IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Meliorated Cooperative Message Authentication Scheme in VANET

Anushree K[1], Divya K[2], Pavithra A[3], Asmitha Shree R[4]

Sri Krishna College of Technology[1, 2, 3]

Assistant Professor, Sri Krishna College of Technology[4]

Abstract: Most security- and privacy-preserving protocols in vehicular ad hoc networks (VANETs) heavily rely on time-consuming cryptographic operations which produce a huge volume of cryptographic data. These data are usually employed for many kinds of decisions, which poses the challenge of processing the received cryptographic data fast enough to avoid unaffordable delay. Now a day in Vehicular Communication, a Vehicular ad-hoc network (VANET) is facing problem with vehicle anonymity and location privacy while communicating among the vehicle. For security purpose Vehicular Public Key Infrastructure (VPKI) has been used. Security becomes very important for VANET considering the criticality of secured application. By using elliptic curve cryptography PKI algorithm provides trustworthiness of vehicular communications and privacy of vehicles, and enables vehicles to react to vehicular reports containing cryptographic data. New Technique HMAC provides secure and efficient communication in VANET environment. Using malicious Vehicular Analyzer algorithm and Elliptic Curve Cryptography (ECC) malicious messages are identified. It also detects the accident and other problems in the path of the vehicles. Elliptic Curve Cryptography (ECC) algorithm is used for stronger security during communication.

Keywords: Vehicular Ad Hoc Networks (VANETs), Vehicular Public Key Infrastructure (VPKI), PKI algorithm, Elliptic Curve Cryptography (ECC), HMAC, OBU, RSU.

1. INTRODUCTION

Thousands of people around the world die every year in road accidents and many more are severely injured. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. Vehicular Ad Hoc Networks (VANET) is used to collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it. VANET comprise of entities such as sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. The RSU distributes this data, along with data from road sensors, weather centers, traffic control centers, etc. to the vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. The network makes extensive use of wireless communications to achieve its goals but although wireless communications reached a level of maturity, a lot needed for such a complex system. The vehicles are connected to one other network when car goes outside of its range that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Ad hoc networks have been studied for issues of stability; reliability and scalability are of concern in VANET. The general architecture of VANET communication is with Road Side Unit (RSU).

In vehicular networks, it is expected that there will be limited access to an infrastructure network that will be supported by roadside base stations.

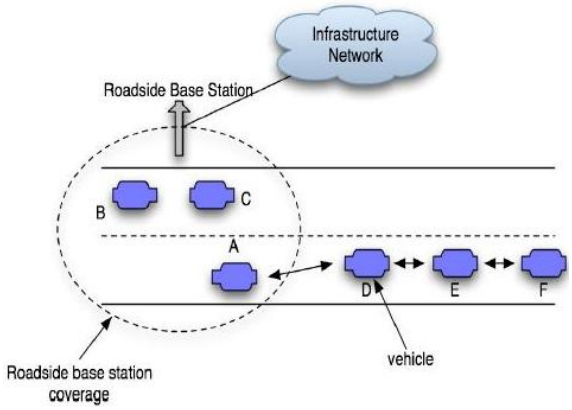


Figure 1: Vehicular Architecture

Such access is limited in its nature for two reasons. First, the deployment of the infrastructure is expected to be slow and incremental leading to wide areas where there is no access to the infrastructure. Second, a complete deployment is expected to be sparse because of cost. The coverage provide by a roadside base station may be on the order of 200-300m while roadside base stations may be placed every km or so. Consequently, not all vehicles will be connected to the infrastructure at all times. To obtain access to safety or other types of information, it becomes necessary to rely on vehicle-to-vehicle communications. Vehicles A, B, and C have access to a roadside infrastructure, which has limited coverage. These vehicles can obtain information from the roadside base station. However, vehicles D, E, and F have no communications with the fixed infrastructure. For instance, Vehicle F will

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

have to rely upon information from vehicle E, which in turn has obtained information that has passed through vehicles A and D. In this scenario immediately creates issues that how to disseminate information the security of information. The vehicles that are in the range of a roadside infrastructure may be connected to the infrastructure for extremely small durations of time because of small coverage and high vehicular speeds. So the amount of information that can be pulled from the infrastructure is necessarily limited. It is also possible that vehicles move into the range of the roadside infrastructure with some information obtained from cooperating vehicles they have encountered. The issue then becomes one of updating the information, enhancing the reliability or relevance of information or obtaining information that complements that already available to the vehicle

2. EXISTING SYSTEM

ECC based CRL, greatly reducing the checking time. Than the HMAC both of them are based on pseudonyms, few invalid messages for verification delay for a re-batch and then lose their efficiency. The performance analysis can achieve more efficient and security in ECC signature based authentication while keeping conditional privacy for VANETs.

