International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244
Impact Factor: 4.054

FRAMEWORK FOR AUTHENTICATE THE MESSAGE IN VECHULAR AD-HOC NETWORK

Madhavi Sinha*

Ankit kumar**

Abstract: *Vehicular Ad- Hoc Networks (VANET) is a special kind of ad- hoc wireless networks that include wireless communication devices with short range, each representing a road vehicle or a static device. Networks VANET (Vehicular Ad- Hoc Networks) represents an area of research interest because of the advantages they bring in development Application traffic optimization , improve road safety , reduce pollution in major urban and more. Many experts consider that this form of ad- hoc network Mobile will become increasingly important in coming years. The development of applications and protocols for VANET networks pose problems unique security induced by devices used for vehicle or sporadic connectivity need to protect the identity of the users. Information which is passed in the VANET network frequently require increased measures to ensure the security of the message. This paper proposes a security protocol to ensure proper submission particular characteristics of VANET systems. The proposed solution is shown to be adequate to protect messages sent between participants traffic. Overall, this paper shows an experiment that wants to turn the compromise between advantages and disadvantages in a step forward in what concerns security in vehicular networks ad- hoc.*

*Associate Professor, Department of Computer Science &Engineering, Birla Institute of Technology, Mesra, Jaipur campus, Jaipur

**Research scholar, Dept. Department of Computer Science &Engineering, Birla Institute of Technology, Mesra, Jaipur campus, Jaipur

1. INTRODUCTION

VANET Vehicular Ad- hoc Network provides a communication protocol between nearby vehicles or between a vehicle and infrastructure. It is expected that to it use the wireless communication baseband 5.9Ghz technology using Dedicated Short -Range Communications (DSRC) .Cars are used to create a mobile ad- hoc network in which they communicate with each other. Each node is actually a wireless router that allows other nodes to connect to the network, expanding the range. It is estimated that the first systems that implement this technology will be designed for police and firefighters, so that the vehicle can communicate with each other for safety reasons. Vehicular ad- hoc network can be seen as a component of Intelligent Systems Transportation (ITS). The main purpose of these networks remains occupant safety and convenience of traffic. By equipping vehicles with communication equipment, and organizing them in ad-hoc networks, we do not remain just a step for the design of services and applications that improve vehicle driving experience. Vehicular ad-hoc networks (VANETs) provide infrastructure less, rapidly deployable, self-configurable network connectivity. The VANET network is the collection of vehicles interconnected by wireless links (Roadside Unit, OnBoradUnit) and willing to store and forward data to the other vehicles. As vehicles move in VANET and arrange themselves randomly, routing of message is done dynamically based on network connectivity and speed. Like the other network VANET network are particularly very important due in part to the vehicles' high rate of mobility and the many different signal- weakening barriers, such as buildings, in their geographical position.

Due to their huge potential, VANET have gained a huge attention in both industry and academic world. Research activities range from lower layer protocol design to safety applications and implementation of them is covered by all the country and universities. We need a safe and reliable VANET system, while exchanging information protect the VANET network against unauthorized message modification, message injection, eavesdropping. The security of VANETs is one of the most significant issues because their information transmission is transmitted in open access (wireless network) environments. It is essential that all transmitted data should not be injected or altered by users who have malicious goals or objective. Last few years VANET have usual increased attention as the potential

technology to promote the active and defensive safety on the road and the drivers, as well as travel ease. Trust and privacy are compulsory in vehicular communications for successful approval and deployment of such a technology.

2. STATE OF ART

Research on VANET security is abundant and demonstrates, PKI encryption and decryption are very complicated and create a large calculation overhead during communication to provide the security. The method which is used by Choi JY, Jakobsson M, Wetzel S (2005) Balancing auditability and privacy in vehicular networks. They use the RSA and MAC to provide message security and RSUs to authenticate message integrity. The method in assumes that each vehicle has a black box that generates the vehicle's public/private key. However, each key is very long because it is based on the continued product of two numbers, and this imposes a huge burden during message transmission.

