MODIFICATION THE SECURITY OF FLIP PROTOCOL BY CHANGING THE BASE POINT SELECTION

Nabamita Deb and Moumita Roy

Department of Information Technology Gauhati University
Guwahati, India

ABSTRACT

One of the most promising applications in VANETs is vehicle chatting, which allows like-minded vehicles to chat on the topics of common interest on the road. But, some privacy challenging issues emerged recently in vehicle chatting application. The probable issues are how to find a like-minded vehicle on the road and how to prevent one's interest privacy (IP) from others who are not like-minded. In this paper, in order to address these challenging issues, we study an efficient privacy preserving finding like-minded vehicle protocol (FLIP), and apply the provable security technique to enhance its security.

KEYWORDS

VANET,vehicle chatting, ECC, base point, ECDSA, interest privacy, finding like-minded vehicle

1. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) have been subject to extensive research efforts not only from the government, but also from the academia and automobile industry in recent years. In VANET, an OnBoard Unit (OBU) device is attached with all vehicles which allows them to communicate with each other, i.e., vehicle-to-vehicle (V-2-V) communication, as well as to the Roadside Units (RSUs), i.e., vehicle-to-infrastructure (V-2-I) communication. Now, if we compare it with the traditional ad hoc network, then it can be seen that the hybrid of V-2-V and V-2-I communications makes VANETs more promising, and it can also provide a board of safety-related (e.g., emergency news, warning about collisions) and non-safety-related (vehicle-vehicle chat, sharing files, downloading videos on the road) applications which are basically close to our day to day activities.

And because of these applications, VANETs are being attractive to the public. Though several researches are being conducted on VANET, but as per our knowledge, the interest privacy, as a special privacy requirement in vehicle chatting application, has not been yet explored much. Therefore, how to identify a vehicle who is like-minded and establish a shared session key for secure chatting, and how to prevent other vehicles who are not like-minded from knowing one vehicle's interest have become two newly emerging privacy challenges in vehicle chatting application.[4]

DOI:10.5121/ijcsit.2017.93011

2. SYSTEM MODEL AND DESIGN GOAL

2.1 SYSTEM MODEL

We consider a scenario which consists of a number of vehicles V = {V1, V2, · · ·} and a single offline trusted authority (TA). Since our problem is confined to the scenario where vehicles are required to find like-minded vehicles with common interest on the road without the assistance of RSUs, RSUs are not included in our current model. Trust Authority (TA): TA is a trustable and powerful entity. Its responsibility is to manage the whole network, such as, to initialize the system, to register the vehicles in the system by assigning a finite set of pseudo-IDs and the corresponding key materials to each vehicle. It should be noted that TA is an offline entity and is not directly involved in the V-2-V communications.

When two vehicles Va, and Vb ∈ V are within their transmission range, they can chat on the topics of common interest on the road.

2.2 DESIGN GOAL

Security requirements and design goal: Security and privacy are always of vital importance to the flourish of vehicle chatting application in VANET. Without the guarantee of vehicle's privacy including identity privacy, location privacy and interest privacy, vehicle chatting application can't be widely accepted by the public. Therefore, it is essential to protect vehicle's privacy. Specifically, the following security requirements should be ensured in vehicle chatting application:

i) Vehicle's real identity should be protected;
ii)Vehicle's location privacy should be guaranteed; and
iii) Vehicle's interests should be protected against others who don't have the common interest.

In regard of the former two security requirements, each vehicle can use pseudo-ID to conceal the real identity, and periodically change multiple pseudo-IDs to achieve the location privacy. However, for the third security requirement, vehicles should use some IP-preserving protocols to find other vehicle that have the common interest on the road. Concretely, when a vehicle Va wants to talk with another vehicle Vb nearby, if Vb has the common interest with Va, Va and Vb can establish a shared session key used for secure chatting on the topics of common interest. However, if Vb doesn't have the common interest with Va, neither Va nor Vb can know the counterpart's interest. Besides the above requirements, the time complexity should be less, the computational cost needed should be less and the protocol should be resistant to attacks. In this paper, these points will be taken into consideration.