3. PROPOSED SYSTEM

A protocol has been proposed that takes the advantages of the existing schemes and improves them so as to achieve authentication, conditional privacy and security against attacks. Provides data integrity, data origin authentication, non-repudiation, reliability and efficiency. It is based on ECDSA as a 160-bit key in ECC is as secured as 1024-bit key in RSA and, ECC is faster and occupies less memory space. Also it guarantees security as ECDLP is more secure as compared to its counterparts HMAC and CRL.

An RSU aided message authentication scheme also provides conditional privacy preservation. When a vehicle comes in the range of an RSU, it shall request the RSU for a temporary ID known as pseudo ID which will be valid till the vehicle moves to another RSU's range. Vehicle uses pseudo ID for its identity instead of its actual identity.

When the vehicle wants to send data the vehicle shall sign the message with its private key using ECDSA signature and append its temporary ID in place of sender address the vehicle which receives the message shall query the RSU for the public key of the sender vehicle and provides the sender's pseudo ID in the request. The RSU shall find out the actual ID from the pseudo ID and broadcast the corresponding public key of the sender vehicle. The interested vehicles shall verify the sender vehicles signature and thus authenticate the message but the sender' identity remains anonymous to the receiving vehicles.

3.1. Network Model

After taking into consideration both practical implementation and performance issues.

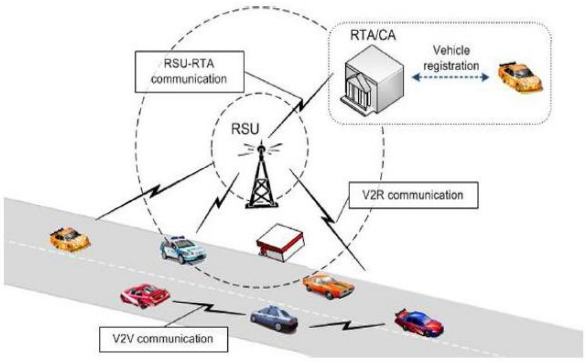


Figure 3.1 Network model of VANET architecture

A VANET composed of a large number of vehicles V = {V1, V2, ...} and a spot of roadside units (RSUs) R = {R1,R2, ...},. In the VANET, each vehicle Vi , V has a unique nonzero identifier and moves from one place to another either along a fixed route (e.g., bus) or by choosing a dynamical path (e.g., taxi), while each RSU Rj _ R is placed at some critical locations Lj in the area. The communications between vehicle and vehicle are bidirectional, i.e., two vehicles within the transmission range TV can communicate with each other. However, since RSU's transmission range TR is larger than TV, the communication between vehicle and RSU is not entirely bidirectional. Assume that the distance between vehicle Vi and RSU Rj is $D = |Vi - Rj|$. When $TV < D \leq TR$, only Vi can detect the existence of Rj; when $0 \leq D \leq TV$, Vi and Rj can communicate with each other.

3.2 RSU Installation Phase

After vehicle registered, the transport authority shall deploy RSUs at each road section. It shall upload the details of the entire vehicle registered till date to the RSU. In turn the RSU also will be registered with the TA and its public key shall be conveyed to all the registered vehicles.

3.3 Trusted Authorities

A VANET consists of three network components it guarantees the security as shown in (Fig 3.1:Network model of VANET) vehicles (users), Road Side Units (RSUs) and Regional Trusted Authorities (RTAs). The vehicle can be used by the passengers and it may be the driver.Vehicles in a VANET are equipped with tamper-resistant trusted components or tamper-proof device (TPD). RSUs are immobile and act as gateways to a VANET, outside networks are enabled with the vehicles Conventionally, the VANET is splitted into different regions (e.g., states or provinces), and an in individual region it seems to be assigned as RTA .The RTA which provides an authenticated recognition trusted party in a VANET for security to each vehicle in the network and is queried for investigation at the network. For revoking vehicles The RSUs assist the RTA in queries and in tracking the real identities of vehicles.

