified hierarchical trust Public Key Infrastructure (PKI) model in which nodes can dynamically assume management roles. The roles that were undertaken by the nodes in the hierarchical model were: Root Certificate Authority (RCA), Delegated Certificate Authority (DCA), and Temporary Certificate Authority (TCA).

Bing Wu et al. [7] proposed SEKM (Secure and Efficient Key Management) which builds PKI by applying a secret sharing scheme and an underlying multicast server group. In SEKM, the server group creates a view of the certification authority (CA) and provides certificate update service for all nodes, including the servers themselves. A ticket scheme is introduced for efficient certificate service. In addition, an efficient server group updating scheme is proposed.

Yiling et al. [8] proposed a new group key management algorithm suitable for the wireless environment. This new approach is a two-level structure where the group of users are sub-divided into clusters, hence reducing the rekeying cost in the key updating. The paper also proposes that the method can achieve better efficiency when compared to the conventional Logical Key Hierarchy scheme.

Poovendran et al. [9] reported the distributing cryptographic keys to a secure multicast group with a single sender and multiple receivers. This paper addresses, the problem of storage, minimizing the GC (centralized group controller) key storage while preserving the logarithmic key storage and key update communication.

Hongmei Deng et al. [10] proposed a distributed key management and authentication approach by deploying the recently developed concepts of identity-based cryptography. Without any assumption of prefixed trust relationship between nodes, the ad hoc network works in a self-organizing way to provide the key generation and key management service, which effectively solves the problem of single point of failure in the traditional public key infrastructure (PKI)-supported system.

Jing Shyang et al. [11] reported about the main concern in a public-key setting i.e., the authenticity of the public key. This issue was resolved by identity-based (ID-based) cryptography where the public key of a user could be derived from public information that uniquely identifies the user. The paper also highlights about importance of Elliptic Curve Cryptography.

Owing to the advantages of IBE and ECC we further discuss the model construction.
3.0 MODEL CONSTRUCTION

In this section, implementation of algorithm by following a mathematical design principle is explained.

![IBE based Protocol for VANET](image)

Fig. 3 Architecture of proposed model

This section outlines the implementation of the design architecture which includes ECC, Pairings and finally IBE. First of all, the basics of Elliptic Curve Cryptography (ECC) theory which is the important development tool for all arithmetical calculations need to be known. Mathematics on Elliptic curve Arithmetic, Pairings cryptography and arithmetic of IBE are not covered. This section explains the basics of IBE and finally the model construction in detail. Examples of software functions are also presented. ECC is considered as the basis for all mathematical calculations for big integer arithmetic. Pairing based cryptography and Boneh Franklin's IBE schemes are discussed in detail ahead which forms our implementation.

3.1 Identity Based Encryption

Identity-Based Encryption (IBE) dramatically simplifies the process of securing sensitive communications. For example, the following diagram illustrates how Alice would send a secure message to Bob.

![Identity based encryption](image)

Fig. 4 Identity based encryption [17]

Step 1: Alice encrypts the email using Bob's email address, "bob@b.com", as the public key.

Step 2: When Bob receives the message, he contacts the key server. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements.

Step 3: After authenticating Bob, the key server returns his private key, with which Bob can decrypt the message. This private key can be used to decrypt all future messages received by Bob.

The private keys need to be generated only once, upon initial receipt of an encrypted message. All subsequent communications corresponding to the same public key can be decrypted using the same private key, even if the user is offline. Also, because the public key is generated using only Bob's email address, Bob does not need to have downloaded any software before Alice can send him a secure message.

3.2 Algorithm for Boneh-Franklin IBE

We are given \( p \) as defined above, \( E(F_p, \mathcal{P}) \) and its generator \( \mathcal{P} \) of order \( m \), as defined above, \( t \) such that \( m = p + 1 \), the map \( \mathcal{e} \), and appropriate cryptographic hash functions \( H_1, H_2, H_3, H_4 \) as public system parameters. Suppose, again, A wishes to send an encrypted message to Bob, B.

[A] Key Generation:

SYSTEM SECRET MASTER KEY (s): The system selects \( s \in Z_m^* \) randomly and guards this secret carefully.

SYSTEM PUBLIC KEY (Ppub): The system computes and then publishes Ppub = sP.