3. OPTIMUM BASE POINT CHOICE ALGORITHM

Base point or generator point selection in ECC is the prime step for its security. The efficiency of the choice of base point is needed for reducing the time complexity of the algorithm thereby reducing the overall computational cost. So, the effectiveness of base point is necessary. Some chooses a random point on the curve as base point while some chooses the smallest point on the curve as the generator point. But there are some algorithms which gives optimum base point

selection method. One such method is described below and it uses quadratic residue of mod p to find the base point [1]. The base point of ECC on GF(p) is given below:

In ECC of GF(p), p is a prime number and Fp is a finite field of mod p. ECC uses modular arithmetic, so in modular form, the elliptic curve equation E over Fp can be defined as:

$$y2modp = (x3 + ax + b)modp, \qquad where\ 4a3 + 27b2 \neq 0modp$$

Here, a and b are the curve parameters as stated earlier. Now if there is a point (x,y) which meets the above equation, then the number (x, y) is a point on the elliptic curve E. E(Fp) is used to represent set of all point which meets the curve E. The domain parameters of ECC on GF(p) are (q, a, b, p, n, h) where q is the module, a and b are the coefficient of ECC, n is the order of the base point, h is the cofactor of n.. Let assume a and p are integers, p>0, so if there is solution to x2 = a mod p, we called a is quadratic residue of mod p; if the solution doesn't exist, a is quadratic non-residue of mod p. if the numbers among 1,2,…, p which are relatively-prime with p must be quadratic residue of mod p, but some of them may be congruent about mode p. The basic idea of the algorithm is that at first we have to select an effective random point on the curve and then scalar multiplication is done using the random point. Finally, the scalar multiplication value is being used to judge the base point of the elliptic curve.

ALGORITHM 1: THE BASE POINT CHOICE ALGORITHM OF ECC ON GF(P).

Input: a, b, p, n, h.

Output: Effective base point G on curve having order n.

Steps:

S1. Randomly choose x ($0 \leq x < p$);

S2. a =(x3 + ax + b) mod p;

S3. Judging whether a belongs to quadratic residue of mod p, if so y is gotten, marked G = (x, y) go to S4, if not, go to S1.

S4. According to point G to compute G = hG, then judging whether G meets y2 = x3 + ax + b and G is not infinite point. If so, G is the solved base point, then go S5, if not, go to s1.

S5. Return G

ALGORITHM 2: TO JUDGE WHETHER A IS QUADRATIC RESIDUE AND GET THE COORDINATE Y.

Input: a, p, among them, a is gotten from S2 of Algorithm 1, p is mod;

Output: a, y, among them, a is gotten from S2 of Algorithm 1, y is y-coordinate;

STEPS:

S1. If a=0, return (0, 0), or go to S2

S2. sum←0, y←1, i←1

S3. for i←1 to p do
sum← (sum+i) mod p,

if a=sum then

return (a,y),

else y←y+1, i←i+2,

if i=p

return (-1,-1)[1].

4. FLIP PROTOCOL

In this section, we study our basic protocol which is efficient privacy -preserving finding like-minded vehicle protocol (FLIP and it mainly consists of two parts: system initialization and privacy preserving finding like-minded vehicle on the road.[3]

4.1 SYSTEM INITIALIZATION:

Notation: Let an integer k € N, then 1ª is the string of a 1s. If x,y are two strings, then x||y is the concatenation of x and y. In system initialization phase, the Trusted Authority (TA) first initializes the whole system by running the following steps. Given the security parameter l, TA generates an elliptic curve group G = <P>, where the generator P is being chosen with the protocol described in section (IV). Then, TA chooses a random number s € Z*q as the master key and compute the corresponding system public key Ppub = sP . In addition, TA also chooses four secure hash functions H, H0, H1, and H2, where H : {0, 1}* → G and Hi : {0, 1}* → Z*q , for i = 0, 1, 2. In the end, TA publishes the public system parameters params as {G, P, q, Ppub, H, H0, H1, H2} and keeps the master key secretly. When a vehicle Vi € V itself to the system, TA first checks the vehicle Vi's validity. If Vi is valid, TA generates a family of pseudo-IDs and the corresponding key materials for Vi using Algorithm 3. In such a way, Vi can constantly change its pseudo-IDs to achieve identity privacy and location privacy on the road.

