A Novel approach for Implementing Security over Vehicular Ad hoc network using Signcryption through Network Grid

Vijayan R
Network and Information Security Division
School of Information Technology and Engineering
VIT University
Vellore, India

Sumitkumar Singh
Master of Technology
School of Information Technology and Engineering
VIT University
Vellore, India

***Abstract*— Security over Vehicular ad hoc network and identifying accurate vehicle location has always been a major challenge over VANET. Even though GPS system can be used to identify the location of the vehicle they too suffer from major drawbacks. A novel approach has been suggested by the author wherein the VANET is made more secured by using Signcryption technique and at the same time unique approach of using Network Grid to flawlessly identify the location of the vehicle has been proposed.**

Keywords- Network Grid; Computation Server; Vehicular Node; Public/Private keys.

I. INTRODUCTION

The invention of Vehicular ad hoc network has eased the burden of communication over Vehicle to Vehicle communication and Vehicle to Interface communication. But VANET as compared to Mobile ad hoc network or MANET is highly dynamic and unsecured. Providing security and at the same time preventing the current transmission to attain loss due to frequent path breakage over VANET has always been a major challenge. Moreover, the computation cost required over VANET should be less as compared to MANET. So, even if a security protocol is to be implemented over VANET care must be taken so that the computation cost doesn't increase. A unique public key cryptography technique Signcryption as proposed by Zengh [1] has been suggested in this paper. Signcryption is a cryptography technique which combines the two step of Digital signature and Encryption in one step and hence reduces the computation time up to great extent as compared to Signature-then-Encryption.

The Digital Signature for the automobiles has been proposed in [2]. The major drawback of this technique involves higher computation cost as more number of machine cycles is required for the computation as compared to Signcryption process. The Signcryption provides an entire feature to enhance the security measures like Confidentiality and Integrity of the message. Different types of attacks over VANET have be stated in [4] [5]. The detailed process of using Signcryption will be explained in the proceeding sections. As now we have dealt with the security part we have proposed a technique which can be used to prevent the data transmission loss due to frequent path breakage that often appears over VANET. Many papers have suggested the use of GPS [6] system over VANET but GPS system too faces some serious drawbacks which can be dangerous in some situations. [3] have suggested the advantages of using DSRC therefore DSRC shall be used in this model. Some of the drawbacks of GPS System are the Cost which has to be minimized when being used over VANET, Inaccuracy since not all the GPS devices are updated hence the system cannot state the exact updated road conditions, the network coverage can be weak in challenging locations like between obstacles like tall buildings or sparse coverage areas and many more. In order to minimize these drawbacks we have proposed a unique technique of dividing the entire geographical locations in to network grid and assigning every intersection a unique network ID. An Infrastructure based model has been suggested over this network wherein the vehicle to vehicle communication will be established through the Roadside units (RSU) which are in turn connected to the Computation server (CS). The Details of this process will be explained in the proceeding sections.

II. NETWORK MODEL ENTITIES

The proposed network model as in Fig: 1. consists of Computation Server (CS), Roadside Unit (RSU) and nodes model.

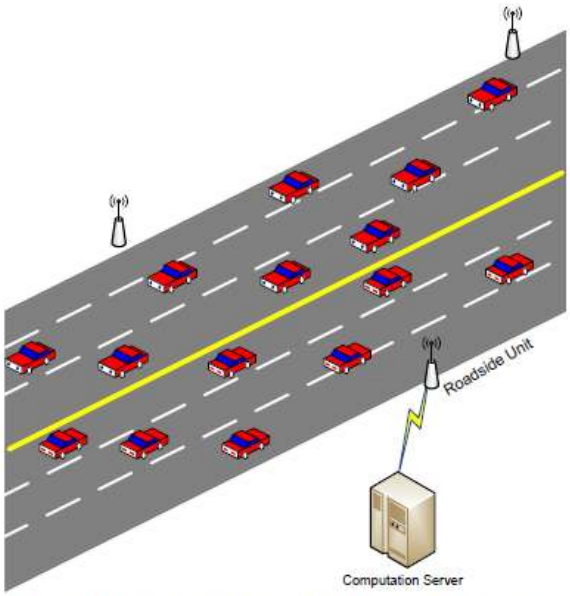

Fig:1 Represents Network model Comprising of Computation Server, Vehicles as nodes and Roadside Units as Access Point

The following are the entities that participate in this network.

A. *Computation Server*

Computation server is responsible for generating unique public and private key as requested by the Source node. The request from the source node is forwarded to the Computational Server through the RSU. The CS is also responsible for selecting the suitable RSU for sending data to the vehicles over the network based on the computation of the current velocity of the vehicle which is received in the request packet from the vehicle.

B. *Roadside Unit*

The RSU acts as an access point between CS and the vehicle. The RSU is responsible for transmitting the requested packet from the vehicle to the CS where the further computation is done.