3.4 Vanet Mobility Model

One key component of VANET simulations is the mobility pattern of vehicles, also called the mobility model. Mobility models are used to determine the location

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

of nodes in the topology at any given instant, which strongly affects network connectivity and throughput. For example, the widely used Random-Waypoint Model (RWM) assumes that nodes move in an open field without obstructions. In contrast, the layout of roads, intersections with traffic signals, buildings, and other obstacles in urban settings constrain vehicular movement. The shortcomings of RWM are widely recognized and there has been recent research interest in modeling "realistic" mobility patterns specifically targeted for VANETs. Each of these works captures different levels of simulation. Vehicles cannot disregard physical constraints posed by the presence of streets and nearby vehicles. Every vehicle's movement is influenced by the movement pattern of its surrounding vehicles. For example, a vehicle needs to maintain a minimum safe distance from the one in front of it, increase or decrease its speed, or change to another lane to avoid congestion.

3.5 Cooperative Message Authentication

Propose an elliptic curve digital signature algorithm (ECDSA) based message authentication in a VANET.
The operation sequence of the proposed scheme is as follows:

1) Source vehicle generates private key and public key.
2) Public key is made available to all the vehicles in the VANET.
3) Source vehicle creates a hash of the message using secured hash algorithm.
4) Secured has his encrypted using private key in the source vehicle and ends it to the destination vehicle.
5) At the destination vehicle, the received encrypted message is decrypted using the public key. The result of the decryption will be the hash of the message.
6) Destination vehicle can then hash the message in the same way as source vehicle did and compare the two hashes strong authentication policy is provided for the destination vehicle. The most important thing defines all the elements in the elliptic curve before used by all the parties. That is called as the domain parameters of the scheme. Let p be the field in the prime case and the pair (m, f) in the binary case. The elliptic curve is defined by the constants (a, b) use in elliptic curve equation. And the order of G, be the smallest non-negative number n such that nG=∞, it is prime. Since is the size of a subgroup of E (FP) follows from Lagrange's theorem that the number H=⎪E (FP) ⎪is an integer. In cryptographic cofactor applications is called h, must be small and preferably h=1. The prime case the domain parameters are (p, a, b, N, g, h) and in the binary case they are (M, P, a, b, n, G,h). Several classes of curves are weak and should be avoided: Curves over F2M non-prime m are vulnerable to descent attacks. Curves such that n divides PB19=1(where p is the characteristic of the field – q for a prime field, or 2 for a binary field) for sufficiently small B are vulnerable attack which applies usual Discrete Logarithm Problem (DLP) on a small degree extension field of FB to solve ECDLP. Curves such that E (Fq) =Q are vulnerable to the attack that maps the points on the curve o the additive group of FQ.

3.6 Key Size

ECC achieves the security level with smaller keys. Key length is most important feature in Elliptic Curve Cryptography. FQ curve over needs 80-bit security, where Q=2160. The contrasted with finite-field cryptography (e.g., DSA) which requires 3072-bit public keys and 160-bit private keys, and integer factorization cryptography (e.g., RSA) which requires a 1024-bit value of n, where the private key should be just as large.

3.7 Asymmetric Data Encryption

Group manager distributes and efficiently allocates the public keys and authenticate by using the ECC authentication mechanism. The Group owner's file has been applied security. The confidentiality of this transformation is data in theory secure; we will simply give the safety via the cryptography formula named as ECC. Since client files are stored in the server, they have lesser security options. For crypto process the ECC algorithm for the encryption and decryption process.

3.8 Asymmetric Data Decryption

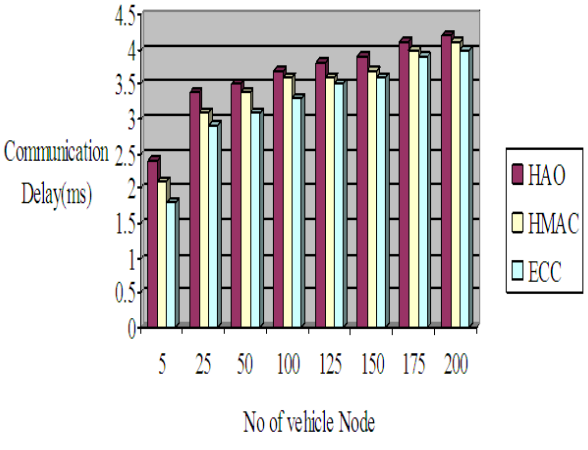
Using the ECC algorithm file is converted as crypto files. In order to get view the original content of the files, the encrypted files should be decrypted. Each and every encrypted file should be decrypted. Using Respective Private keys, files are decrypted using the ECC Key Generator Decryption process is done by ECC Algorithm, Since ECC has 166 key lengths it executes faster and more secured algorithm than RSA.20

3.9 Pairing

Pairing-based cryptography is used to pair two cryptographic groups to a third group to construct cryptographic systems. If the same group is used for the first two groups, the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group. In this way, pairings can be used to reduce a hard problem in one group to a different, usually an easier problem in another group.

