Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Framework for Group Authentication in VANET Network and its analysis

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

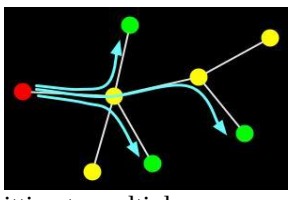
Madhavi Sinha
Associate Professor
Dept. Department of Computer Science & Engineering
Birla Institute of Technology, Mesra, Jaipur campus, India

Abstract— Group communication is indispensable in vehicle networks, while group of friends drives vehicles to travel together they can create a group to share information such as map information and multimedia , even if their vehicles are moving close or apart from each other on the same roadway. Securing the group from both outside or inside attackers is a prominent challenge in vanet system. Securing the group generally used the public key cryptography in the vanet system, which is a challenge to manage the key agreement and secured the communication between vehicles. Hence, an efficient cryptography schemes which has less computation overhead and less time complexity is essential. There are many different authentication protocols for vehicular networks particularly take the secure propagation of traffic-related information into account. So in this paper we used the group-based Elliptic Curve and Shamir secret sharing key exchange mechanism to authenticate the vehicles and validate the data propagation in secured group communication.

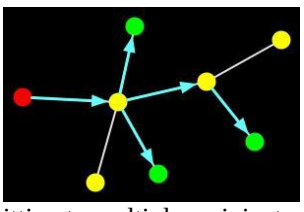
Keywords- Vehicle, Authentication, group communication, Elliptic Curve Shamir secret sharing exchange mechanism.

1. Introduction :

Group communication in vanet play a significant role in vanet communication .that means Group communication enable a vehicle in vanet network to efficiently send the information to an arbitrary set of different node who want to communicate in vanet network. By using the group communication a vehicle a node is rid of sending separate copies of the message for every target vehicle. It need only send one copy of the message and multiple copies of the same message are created and transmitted within the vanet network in a manner that cover all the RSU range vehicle.



Transmitting to multiple message using individual node-to-node connections



Transmitting to multiple recipients using multicast

Group communication in vanet is useful for implementing many network applications that involve communication in groups, e.g. video conferences, music sharing, Internet-based PayTV networks and online games.

1.1 Privacy in group Communication in vanet network

As in vehicle-to-vehicle communication, one of the most essential security concerns in group communication is maintaining the security of communication in open environment. How we could manage the vanet network vehicle that are in the same “group" exchange data such that outside the group can decipher what is being sent in the message. A natural way to guarantee this would be to have vehicle share a common shared key, called the group key, and to require that all group transmissions from any vehicle within the group be encrypted using that key. If the group is formed in the VANET network the group key is known to all the group members, then encryption protocol would trivially deal with the privacy problem. This, however, is not as affable as it seems. The facts are that in VANET groups are highly dynamic in nature vehicles leaves or join the group at various instances of time. The problem basically boils down to design a protocol that distributes a group key to all members in the group and that also updates the key over time such that only group manager or RSU(ROAD SIDE UNIT) is able to change the value of group key at any moment. Such a key

distribution protocol should certifies that for any instant t, the group key at a time t appears it cheacks the secrete share key which is generated by the help of group key whether it is matching or not. The group keys and hashed value S is given below helps in the following incidents:-

- ...are given access to all messages which is transmitted over the group (whether made at time t or any other instant).
- ... are allowed to join the group at instants before or after t (and thus to have full knowledge of group keys at other instants) and
- ... Are allowed to join together with each other (they can share any of the secret information that they have) in an attempt to break the protocol.

2. State of arts.

2.0 Homomorphic encryption

Homomorphic encryption technique is today commonly used for cryptography because it has very less computational overhead and it compute a wide range of functions with computational security. With the use Homomorphic encryption we can avoid the bitwise encryption which creates the scrambled circuits. Homomorphic encryption schemes are a special class of public key encryption schemes. The first Homomorphic cryptosystem, called the Goldwasser-Micali (GM) cryptosystem, was proposed in 1984[11]. Due to its prohibitive message expansion during encryption (i.e. each bit of plaintext is encrypted as a cipher text of at least 1024 bits), it is not practical for data mining applications. The natural extension of the Goldwasser-Micali (GM) cryptosystem is the Benaloh cryptosystem [21], which allows the encryption of larger block sizes of size 2048 at a time. Although the message encryption is not as bad as in the Goldwasser-Micali(GM) cryptosystem.