C. *Vehicular Node*

The Vehicular nodes are the entities which will exchange messages through the CS. Every node possesses a unique Vehicular ID (VID) through which it is identified. In case of source node, the source node will be aware of the destination nodes unique id (DID). Based on the DID the source request the CS for the transmission. The detailed process of transmission is explained in proceeding section.

III. PROPOSED NETWORK MODEL

The proposed network model uses Signcryption as the security model whereas Network grid to identify the location of the vehicles. In our model every vehicle is supposed to register with the service provider before entering into the network. Once registered, every vehicle will be assigned a unique Vehicle Identity (VID). This ID can be the vehicles chassis number or the vehicle number. After the registration every vehicle will be identified by its VID. During the process of registration, the vehicle will also be given the IDs of the other vehicles allowed to communicate within the network. For a source vehicle the destination vehicle will be identified by its destination ID (DID) which itself will be the VID of the destination. After getting assigned by Unique identification number the vehicle is now allowed to transmit within the network. Our model follows proactive routing technique wherein every node is required to transmit beacon at regular interval to identify its location to other nodes within the network. These beacons are also received by the CS which can be used to transmit the packet to the node which is not within the transmission range of the Source node. The initial transmission requires the Source vehicle to send REQUEST packet to CS which will contain the Current Velocity (CV), Vehicle ID (VID), Destination ID (DID) and Time (T) at which the message was created. Once the Request packet is received by CS the initial computation is done over the REQUEST message. First, the VID and DID is verified and if found to be true the further computation is done. Public and private keys are now generated and are transmitted to the Source and destination nodes. The transmission is done by evaluating the CV and forwarding the packet to appropriate RSU. Our model follows a unique network grid model which allows the CS to accurately identify the location of the node and forward it accordingly.

The detailed step of Network Grid will be explained in proceeding section. Once the keys are received by the source node the process of Signcryption [1] is carried out. The detailed step of Signcryption is explained in proceeding section. After the Signcryption, the processed packet is transmitted to the CS by encrypting it with the Shared Key between the Source node and the CS. The processed packet also contains the current velocity of the source node. After receiving the encrypted packet from Source node the CS decrypts the packet and sends the packet to destination node depending upon its location over Network Grid. The destination node now receives the packet and Unsigncrypt the message to obtain the original message.

IV. THE NETWORK GRID

A unique network grid is followed in this paper. The entire geographical region is divided into grid as in Fig 2. In highways or in the urban areas the roads are normally divided into Lanes.

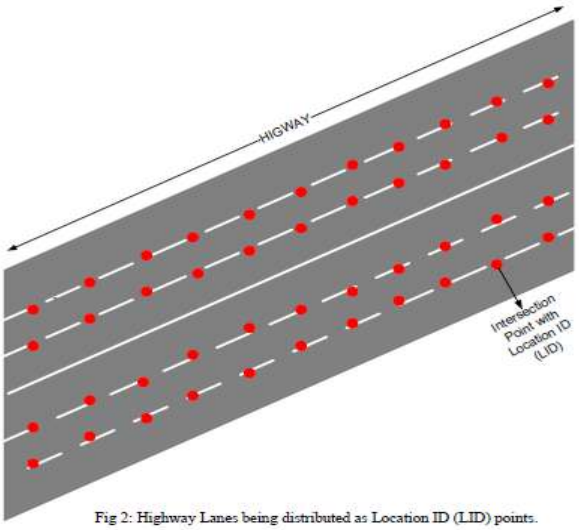

Fig 2: Highway Lanes being distributed as Location ID (LID) points.

Therefore we can make use of such geographical features and divide the Lanes into Network Grids as in Fig.2

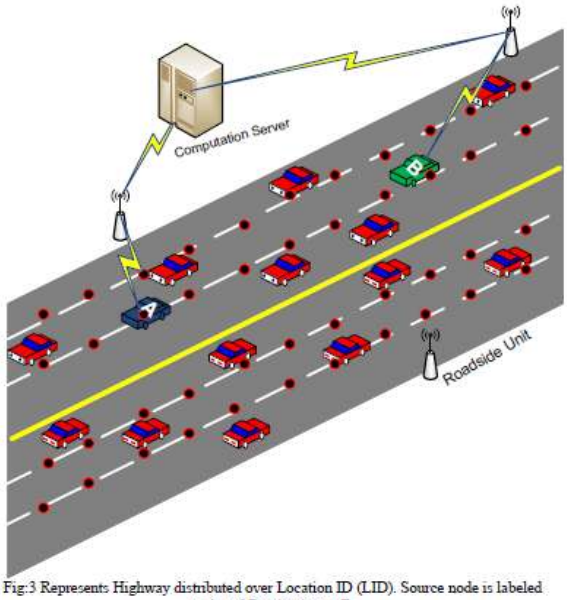

Fig:3 Represents Highway distributed over Location ID (LID). Source node is labeled as A and Destination as B.