Zhang C, Lin X, Lu R, Ho P-H, Shen X (2008) An efficient message authentication scheme for vehicular communications. (IEEETrans Veh Technol 57(6):3357–3368) proposes a security mechanism for excessive calculation burden during message authentication. When a vehicle enters an RSU's communication range, it negotiates with the RSU for a common secret key to send the hello message. When the vehicle requires to transmit a message to other vehicles, it calculates an HMAC value using with well known hash function, in combination with a secret key which is used to validate the message. When the RSU receives the message, it announces the result of message authentication within a fixed time interval to help the vehicle confirm the message's integrity. These announcements are sent at fixed time intervals to conserve network resources. Because the hash functions perform this calculation, the HMAC can provide quick authentication and decrease the burden of encryption and decryption.

As mentioned by the above two author there are two problems with their methods:-

1. Vehicles in different RSU communication ranges cannot authenticate with each other the message-receiving vehicle cannot confirm message integrity because it does not know the common secret key of the source vehicle.
2. Message handoff when a vehicle moves between different RSUs is problematic. When a vehicle moves from one RSU range to another, the new RSU must obtain the vehicle's certificate for source authentication before negotiating a new common

secret key. This authentication method is not only inefficient but also dangerous, because it frequently exposes certificates.

3. DIFFERENT SECURITY REQUIREMENT FOR THE VANET SYSTEM.

- **Confidentiality**: is the assurance that the data could not have been accessed by any other vehicles than the designated recipient for whom it was meant; thus insuring that the data was untouched in anticipation of reception. Confidentiality is generally obtained by cryptography techniques in VANET network.
- **Availability:** It is the section of time that a system is in a functioning tenure. In safety applications like post-crash warning in the wireless channel has to be available, so that forthcoming vehicles can still gets the warning messages. If the radio channel goes out (e.g. jamming by an attacker), then the warning message can never be broadcast and the application used itself becomes abject. Hence high availability of communication systems is obligatory.
- **Authentication:** It is the authentication of a vehicle to identity prior to granting access to the VANET network. It can be composed as the first line of defense against intruders in the VANET network... In safety application, where trust plays a prominent role. Authentication declares that the given message is trustworthy by correctly identifying the originator of the message. With ID authentication the receiver becomes worthy to have a unique ID of the sender. The ID could be the license plate or chassis number of the vehicle. In other cases receivers are not concerned with the actual identity of nodes. They are gratified if they are able to verify that the sender has a certain property with related to the vehicle authenticity. Property authentication is a security requirement that permits the verifying properties of the sender, e.g., a colored traffic sign. For applications using location information, location authentication allows to authenticate that the sender is essentially at the claimed position, or that the message position claim is valid.
- **Data integrity**: -It is the declaration that the content of the data was not modified while in transit. It differs from privacy trust and authenticity in the sense that it verifies that detection of data modifications.
- **Non-repudiation**: It is the process of authentication that the data was sent with vehicles credentials and other information so that without denial or repute the data

can be related to the sender vehicles. Non-repudiation aims to avoid one entity to deny having done some action. The most common examples in computer networks are related to sending some information (NRO, Non- repudiation of Origin) or receiving it (NRR, Non-repudiation of Receipt). However, both services are different by nature and so are their implementing mechanisms in VANETs.

4. PROPOSED METHODOLOGY

Security protocol is designed and implemented for vehicular ad-hoc networks with property as existing OBU (on board unit) which can communicate with each other and with existing infrastructure. T he aims to ensure the transmission of messages between different vehicle to securing vehicle communication in traffic .The method is designed for heavily traffic .which suffers from high dynamicity of the connecting the nodes in the network.

The main components considered in protocol design are Vehicle and Road Side Unit (CityTrafficLight). The component on which our framework work are

Messaging secured between vehicles in traffic is based on the existence of a third party certification authority present in that geographical area,

The distance between road side unit and vehicles who want to communicate,

The path on which they are moving, that the vehicle destination is in transmission range, or the need to select a route that includes several hops in the transmission of messages.

