IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Analysis of Efficient Security Depends on Pairing Based ECC in VANET

K. Iswarya[1], K. Haridas[2]

M.Phil Research Department of Computer Science, NGM College, Pollachi, India[1]

Assistant Professor Department of Computer Science, NGM College, Pollachi, India[2]

Abstract: The Vehicular ad hoc network (VANETs) is self organizing network in which vehicles communicate with each other without the presence of any infrastructure. It has a wireless device send information to near vehicles and Road side units. It has prone to several different attacks. Here we need high security to secure our messages from the hackers. There are several algorithms to provide the security; ECC (Elliptic Curve Cryptography) is one of the algorithms that provide security by using minimum number of keys. In this paper we have discussed about the VANET security by using ECC. Elliptic curve arithmetic can be used to develop a variety of VANET security schemes including key exchange, encryption and digital signature.

Keywords: VANET, Security Requirements, ECC, Pairing based ECC, Encryption, Decryption

I. INTRODUCTION

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

The Vehicular ad hoc networks (VANETs), is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. It includes two types of communication that's are V2V communications and V2R communications and is important component of ITS. Communication between V2V and V2I are "ad-hoc" in nature. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet. ECC (ELLIPTIC CURVE CRYPTOGRAPHY) is one of the Algorithms which are used to provide security to this VANET. Public-key cryptography systems use hard-to-solve problems as the basis of the algorithm. The defense is "simple" keep the size of the integer to be factored ahead of the computational curve! In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington). ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curves combines number theory and algebraic geometry. These curves can be defined over any field of numbers (i.e., real, integer, complex) although it is generally used over finite fields for applications in cryptography. An elliptic curve consists of the set of real numbers (x, y) that satisfies the equation: $y2 = x3 + ax + b$. The set of all of the solutions to the equation forms the elliptic curve. Changing a and b changes the shape of the curve, and small changes in these parameters can result in major changes in the set of (x, y) solutions.

II. LITERATURE REVIEW

This section refers the background knowledge on security in ADHOC networking, cryptographic background and the various methods available for key management in vehicular ADHOC networks. Elliptic curve cryptography has been thoroughly researched for the last twenty years. The actual application of elliptic curve cryptography and the practical implementation of cryptosystem primitives in the real world constitute interdisciplinary research in computer science as well as in electrical engineering. Elliptic Curve Cryptography provides an excellent solution not only for the data encryption but also for the secure key transport between two communicating parties

M. Bayat, M. Barmshoory, M. Rahimi, and M. Aref, "A secure authentication scheme for VANETs with batch verification," Wireless Networks, vol. 21, no. 5, pp 1733-1743, 2015.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

Vehicular Ad-hoc Networks (VANETs) will start becoming deployed within the next decade. Among other benefits, it is expected that VANETs will support applications and services targeting the increase of safety on the road, and assist in improving the efficiency of the road transportation network. However, several serious challenges remain to be solved before efficient and secure VANET technology becomes available, one of them been efficient authentication of messages in a VANET. Previously they have discussed and analyzed a recent authentication scheme for VANETs introduced by Lee et al. Unfortunately this scheme is vulnerable to the impersonation attack so that a malicious user can generate a valid signature on behalf of the other vehicles. Based on the attack, they have proposed an improved scheme and introduce a simulation expressing the efficiency.

D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves," Journal of Cryptology, vol. 23, no.2, pp. 224-280, 2010

Elliptic curves with small embedding degree and large prime-order subgroup are key ingredients for implementing pairing-based cryptographic systems. Such "pairing-friendly" curves are rare and thus require specific constructions. Here they gave a single coherent framework that encompasses all of the constructions of pairing-friendly elliptic curves currently existing in the literature. We also include new constructions of pairing-friendly curves that improve on the previously known constructions for certain embedding degrees. Finally, for all embedding degrees up to 50, we provide recommendations as to which pairing-friendly curves to choose to best satisfy a variety of performance and security requirements.

M. Ghosh, A. Varghese, A. Gupta, A. Kherani, and S. Muthaiah, "Detecting misbehaviors in VANET with integrated root-cause analysis," Ad Hoc Networks, vol. 8, no. 7, pp. 778-790, 2010.