4. RESULT

Average communication delay:



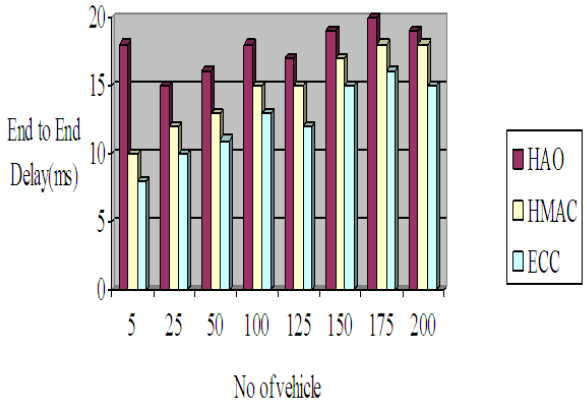
DOI 10.17148/IJARCCE.2016.5256

IJARCCE

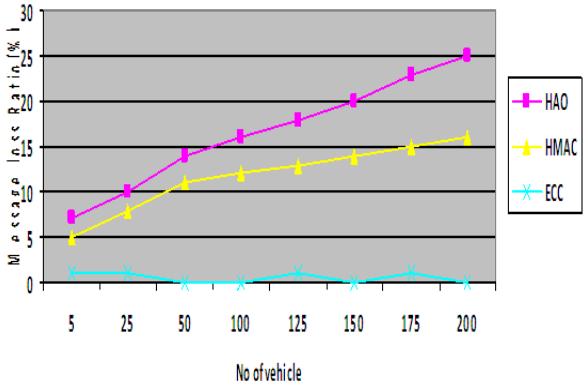
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Average communication End to End delay:



Message Loss Ratio:



5. CONCLUSION

The proposed method has to provide an efficient method for a class of ID based cryptosystem using Elliptic Curve Cryptography (ECC). The propose method focuses an ID-based ring signature scheme pairings with elliptic curve cryptography. The aim is to analyses security and efficiency of the pairing an elliptic curve is applied for secure id based cryptography. The proposed method is used to reduce the number of computations of the pairing for the verification of the id based signature and also decoding of the id based public key cryptosystems with authentication factor. The enhanced version of OLSR called V-OLSR designed for VANETs. The evaluation of OLSR protocol which routing metric is based on a source to receiver delay measurement and a cross layered physical BER ratio both measured when establishing a route, the delay parameter takes the precedence over the BER parameter. Elliptic Curve Cryptography (ECC) will be applied in the Vehicular Ad hoc Network (VANET).Hash function is going to use to verify the messages exchanged with the VANET environment. This will be helpful to achieve message authentication.

REFERENCES

[1] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mo- bile Netw. Veh. Environ. Anchorage, AK, USA, May 2007, pp. 103–108.

[2] W. Mao, Modern Cryptography: Theory and Practice. Englewood Cliffs, NJ, USA: Prentice-Hall, 2003.

[3] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with pro-tection against RSU compromise in group signature based VANETs," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, Dec. 2008.

[4] H. Krawczyk, R. Canetti, and M. Bellare, "HMAC: Keyed-hashing for message authentication," RFC 2104, Feb. 1997.

[5] C. P. Schnorr, "Efficient signature generation by smart cards," J. Cryptol., vol. 4, no. 3, pp. 161–174, 1991.

[6] A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in Proc. Top. Cryptol.—CT-RSA, vol. 5473, Lecture Notes in Computer Science, 2009, no. 2009,pp. 309–324.

[7] S. Frankel, R. Glenn, and S. Kelly, The AES-CBC cipher algorithm and its use with IPsec, RFC 3602, Sep. 2003. [24] D. Eastlake and P. Jones, US secure hash algorithm 1 (SHA1), RFC 3174, Sep. 2001. Telecommunications Conf., Atlanta, GA, USA, Dec. 2013,