Communication between vehicles in a network characterized by a high degree of dynamism, geographical positioning, and sporadic connectivity between automobile securities problems unique. This protocol is aims to solve these issues, covering the following general issues relating to safety:

Vehicle is considered a mobile entity that exchange messages with other vehicle well with existing infrastructure (i.e. traffic road side unit at crossroads secure). The purpose Protocol is to provide a solution for securing messages between vehicles so that the entity to be able to check the validity of incoming messages. Secure traffic road side unit (part of infrastructure) have the role to verify the message and signed the message with third parties certification authority entities that help prove the authenticity of messages. Certifying Authority will knows that the road side unit can communicate with each other if they want to validate certain data. The main aspects that rely solution the sending of

ISSN: 2278-6244
Impact Factor: 4.054

messages, timing of car existing certification authority in the geographical area when communication happen. Protocol is modular, scalable, structured seen in the figure below.

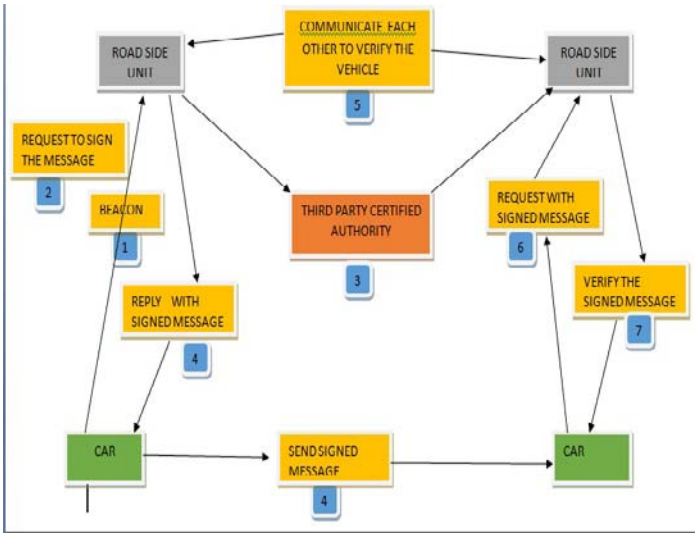

Fig: 1.0 new protocol design for secure VANET

The proposed method is structured in many states. Range of transmission of a car is less than the range of transmission of Road side Unit to Signing a secure message by Road side unit when a vehicle wants to send information to another vehicle, first Road side unit the beacon waits in whose coverage area is. Beacon message is transmitted periodically by all vehicle of zero coverage in a message broadcast (vehicle will transmit a data packet traffic light containing information that must signed by them .Considering the specific mobility transmission that has a vehicle, sending the message to be signed by the message that can be achieved in two ways:

The protocol is structured in several states. Communicating vehicle place only when the car has a message that is in coverage) of a Roadside unit. Transmission range of a vehicle is less than the transmission range of secure Road side unit. Signing a secure message by third party When a vehicle wants to send information to another vehicle, first road side unit has the beacon message waits in whose coverage area is .Beacon message is transmitted periodically by all vehicle of a message (broadcast) . Upon receipt Beacon vehicle will transmit a data packet traffic road side unit containing information that must considering the specific mobility in VANET networks and restricted area of transmission.

- When a vehicle wants to send information to another vehicle, first traffic road side unit the beacon waits in whose coverage area is. Beacon message is transmitted periodically by all OBU in the area of
- If the traffic light is in the range of the car, the message will be sent directly semaphore for signature
- If the traffic light is not in range of the car, the message will be routed, hop by hop through intermediate cars to reach the issuing beacon lights.

Important information contained in the package are the timestamp for the moment is the message, the current location and the actual message. All this information will be signed by the issuing beacon lights.