Benaloh cryptosystem unpractical for privacy preserving data mining .A more recent scheme is the Paillier cryptosystem [18], which avoids many of the drawbacks of the earlier Homomorphic cryptosystems. The Paillier cryptosystem use the new method for encryption they use the 1024 bit encryption message size of least 2048 bits large plain texts.

They use the following equation for cryptography.

A B

$E(w_1), \ldots, E(w_d)$

$$c = \sum_{i=1}^{d} E(w(i))^{v(i)}$$

2.1 Secret Sharing

Secret sharing was introduced independently by Shamir [3] and Blakley [2] in 1979. They proposed that one user has a secret which it distributes among n other users in a way that none of the n users alone can recover the secret. They have shared the secret in such a way that the information of at least t of the n users is needed to recover the secret which is computed by using the hash function with the secret key, where t is a predefined threshold. If less than t parties are attempted to recover the secret will fail and they will not learn anything about the secret. A (t, n) secret sharing scheme is a set of two hashed functions S and R. The function is a one way hashed function which generates the shared value S and takes the input secret s and creates n secret shares key:

S(s) = (s1, . . . , sn). The two functions are selected in a way that, for any set I €{1, . . . , n} of t indices R(I, s0t1 , . . . ,siti) = s. Furthermore we require that it is impossible to recover s from a set of t − 1 secret shares. A secret sharing scheme is additively Homomorphic scheme if R (I, st1 + s0t1 , . . . , St1 + St0) = s + s0.

A very simple (n, n) additive secret sharing scheme is S(s) = (r1, . . . , rn−1, r), where ri is random for i €{1, . . . , n − 1}, and r = s − Pn−1 i=1-r. To recover s all secret shares are added: s = r +Pn−1.

3.0 PROPOSED DESIGNE FOR FRAMEWORK

Key element:

a) RSU (Road Side Unit): the Road side unit is responsible to register the vehicle who wants to participate in vanet to form a group. The responsibility of road side unit is to issue a secret token to each user during registration. Later, authentication process is performed based on the secret tokens issued by the road side unit. Since tokens are used in authentication of vehicle identity which is protected. In order to prevent malicious vehicle to reveal their tokens to attackers, each token is a unique integer which is dynamically generated by the RSU which is the function of a polynomial.

b) Group vehicle: Join a group in vanet and become a group vehicle, each vehicle needs to register with the Road side Unit to send their request with their identity and their Identity certificate (issued by Government trusted Authority). Based on their identity provided to RSU they check their identity with the help of trusted authority and conformed with their identity after being successfully registered with Road Side Unit, each user receives a secret token from the RSU (road side unit). Each Vehicle with a unique token can prevent malicious Attacker to give their tokens to Impersonators.

c) Attackers: We consider the attacker from both side (outsider attacker or insider attacker) the inside attackers are the vehicles who are genuine vehicle and own genuine tokens from the RSU. We consider that the insider attackers may

collude to forge tokens for non-group vehicle. The outside attackers are imitator who do not own any tokens and try to impersonate vehicle to fail the authentication protocol. We also assume that the RSU does not collude with any user. If the RSU colludes with any vehicle by revealing the secret of the RSU to the vehicle, the colluded vehicle can do harm to the group. In addition, we assume all vehicle acts honestly in the authentication. If any vehicle acts dishonestly by revealing an invalid value, the authentication is failed.

3. One Ime Authentication Protocol For Vanet Group Communication:

In our model we have assume that there are n number of vehicle such that V1, V2 …Vn are already register with the RSU.

1.1 System setup

SCHEMA 1:

During registration, RSU constructs a random value (t -1)th (i.e., t<n) degree polynomial f (x) with f (0) = S , and computes secret tokens of users as Yi= f(x) , for i= 1, 2,..,n, where xi is the public information associated with user Vi . RSU sends each token Yi to vehicle Mi secretly.