When a vehicle Vi € V itself to the system, TA first checks the vehicle Vi's validity. If Vi is valid, TA generates a family of pseudo-IDs and the corresponding key materials for Vi using Algorithm 3. In such a way, Vi can constantly change its pseudo-IDs to achieve identity privacy and location privacy on the road.

ALGORITHM 3: VEHICLE REGISTRATION ALGORITHM

1: procedure VEHICLEREGISTRATION

INPUT: *a verified vehicle Vi € V*

OUTPUT: *a family of pseudo-IDs and the corresponding key materials*

2: choose a family of unlinkable pseudo-IDs PID = {pid1, pid2, · · · }

3: for each pseudo-ID pidi € PID do

4: randomly choose a private key xi € Z*q

5: compute the corresponding public key Yi = xiP

6: assert (pidi, Yi) with certificate certi signed by TA with s

7: end for

8: return all tuples (pidi, xi, Yi, certi) to Vi

9: end procedure

B. Privacy-preserving Finding Like-minded Vehicle:

When a vehicle Va € V is on the road and wants to find a like-minded vehicle Vb € V on the common interest *Iα* nearby, they will run the following steps to establish a shared session key sk regarding the common interest *Iα*.

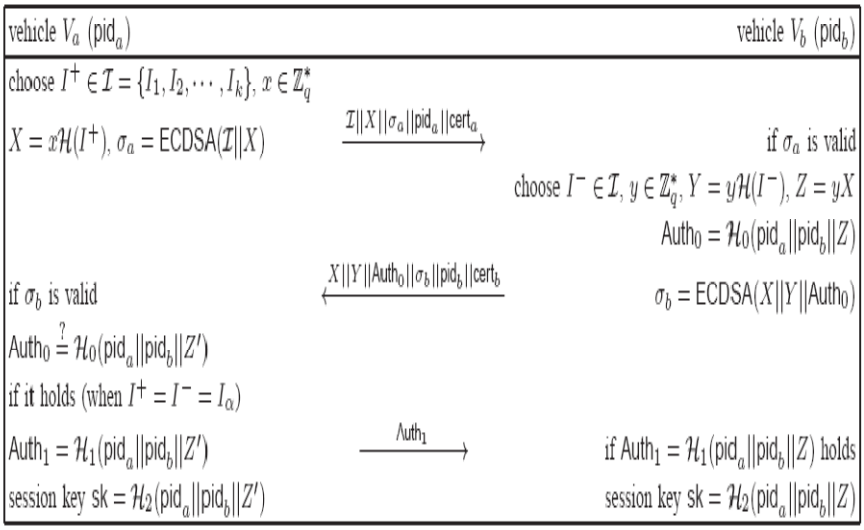

Figure.1: Privacy-preserving Finding Like-minded Vehicle Protocol [3]

Step 1

Va first sets an interest set I, which consists of k kinds of interests {I1, I2, · · · , Ik}, where Va's actual interest I+ is involved. Then, Va chooses a random number x € Z*q, computes X = xH(I+), and uses the ECDSA algorithm to make a signature σa = ECDSA(I||X) on I||X with regard to the pseudo-ID pida and the certificate certa. In the end, Va broadcasts the request I||X||σa||pida||certa to the nearby vehicles.

Step 2

Upon receiving the request I||X||σa||pida||certa, a nearby vehicle Vb first checks the validity of σa with pida||certa. If it is invalid, Vb neglects the request. Otherwise, Vb chooses his interest I– € I and a random number y € Z*q , computes Y = yH(I–), Z = yX, and Auth0 = H0(pida||pidb||Z). In addition, Vb makes a signature σb = ECDSA(X||Y ||Auth0) on X||Y ||Auth0 with regard to the pseudo-ID pidb and the certificate certb, and returns the response X||Y ||Auth0||σb||pidb||certb to Va. Note that, in the protocol, Vb is only allowed to make at most one response for the same request.