When the message gets back from the road side unit message with signature there on, vehicle will convey this message to the destination. If issued periodically beacon message is sent as a secure broadcast, the signed message to be sent back car is sent in the form of unicast, as the vehicle is in the range of the light. Message transmission to the destination vehicle can be done in two ways: target vehicle is in the range of the source vehicle, so the message is routed directly

Destination vehicle is not in range of the source vehicle, so the message is routed using existing intermediate cars to their final destination

When the message reaches the destination, the destination vehicle must validate that message before processing it. The way they could check a message on destination is sending it to a stop in the immediate neighbor. Road side unit communicate with each other so that the message can verify the signature. sending the message to the road side unit in the neighbor can be made directly, if it is within range (transmission) the car or routed through multiple hops (intermediate cars), if not in range. Data validation can be done only at the road side unit, this message and signature checking related fields which was established signature. Verification results will sent to the car who called validation for the message. If the answer is yes, then the message can be processed further, or otherwise it is discarded the message.

Geographical Location is a very important field that certifies that the message transmitter located in a specific geographic area. Footstep on the geographical position (latitude, longitude) requires network users to probing site. The easiest and safest way to check the

appearance of terms location is existent route infrastructure require validation infrastructure (road side unit secure) so when a car receives a message, all the infrastructure can decide whether to accept the message geared location.

At a high level, the location is a metadata component emitted from a wireless infrastructure (road side unit) for a mobile device. To use fingerprint positioning a application must trust infrastructure for validation geographical position. For any type of communication infrastructure require cars to sign those messages. Role infrastructure is only to sign and validate messages automotive transmission range.

6. STRUCTURE AND DETAIL OF SAFETY MESSAGES - DIGITAL SIGNATURES

Generating keys has two phases. The first phase of the algorithm is in choosing parameters::

1. Choose a hash function H. output hash function application can be truncated to size chosen pairs of keys.
2. Choose the key length L and N.
3. Choose a prime number of N bits. N must be less than or equal to the length of g. The result of applying the hash function.
4. choose a prime number p of L -bit mode so that p -1 to be a multiple of q
5. g is chosen , a number whose multiplicative order modulo p is q. It is set by choosing g = h(p -1) / q mod p for arbitrary h (1 < h <p -1) (check again if the result is equal to 1) . Usually h = 2.

The second phase of the algorithm computes the public key and private key for a user specifically:

1. Choose a random number x with the property 0 < x < q.
2. calculate y = pow(g,x)mod p
3. The public key is (p , q , g, y) .
4. Private Key is x.

6.1 Signing the message consists of the following:

Consider the hash function H and m message

1. generate a random value K for each post 0 <k <q
2. compute r = (pow(g,k)mod p) mod q
3. calculate s = (K-1(H (m) + x*r)) mod q
4. recalculate signature if r = 0 and s = 0 the signature is (r, s)

5. Signature accepting if at least one of the conditions 0 <r <q and 0 <s <q is not is satisfied
6. compute w = (s)-1mode q
7. compute u1 = (H (m)*w) mod q
8. calculate u2 = (r*w) mod q
9. compute v = ((pow(g u1)* y u2) Mod p) mod q signature is valid if v = r

The proof of correctness of the algorithm can be done as follows: first time, if g = h (p-1) / q mod p then it follows that g q ≡ h (p-1) ≡ 1 (mod p) according to Little Fermat Theorem Fermat. How g> 1 and q is prime, g have the same order of q

Algorithm used for creating the digital signature:

1. Choose two large distinct primes p, q. Calculate n=pq.
2. Calculate • (pq). This happens to be (p−1)(q−1).
3. Choose e such that gcd(e,• (pq))=1 and 1<e<• (pq).
4. Compute d such that de=1mod• (pq).
5. Do some crypto; c=te mod n and t=cd mod n.
6. . Fermat's little theorem states that ap=amod(p) An alternative, equivalent definition is that ap−1=1mod(p).
7. a• (n)=1 mod n
8. • (x) function, it's the number of numbers less than or equal to x which are also coprime to it. For any given prime p, every number less than itself is coprime to it, which means • (p)=p−1. If you're wondering about why • (1)=1, well, gcd(x,1)=1 is the definition of coprimality, including for 1 itself.
9. Now, it's also possible to get the value of • (xy)=• (x)• (y).
   n=pq⇒• (n)=• (p)• (q)⇒• (n)=(p−1)(q−1).