RSU makes H(s) is publicly known, where H is a one-way hash function. The threshold value t is an important security parameter that has very high impact on the security of group authentication protocols. Using a (t,n) secret sharing scheme to issue tokens in the registration can prevent up to t- 1 inside attackers, who are legitimate vehicle, colluded together to forge tokens. From now on, we assume that there are j vehicle with their tokens f(x1), f(x2),..,f(xj) where T< j<n, who want to execute the group authentication protocol. The basic idea of this protocol is that each vehicle releases the token obtained from the RSU during the registration process. If all released tokens are valid, the outburst of the released tokens can reconstruct the secret "S". One-way hash of the secret is used to compare with the one-way hash of the reconstructed secret. If there is illegitimate vehicle who does not own a valid token on the polynomial f (x), the reconstructed secret will be different from the secret S.

They follow the following algorithm to validate the authenticity of vehicles in group communication.

Step 1: Each Vehicle Vi reveals his token f(xi) , to all other vehicles simultaneously.

Step2: After knowing all tokens, f(xi) for i=1,2,....j. we use to reconstruct the value of secrete by using the Lagrange interpolating formula . Each vehicle has

$$S' = \sum_{i=1}^{j} f(x_i) \prod_{r=1, r\neq j}^{j} \frac{x_r}{x_i - x_r} \bmod p$$

Where P is the prime number and p>(f(0)=S) and after compute the value of H(S') and H(S) for all the vehicle in the group who want to participate in the group the compare the value of Hash function H(S) and H(S') .all the vehicle whose hash value is matched then they are authenticated and the vehicle whose hash value is not matched then they are malicious vehicle .

This authentication protocol is used only one time since the secret and tokens are exposed to the entire vehicle in the group. The authentication not only one-to-one authentication protocol this is also a many-to-many authentication. The proposed framework is very efficient to authenticate multiple vehicles belonging to the same group without revealing identity of each vehicle.

SCHEMA 2: GROUP AUTHENTICATION PROTOCOL WITHOUT REVEALING TOKENS

In schema 1 token are revealed to the entire group of vehicles present in the group, each token which is generated by shared key can be used once for authentication. The secret s is also exposed to the entire vehicle in the group. We propose a way to protect tokens to share among all the group members. In addition, the secret does not require to be recovered in each authentication. Group authentication in vanet without revealing tokens, authentication can be archived by without revealing tokens and the secret to the entire vehicle. The basic idea of our approach vehicle has the property of strong t -consistency. Let each vehicle select a random polynomial with (t -1)th degree and generate shares for other vehicle. Then, each vehicle releases the additive sum of his own token obtained from the RSU during the registration and sum of shares of polynomials generated by vehicles. Due to the property of secret sharing, the released sums are shares of the secret polynomial f (x) of tokens and sum of polynomials generated by vehicle. If all vehicles act honestly and own valid tokens, the released sums should be strong t -consistent; otherwise, the released sums are not strong t -consistent. Since the vehicle do not need to reconstruct the secret in the protocol and the tokens have not been exposed straight, the RSU does not need to publish the one-way of the secret s during system set up and the tokens can be reused.

Each vehicle Vi selects a random polynomial, f (xi), with (t -1)th degree. For the Polynomial f (xi), vehicle Vi computes shares as fi(xr) , for r=1, 2,..,j, r≠i , for other vehicle. Vehicle Vi sends each share, fi(xr) to vehicle Vr secretly.

After receiving fi(xr) for r=1, 2,..,j, each vehicle uses his token fi(xr) to compute

$$y = f(x_i) + \sum_{i=1}^{j} f_r(x_r) \bmod p$$

Step3. After knowing Yi, for i= 1, 2,. ..j, each vehicle checks whether they are strong t - consistent. If they are not strong t -consistent, there are illegitimate vehicle; else, all vehicle have been successfully authenticated belonging to the same group.