Step 3

After receiving the responsor Vb's response X||Y||Auth0||σb||pidb||certb, the requestor Va first checks the validity of σb with pidb||certb. If it is invalid, Va neglects the response. Otherwise, Va computes Z'= xY , and checks whether Auth0?=H0(pida||pidb||Z'). If it holds, Va computes and sends Auth1 = H1(pida||pidb||Z') to Vb, and calculate the session key sk = H2(pida||pidb||Z').

Step 4

When Vb receives Auth1 = H1 (pida||pidb||Z'), he checks whether Auth1? = H1 (pida||pidb||Z). If it holds, Vb calculates the session key sk = H2 (pida||pidb||Z). If I+ = I– = Iα for some $1 \leq \alpha \leq k$, Va and Vb have the shared session key sk, i.e., the vehicle Va successfully finds an like-minded vehicle Vb on the road.

As it can be seen that, ECDSA is being used for signature generation and verification, now besides strengthening the base point of ECC, we can also strengthen the hash function required to be used in ECDSA. From [3], it is not being said which hash function is used, but here we use Sha-256 in place of the traditional Sha-1 which is normally being used in ECDSA. The reason Sha-256 is being used is because of the fact that it is more secured than the other hash algorithms and moreover it shows efficient results while coding with java. A comparative study is being shown in [11, 12, 13, and 14] about the advantages of taking Sha-256 in place of other hashing algorithms. Since the protocol steps remain the same, so with that the correctness of the protocol follows.

5. EFFICIENCY

The efficient and optimum choosing of base point made the protocol more efficient in terms of computational costs. If we consider Tm being the time taken for one point multiplication with the generator point G and Ts and Tv the time taken for ECDSA signing and verification, respectively, then since these operations are mainly responsible for the speed of FLIP, we can neglect others such as hash operations. Now, from the FLIP protocol of [3], only 2Tm + Ts + Tv will be required by both the requestor Va and the responsor Vb. The execution time of Tm is being found as nearly 2.11 ms, that is Tm ≈ 2.11 ms, and based on the results of [7], we know, Ts ≈ 2.14 ms, Tv ≈ 3.58 ms for a 256-bit ECDSA. Then, the computational costs are only 2Tm + Ts + Tv ≈ 9.94 ms. Since, efficient choosing of base point reduced the computational cost to a good extent, that is, the time taken to perform one point multiplication, ECDSA signing and verification, has been found very less and therefore, it is more efficient than the one described by [3].

6. SECURITY ANALYSIS

We know ECDSA signature cannot be forged and if the transcripts are being altered by the adversary, it will get detected. Now in the paper of FLIP by Rongxing Lu et.al. it is already proved that its IP can be protected in the due time and since we also used the same tool that is ECC and same basic protocol, then obviously in the enhanced one its IP will also be protected. In addition to that we used an optimum base point choice algorithm which is more efficient than the one in [3]. The base point choice algorithm reduces the time complexity to [1] which is better than the one considered in [3], thereby reducing the overall computational cost. Along with that, in ECDSA, SHA-256 is being taken as the hash function which strengthens the security of FLIP protocol because the security of ECC lies in its efficient base point selection and strong hash function.

7. PERFORMANCE EVALUATION

In the FLIP protocol, in order to prevent successive guessing attack from non-like-minded vehicle, the responsor Vb is only allowed to respond once for the same request. Therefore, when large number of interests is being considered by the requestor Va, the harder the actual interest Iα € I can be guessed by non-like-minded vehicle, and thus the IP can be protected. But when the size of the interest becomes large, it takes more for Vb to choose the correct interest which causes delay in finding like-minded vehicle. So, in this section we implement the protocol in java with the changes being made and try to record how the size of the interest affects the time taken required to find like-minded vehicle. Fig 2 reflects the time taken for finding a like-minded vehicle under the different size of interest.