IMPLEMENTATION ISSUES

1. Only Road side unit have the authority to verify the signature .so there is no any such method by which vehicle can verify the message.
2. Each vehicle have the on board unit through which they can send and receive the message from road side unit or from the other vehicles.
3. A representation of a certifying authority which issue the certificate to each vehicle who want to join the VANET network.
4. A certificate which is issued by the certifying authority is valid up to one region of issue.
5. Relocation new certificate won't required in nearby location.

7. CONCLUSION:

In this paper, we have proposed the new secured model for VANET system for vehicle communication using public key cryptography which has very less overhead than other cryptography technique .Here we focus only why vehicular networks need to be secured, and this problem requires a specific approach to get the security in VANET network. We have proposed a model that identifies the most appropriate communication aspects. We have also identified the major threats and security flaw which is possible in VANET. The security framework along with the related protocols has been proposed which shows how and to what extent it protects availability, authorization, privacy, trust. We have been proposed that public key cryptography is suitable as solution for the considered problem. In terms of future work, we intend to further develop this Proposal. In particular, we intend to explore in more detail the respective merits of key distribution by the manufacturers or by governmental bodies; we will also perform additional numerical evaluations of the solutions.

REFERENCES:

[1] Carlos J. Bernardos, Ignacio Soto, Maria Calderon, "VARON: Vehicular Ad hoc Route Optimisation for NEMO, "Computer Communication 30(2007) 1765-1784

[2] D.Boneh, M.Franklin, "Identity-based encryption from the Weil pairings, "Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229.

[3] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati and Deepak B. Phatak, "A novel remote user authentication scheme using bilinear pairings, "Computers & Security, Volume 25, 2006, pp.184-189.

[4] Chun-Ta Li, Min-Shiang Hwang, Yen-Ping Chu, "A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks, "Computer Communications 31 (2008), pp.2803-2814.

[5] Chih-Yin Lin, Tzong-Chen Wu, Fangguo Zhang, Jing-Jang Hwang, "New identity-based society oriented signature schemes from pairings on elliptic curves, "Applied Mathematics and computation 160 (2005) 245-260

[6] Yi-Wei Lu , L Wu, "Electronic payment systems by group blind signatures, ". ethesys.yuntech.edu.tw, 2003.

[7] KG Paterson, "ID-based signatures from pairings on elliptic curves, "Electronics Letters, Volume 38, Issue 18, 29 Aug 2002 Page(s): 1025 – 1026

[8] Klaus Plößl, Hannes Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks, "Computer Standard & Interfaces, Volume 30, Issue 6, August 2008, Pages 390-397

[9] M. Raya, J. P. Hubaux, "Security aspects of inter-vehicle communications, "Proceedings of the 5th Swiss Transport Research Conference (STRC), 2005.

[10] M.Raya, J. P. Hubaux, "The security of vehicular ad hoc networks, "Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005, pp.11-21.

[11] M Raya, D Jungels, P Papadimitratos, I Aad, JP, "Certificate Revocation in Vehicular Networks, "Laboratory for Computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland, LCA-Report-2006-006

[12] Maxim Raya, Jean-Pierre Hubaux, "Securing vehicular ad hoc networks, "Journal of Computer Security, 15, 2007, pp.39-68

[13] Narn-Yih Lee, Chien-Nan Wu, Chien-Chih Wang , "Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings, "Computers and Electrical Engineering, Volume 34, Issue 1, January 2008, Pages 12-20.

[14] Neng-Wen Wang, Yueh-Min Huang, Wei-Ming Chen, "A novel secure communication scheme in vehicular ad hoc networks, "Computer Communications, Volume 31, Issue 12, 30 July 2008, Pages 2827-2837.