Misbehavior detection schemes (MDSs) form an integral part of misbehaving node eviction in vehicular ad hoc networks (VANETs). A misbehaving node can send messages corresponding to an event that either has not occurred (possibly out of malicious intent), or incorrect information corresponding to an actual event (for example, faulty sensor reading), or both, causing applications to malfunction. While identifying the presence of misbehavior, it is also imperative to extract the root-cause of the observed misbehavior in order to properly assess the misbehavior's impact, which in turn determines the action to be taken. This paper uses the Post Crash Notification (PCN) application to illustrate the basic considerations and the key factors affecting the reliability performance of such schemes. The basic cause-tree approach is illustrated and used effectively to jointly achieve misbehavior detection as well as identification of its root-cause. The considerations regarding parameter tuning and impact of mobility on the performance of the MDS are studied. The performance of the proposed MDS is found to be not very sensitive to slight errors in parameter estimation.

J. Tellez, S. Zeadally, and J. Camara, "Security Attacks and Solutions for Vehicular Ad-Hoc Networks", IET Communications Journal, vol. 4, no. 7, 2010

Vehicular ad hoc networks (VANETs) have attracted a lot of attention over the last few years. They have become a fundamental component of many intelligent transportation systems and VANETs are being used to improve road safety and enable a wide variety of value-added services. Many forms of attacks against VANETs have emerged recently that attempt to compromise the security of such networks. Such security attacks on VANETs may lead to catastrophic results such as the loss of lives or loss of revenue for those value-added services. Therefore making VANETs secure has become a key objective for VANET designers. To develop and deploy secure VANET infrastructures remains a significant challenge. The authors discuss some of the main security threats and attacks that can be exploited in VANETs and present the corresponding security solutions that can be implemented to thwart those attacks.

C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM'08, Apr. 2008, pp. 816–824.

Computing real-time road condition is really tough and it is not achieved using GPS. However, a malicious node can create multiple virtual identities for transmitting fake messages using different forged positions. A malicious vehicle can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions. To overcome these difficulties we propose that vehicle should be authenticated by Trusted Authority (TA) via RSU, only then the navigation query sent to RSU through tamper proof device (in the Vehicle) for identifying best destination route. After authentication, TA generates a re-encryption key to requested vehicle for encrypting the query. Based on vehicle request, contacted RSU identifies the shortest path to reach the destination RSU by passing the vehicle request to neighboring RSU's. After identification of shortest path, it sends the encrypted message to requested vehicle using re-encryption key. Finally it decrypts the message using its own private key. Moreover, the network checks each vehicle speed for avoid accident based on predecessor and successor vehicle's speed using chord algorithm. It also implementing priority based vehicle movement so, Network gives high priority in emergency vehicle, it gives medium priority for registered vehicle and it gives low priority for unregistered vehicle.

III. VANET SETTINGS

Several applications are enabled by VANETs, mainly affecting road safety. Within this type of application,

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

messages interchanged over VANETs have different nature and purpose. Taking this into account, four different communication patterns (depicted on Figure 2) can be identified:

V2V warning propagation (Fig. 1-a). There are situations in which it is necessary to send a message to a specific vehicle or a group of them. For example, when an accident is detected, a warning message should be sent to arriving vehicles to increase traffic safety. On the other hand, if an emergency public vehicle is coming, a message should be sent for preceding vehicles. In this way, it would be easier for the emergency vehicle to have a free way. In both cases, a routing protocol is then needed to forward that message to the destination.

V2V group communication (Fig. 1-b). Under this pattern, only vehicles having some features can participate in the communication. These features can be static (e.g. vehicles of the same enterprise) or dynamic (e.g. vehicles on the same area in a time interval).

V2V beaconing (Fig. 1-c). Beacon messages are sent periodically to nearby vehicles. They contain the current speed, heading, braking use, etc. of the sender vehicle. These messages are useful to increase neighbor awareness. Beacons are only sent to 1-hop communicating vehicles, i.e. they are not forwarded. In fact, they are helpful for routing protocols, as they allow vehicles to discover the best neighbor to route a message.

I2V/V2I warning (Fig. 1-d). These messages are sent either by the infrastructure (through RSUs) or a vehicle when a potential danger is detected. They are useful for enhancing road safety. As an example, a warning could be sent by the infrastructure to vehicles approaching to an intersection when a potential collision could happen.

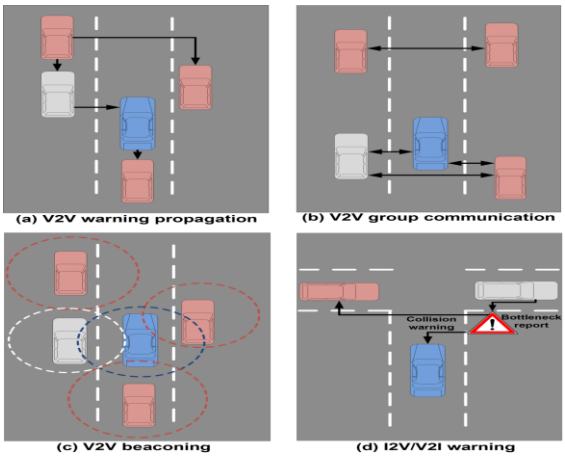

Figure.1

There exist other communication patterns over VANETs (e.g. related to multimedia access, location-based services, etc.). In particular, vehicles could use different communication media like cellular networks (e.g. GSM/GPRS) to get such services. However, we will focus on V2V and V2I road safety communication patterns over VANETs, as they will be more challenging from the security point of view. In fact, each communication pattern has a differ set of security requirements. This matter will be analyzed on the next Section.