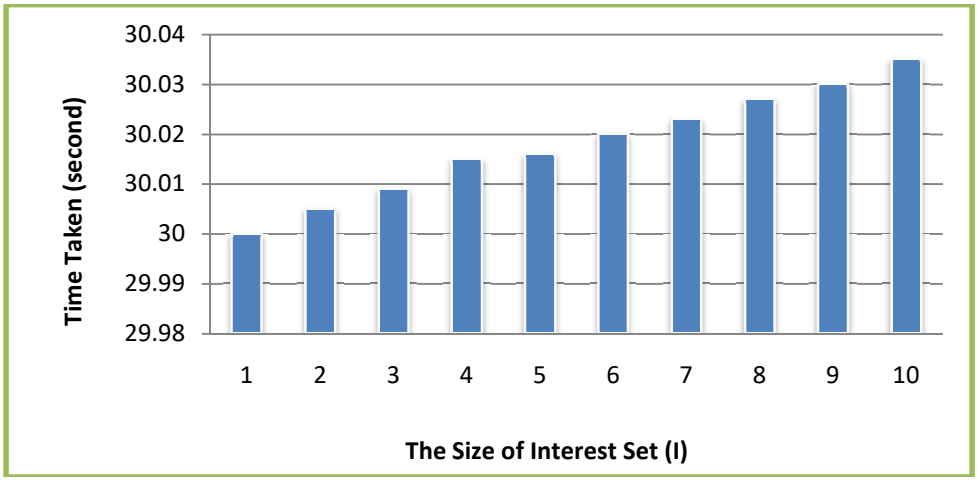

Figure. 2 : Time Taken For Finding Like-minded Vehicle under different I

8. RELATED WORK

Recently, several research works have been reported [5], [6], which are closely related to the proposed FLIP protocol, but focus on other scenarios different from VANETs. Different from the other works, Rongxing Lu [3,4] proposed FLIP protocol, can provide mutual authentication and establish a shared session key between two like-minded vehicles. The security of ECDSA

algorithm lies in the efficiency of base point selection. So, in this paper, we tried to give an efficient base point algorithm through which the security of ECDSA increases thereby increasing the security of FLIP algorithm. Also the overall computational cost is also found to be reduced to a good extent and more importantly, it is a provably secure protocol suitable for VANET scenarios.

9. CONCLUSION

Protecting vehicle's IP can be done by secure finding like-minded vehicles protocol (FLIP) and its importance is hugely related to the success of vehicle chatting application on the road. But, this scenario hasn't paid enough attention in VANET. In this paper, we have tried to study the FLIP protocol, which is an efficient IP preserving protocol, and tried to make it more secure by making changes in the base point thereby reducing the overall computational cost and taking sha-256 as the hash function which is better than the traditional SHA-1 and others in terms of security. In addition, the vehicle's IP is also preserved that is because the protocol keeps each other's IP-preserving if two vehicles don't have the common interest and so, it can be widely accepted by the public.

REFERENCES

[1] Cui, Y., Hu, Y., & Li, T. (2010). An Optimization Base Point Choice Algorithm of ECC on GF(p). 2010 Second International Conference on Computer Modeling and Simulation, 4, 103-105.

[2] Security Issues in Vehicular Ad Hoc Networks by P. Caballero-Gil University of La Laguna, Spain. Online at http://cdn.intechweb.org/pdfs/12879.pdf

[3] Lu, R., Lin, X., Liang, X., & Shen, X. (2010). FLIP: An Efficient Privacy-Preserving Protocol for Finding Like-Minded Vehicles on the Road. 2010 IEEE Global Telecommunications Conference GLOBECOM 2010. doi:10.1109/glocom.2010.5684211

[4] Ho, P., Zhang, Z., & Lu, R. (2008). Special Issue on "Security and Privacy Preservation in Vehicular Communications" Wileys Security and Communication Networks Journal. Security and Communication Networks, 1(3), 191-193. doi:10.1002/sec.34

[5] M. Atallah and W. Du, "Secure multi-party computation problems and their applications: a review and open problems," in NSPW, 2001, pp.13–22

[6] G. Zhong, I. Goldberg, and U. Hengartner, "Louis, lester and pierre: Three protocols for location privacy," in PET 2007, ser. LNCS 4776, 2007, pp. 62–76.

[7] http://www.cryptopp.com/benchmarks.html

[8] http://www.javamex.com/tutorials/cryptography/hash_functions_algorithms. shtml#algorithms

AUTHORS

Nabamita Deb is working as Assistant Proff in the Dept of IT,Gauhati University, and

Moumita Roy is a masters student in the same department