The protocol is as follows:

For each new RSU $K = n+1,...,2n$:

1. All the old vehicle (1…n) agree on the next number – K.
2. Each i'th vehicle ($i \in [1...n]$) randomly chooses a polynomial Pi(X) of degree t-1 where Pi(K) = 0 and $Pi(0) \neq 0$.
3. Each i'th vehicle $i \in [1...n]$ distributes shares of Pi(X): $P_i(1),...,P_i(n)$ among the old vehicle.
4. Each i'th vehicle $i \in [1...n]$ receives $P_1(i),...,P_n(i)$ and calculates: $h(i) = f(i) + \sum_{c=1}^{n} P_c(i)$, then sends h(i) encrypted to the K'th vehicle .

The K'th vehicle decrypts these shares and interpolates them to find out his new share - f(K) (which equals to h(K)).

4. Computational complexity of this proposed system.

The most time-consuming operation for each vehicle is to check the strong t -consistency of released values Y_i for i=1, 2,..,j, in checking strong t -consistency needs to compute the interpolating polynomial of values y_i . The polynomial interpolation becomes the main computational task in our proposed framework. However, the modulus p in our polynomial interpolation is much smaller than the modulus in most public-key cryptosystems, such as RSA cryptosystem [13]. This algorithm is not like the conventional algorithm this proposed authentication protocol authenticates all users at once. Thus, the framed authentication protocol is very efficient in comparing with all existing authentication protocols. When we analysis the any cryptographic algorithm then we consider generally the two thing. Time complexity of the algorithm and what is the space complexity of the algorithm here we will compare encryption-based techniques and secret sharing with respect to these three factors in the following. Public key encryption schemes are (by definition) based on computationally difficult problems, and thus require expensive operations such as modular exponentiation of large numbers (in the order of 1024 bits in size). In contrast it is very efficient to compute secret shares when using the framework describe above by choosing a random polynomial and valuating it in n points. The polynomial is chosen over the same field as the secret key, which means that usually all computations are done with ordinary integers. As we know that public key encryption schemes create cipher texts of at least 1024 bits (with the exception of Elliptic curve based encryption schemes). If we want to use the Homomorphic properties of an encryption scheme we have to encrypt each input in its own cipher text. But in our framework we have use Elliptic curve cryptography which force the secret key in the size of 160 bits. In contrast, secret sharing creates n shares of each input, where each share is of the same size as the secret. We thus always have an overhead of n. secret sharing is for each multiplication requires that each pair of parties exchange information between them. Having to wait for the transmission of these messages at each multiplication clearly slows down the protocol.

To attain the high security we have round the function up to 20 time so we use 2-20 level of security, so we have choose k = - 5, t = 4 (for 2-30, increase these values by 1. the number of modular multiplication to verify the identity is in this algorithm is t(k ± 2)/2 = 14. The number of bytes exchanged in the protocol by the parties during the proof is 323, and the secret si values can be stored in a 320 byte. Even better performance can be obtained by increasing k to 18 (1152 byte). With t = 2 iterations, the number of transmitted bytes drops to 165 and the average number of modular multiplication falls down to 7.6 (which is two times of magnitude faster than the 768 multiplications required by the RSA encryption). The time, space, communication and security of the scheme can be traded off different ways, and the optimal choices of k, t and the eij matrix depend on the relative costs of these resources. Unlike the RSA scheme, the two parties can pipeline their operations (with A preparing xi+j and Yi+j while B is still checking xi and yi), and use parallel multipliers to compute the product of vi or si values in log k depth. Since the protocol uses only multiplication (and gcd or division operations which are very easy to parallelize).

Conclusion:

Key management for secure group communication is a challenge in ADHOC networks. The key management of secret key is the planned in such way that they easily solve the security and privacy of group communication. According to the scenario of group communication, group of friends travelling together can easily obtain the identity and shared key of group of all vehicles. For this reason, it is awkward that a new vehicle can join to the group during the period of traveling. We propose a special type of group authentication framework which provides high level of security without additional overhead of computation and less time complexity. The founded group authentication protocol can be used to authenticate all type of, many-to-many and one-to-one, and can authenticates multiple vehicle at once. We first propose a basic one-time group authentication protocol and then propose a general group authentication protocol without revealing tokens. Our proposed group authentication protocol is very efficient because their computational time is a function of polynomial p (n).

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 29 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, "ComputerCommunications, Volume 31, Issue 12, 30 July 2008, Pages 2827-2837.