USER PUBLIC KEY (QID for identity "ID"): First the system (or any user) applies H1 to the ID to obtain an element \( y_b \in F_p \)

Then is computed

\[ x_0 = (y_b^2 + 1)^{1/3} \pmod{p - 1} \in F_p \]

Set \( Q = x_0 \cdot (x_0, y_0). \)

Then set \( Q_m = lQ \) so \( Q_m \in P \)

USER PRIVATE KEY (R_m for identity "ID"): The system computes RID = sQ_m which is distributed in a secure manner to the user identified by "ID".

[B] Encryption:

STEP 1: A computes B's public key, \( Q_m \), as described above from his identity B.

STEP 2: A computes

\[ r = H_1(rho, M) \in Z_m^* \]

Where rho is a random value, kept secret.

STEP 3: A computes and sends the cipher text

\[ C = rP, rho \oplus H_2(\mu_{m_x}^y), M \oplus H_4(rho) \]

Where \( (\mu_{m_x}^y) = \mathcal{e}_y(Q_m, P_{pub}) \) and \( \oplus \) is Boolean XOR.

[C] Decryption:

STEP 1: B receives cipher text \( C = (U, V, W) \).

STEP 2: B checks if \( U \in P \).

If not, reject the whole thing.

STEP 3: B computes \( rho = \mathcal{e}_y(W, H_3(\mu_{m_x}^y)) \) where R_m is Bob's private key, M' = W @ H_3(rho).

STEP 4: B computes \( r' = H_1(rho, M) \) and \( r'' = H_1(rho, M') \).

STEP 5: B checks if \( U = rP \).

If so, then \( r = r' \) and \( M' = M \) giving B the right message. Otherwise, B rejects the cipher text.

An efficient solution for ECDLP would allow to get \( r \) from \( P \) and \( s \) from \( P_{pub} = sP \) which would then divulge all private keys. Clearly, this "single point of weakness", namely \( s \), is a system vulnerability. Extra precautions need to be taken to assure its secrecy, though a "central secret" is not unheard of in the world of cryptography. Certificate Authorities (like VeriSignTM) used for authentication follow such a model [16]. So, it is critical that discrete logs be difficult to find in our problem setting. This means that ECDLP must be hard for \( \{P\} \) and DLP must be hard for the subgroup of mth roots of unity in \( F_p \). Thus, Fp should be chosen sufficiently large. [15]

The same steps are coded in C program to get four important functions. Each of the files are run in Linux environment for simulation. The message file is stored in IBE.txt file. Some of basic function programs flow diagram are presented next.

4. RESULTS AND DISCUSSIONS

In this section the simulation results of IBE system are explained. The screen shots of the program execution are presented. Further in the section the validation of the results is also explained in detail. All tests were performed on an Intel Pentium IV CPU running at 1.4 GHz with 640MB and SUSE Linux. The tests were run 10 times, and the raw results are available as below. The elliptic curve chosen for the simulation is
Fig. 5 Program flow of Elliptic Curve arithmetic

SETUP: In the first program, user need to enter a random 9 digit number, and then the program (PKG) chooses a 512 bit Prime number and a random point P on the elliptic curve. It then calculates the order of the point P as ‘q’. A master key ‘s’ is chosen and system wide public key is calculated as briefed earlier. The simulation time for the SETUP file to run is around 1.2 Secs.

EXTRACT: The parameters considered in the earlier program are declared global and are accessible by EXTRACT program also. Here the user authenticates his Vehicle ID and gets his private key. This is a one time generation when the vehicle is manufactured in the factory. The simulation time is less than a second and hence very fast.

ENCRYPT: In this case, the correspondent's vehicle ID is entered. Public key is generated and mapped on to the elliptic curve. The wellpairing is done as explained in appendix B (Chooses random strings T and U which can be set constant) and the message fileIBE.txt is encrypted. The times to execute the whole ENCRYPT program takes around 9secs which can be reduced by retaining T and U as constants.

DECRYPT: When the cipher text is received by Bob on the other end of communication channel. User system will be having the same SETUP parameters as depicted earlier. User enters a random strings T, U and his private key.

The Cipher text is decrypted if the Weil pairing Property is satisfied. The decrypt time is around 4 secs and can be reduced by keeping T and U as constants.

4.1 Performance Characteristics

To test the efficiency of the system, encryption and decryption of sample files using the IBE system was done and measured. The files were of three sizes to send: ‘First.txt’ (a 35byte file), ‘Second.txt’ (a 1.5 kilobyte file), and ‘Third.txt’ (a 10 kilobyte file). The tests were run 10 times, and the results are shown in the graph. The file size did not seem to affect the processing of the file to a very large extent.