IV. SECURITY REQUIREMENTS FOR VANETS

Taking into account the different entities and data at stake, in this Section a catalog of security requirements is built. Table 1 specifies the identified security requirements for each VANET setting introduced on the previous Section. Although I2V and V2I were considered to be the same setting, they have different security requirements and so they have been distinguished here.

Vanet setting/ sec. requirement	V2V warning propagation	V2V Group communication	V2V beaconing	I2V warning	V2I warning
Entity Identificatin	✓ (all vehicles)	x	✓ (Sender)	✓ (Sender)	✓ (Sender & Receiver)
Entity Authentication	✓ (Sender)	x	✓ (Sender)	✓ (Sender)	✓ (Sender & Receiver)
Attribute Authentication	x	✓ (Sender & Receiver)	x	x	x
Privacy preservation	✓	✓	✓		✓
Non-repudiation	✓ (Sender)	x	✓ (Sender)	✓ (Sender & Receiver)	✓ (Sender & Receiver)
Confidentiality	x	✓	x	x	**x**
Availability	✓	✓	✓	✓	✓
Data trust	✓	✓	✓	✓	✓

DOI 10.17148/IJARCCE.2016.5994

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

First of all, entity identification imposes that each participating entity should have a different and unique identifier. However, identification itself does not imply that the entity proves that it is its actual identity – this requirement is called entity authentication. Each of the application groups (enabled by the communication patterns previously introduced) has different needs regarding to these requirements. V2V warning propagation needs identification to perform message routing and forwarding – identifiers are essential to build routing tables. Sender authentication is also needed for liability purposes. Imagine that a regular vehicle sends a notification as if it were a police patrol. It should be then needed to prove the identity of the emitting node. In group communications it is not required to identify or authenticate the communicating peers. The only need is to show that both participating entities have the required attributes to become group members – this is the attribute authentication requirement. In fact, this is the only communication pattern that needs this requirement. In beaconing, identification and authentication of the sender is needed. Nearby vehicles can then build a reliable neighbor table. Both requirements are also present in I2V warnings, where only messages sent by the infrastructure are credible. Infrastructure warnings are sent to all passing vehicles within an area, so identification or authentication of the receiver is not needed. On the contrary, V2I warnings also require the emitting vehicle to be identified and authenticated. In this way, only vehicles with a trustworthy identity will be able to send such messages. Accomplishing the cited requirements should not imply less privacy. In fact, privacy preservation is critical for vehicles. In the vehicular context, privacy is achieved when two related goals are satisfied – untraceability and unlinkability (Gerlach, 2005). First property states that vehicle´s actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, second property establishes that it should be impossible for an unauthorized entity to link a vehicle´s identity with that of its driver/owner. However, this privacy protection should be removed when required by traffic authorities (i.e. for liability attribution). This requirement is present in all V2V communications. In fact, privacy should not get compromised even if different messages (no matter if under different communication patterns) are sent by the same vehicle. It does not apply to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received some message. It is needed for the sender in V2V warnings and beacons. In this way, if a vehicle sends some malicious data, there will be a proof that could be employed for liability purposes. In group communications it is not generally required, as the emitting node could be any of the group members. With respect to I2V and V2I warnings, non-repudiation of origin is needed, so wrong warning messages can be undoubtedly linked to the sending node. Non-repudiation of receipt is not currently needed, but it will be in the future. Currently, accident responsibility relies only on the human driver. However, in the future there are some envisioned applications that would automate partially the driving task. In such situation, not receiving a warning message could be critical for liability attribution. Another important security requirement in vehicular communications is confidentiality, that is, to assure that messages will only be read by authorized parties. This requirement is only present in group communications, in which only group members are allowed to read such information. The remaining VANET settings transmit public information. In fact, this requirement is not considered in some previous works (Lin, Sun, Ho, & Shen, 2007). Nevertheless, for the sake of completeness, it will be taken into account in this overview. The availability requirement implies that every node should be capable of sending any information at any time. As most interchanged messages affect road traffic safety, this requirement is critical in this environment. Designed communication protocols and mechanisms should save as much bandwidth and computational power as possible, while fulfilling these security requirements. It is present on all communication patterns, that is, it affects not only V2V communications, but also I2V ones. Finally, related to the information itself, data integrity and accuracy must be assured. Both needs are globally referred as data trust. Data at stake should not be altered and, more importantly, it should be truthful. It also implies that received information is fresh (i.e. refers to the current state of the world). False or modified data should lead to potential crashes, bottlenecks and other traffic safety problems. For this reason, data trust must be provided on all VANET communications.

V. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Recently the bilinear pairing such as Weil pairing or Tata pairing on elliptic curves and hyper elliptic curves were presented.

VI. PAIRING BASED ECC

The basic concept of cryptography is very simple. In a typical cryptographic exchange, information that is meant to be hidden for whatever reason is encrypted, or ciphered into a difficult-to-interpret form. This is called conversion, encryption because it involves the change of clear text, or understandable data, into cipher text, or difficult-to-interpret data. The encryption process in one-half of the entire cryptographic exchange.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 9, September 2016

At the other end of the process is decryption, or the conversion of cipher text into clear text. Decryption is not always a part of encryption, however- some algorithms are called "hashes" as they only apply encryption (that is, from clear to cipher text) and have no means of deciphering the information. However, most cryptographic algorithms can theoretically be cracked, but require extraordinary amounts of computational power to do so.
A safety message authentication scheme networks using an ID-based signature and verification mechanism. An ID-based technique offers a certificate-less public key verification, while a proxy signature provides flexibilities in message authentication and trust management. Message authentication, to ensure the receiving message is true and coming from the claimed source, the traditional message is true and coming from the claimed source, the traditional PKI security schemes are not suitable for VANET. Aiding of roadside unit(RSU) make message authentication in VANET easily, but it is still embedded some problems;

how to authenticate the message transmitted from different RSU range, and to process the vehicle's message hand-off among the different RSU communication range. A comprehensive message authentication scheme which enables the message authentication in intra and inter RSU range, and the hand-off within the different RSUs.

VII. CONCLUSION

Many attacks in VANET network can be prevented and detected by using ECC cryptography. It is used to analyze an efficient security depends on pairing based ECC in VANET. VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services. In this paper we had a brief discussion about the VANET security requirement and how the Vehicle communicates with each other by using paring based ECC.

REFERENCES

[1] Armstrong Consulting Inc. (n.d.). Dedicated Short Range Communications (DSRC) Home. Retrieved October2009,fromhttp://www.leearmstrong.com/DSRC/DSRCHomeset html
[2] J. Edge, An introduction to elliptic curve cryptography, http://lwn.net/Articles/174127/, 2006.
[3] Enge A. "Elliptic curves and their applications to cryptography", Norwell, MA: Kulwer Academic publishers 1999.
[4] Guicheng shen,Xuefeng Zheng, "Research on Implementation of Elliptic Curve Cryptosystem in E-Commerce", International Symposium on Electronic Commerce and Security,2008
[5] jia Xiangya, Wang Chao. "The Application of Elliptic Curve Cryptosystem in Wireless Communication", 2005 IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communication,2005
[6] T.Punitha1,M.Sindhu , "Pairing Based Elliptic Curve Cryptosystem for Message Authentication ",International Journal For Trends In Engineering & Technology Volume 3 Issue 3 – March 2015 ,pages-87-90.
[7] Bhuvaneshwari, S., G. Divya, K.B. Kirithika and S.
[8] Nithya, 2014. A novel approach for secured data
[9] transmission in VANET through clustering. J.
[10] Electron. Commun. Eng., 9: 23-30.
[11] Miller, V., 1986. Use of Elliptic Curves in Cryptography. SPRINGER, Advances in Cryptology-CRYPTO85 Proceedings, Williams, H.C., Springer, pp: 417-426. DOI: 10.1007/3-540-39799-X_31
[12] E. Aimeur, H. Hage, and F.S.M. Onana, "Anonymous Credentials for Privacy-Preserving E-learning," Proc. IEEE MCETECH Conf. e-Technologies (MCETECH '08), pp. 70-80, July 2008.
[13] G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)," Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010.
[14] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco ,"RFID technology for IoT-based personal healthcare in smart spaces,"IEEE Internet Things J., vol. 1, no. 2, pp. 144–152, Apr. 2014.
[15] G. Godor and S. Imre, "Elliptic curve cryptography based authentication protocol for low-cost RFID tags," in Proc. IEEE Int. Conf. RFID-Technol. Appl., 2011.
[16] Taher ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, vol 31 (4): 469–472, 1985.