As in fig 3, the CS receives the packet from a particular intersection. Every RSU are kept at a required distance from the intersections based on its transmission range. Consider a scenario as in Fig 3, where the source node needs to send packet to destination node. The source node first sends the packet by encrypting the packet with unique shared key between Source and CS. The REQUEST packet will contain CV, VID, DID and T. After verifying the IDs the CS will now calculate the CV of the vehicle. This is required since we are working over vehicular network and the vehicle may cross the transmission range of the current RSU after the computation at the CS. During the process of calculation of the CV of the vehicle the CS also evaluates the Time T at which the message was generated. As in Fig 4: which shows a typical propagation delay of the packet which is transmitted from the vehicle at a specific position to the RSU. Based on this delay of message transmission and Current velocity of the message the location of the Vehicle can be identified. As mentioned earlier on that our model follows proactive routing hence every node knows about the current location of the neighboring nodes and also the CS is aware about the nodes as the packets are also received by the RSU. Once the LID of destination node, as requested by the source, is identified the keys are transmitted to the destination node and source node. Once the Keys are received the process of Signcryption is carried out as explained in proceeding section.

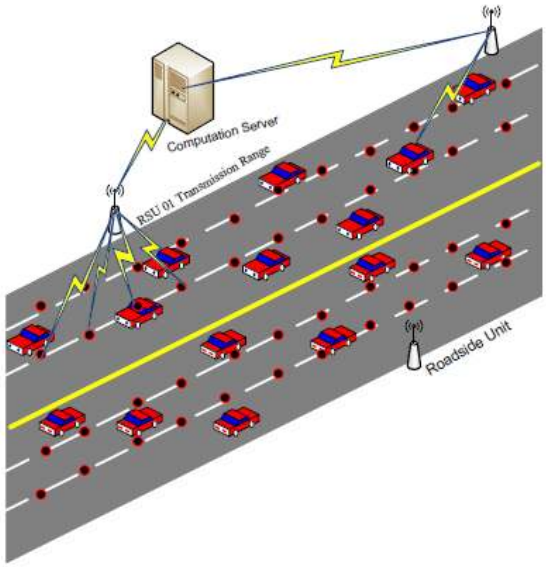

Fig 4: RSU 01 having transmission range over Locations. The message received from last lane node is assumed to have a propagation delay of 30ms whereas message received from middle Lane is assumed to have propagation delay of 60ms.

V. Security Features

The Source node in our model first checks for the location of destination and creates a REQUEST packet containing CV, VID and DID. This whole packet is encrypted by the shared key SKC used between Source node and CS. On receiving the request from the source node for the transmission to the desired destination the CS first checks the VID of the source node. If the ID is forged the node is immediately removed from the network. Thus the source node is termed as malicious or attacker node and is informed to all the nodes within the network about this node. Every node on receiving this message will update their database and remove the node from their destination list. After the verification, CS generates Public key and private key pairs for Source node and destination node and Shared key SKN which will be used by source to encrypt and transmit Cipher text ‘c’, value ‘r’ and ’s’ and by destination to decrypt to obtain the message.. The type of encryption used will depend upon the level of security required by the network. All the keys and values that are generated by the CS are sent to source and destination by encrypting it with their SKC. After receiving the Keys the Signcryption process is carried out at the Source node. The Algorithm 1 represents the detailed process carried out during the transmission. The Notations used during a message transmission are shown in TABLE – I

A. Signcryption at Source

Once the sender has received the PU_a and PR_a it can now perform Signcryption [2] over the message that is to be sent to the destination. It is understood that destination has received the PU_b and PR_b and is ready to receive the message from source node.

Algorithm used for evaluating the message at VANET server from Source Node for Single Mode of Transmission

Algorithm 1:

1. E(SKC[REQUEST(CV,VID,DID,T)]) from source node 'a'
2. Search(VID==VID)
3. **IF** found (VID==VID) **Then {**
4. Generate PU_a,PR_a, PU_b, PR_b
5. **E**(SKC[RPLY(ID_{new},PU_a,PR_a,SKN)]) to Source node
6. **E**(SKC[SEND(PU_b,PR_b,SKN)]) to Destination node
7. **} Else** (Remove Source node from the network)

Following steps for Signcryption are carried out as described in [1] by the source node. The Signcryption process is then followed by the process of Unsigncryption as described in [1].

- Source node selects random value 'x' where x is in the range of (1,…,q-1). This chosen random value 'x' will be used in further Hash function.
- The source now selects PU_b and random value x to compute Hash function out of it. This creates a 128bit string. K = H (PU_b mod p) where 'p' is a large prime number.
- The 128bit key obtained is divided into two halves K1 and K2.
- Source now uses AES encryption technique and encrypts the message using Key K1 to produce Cipher C=E(K1[m])
- It is now followed by one-way keyed Hash function over message 'm' with Key K2 to produce 'r' where r = KH(m).
- Now the sum of PR_a and 'r' is calculated and a modulo is performed over the sum with value 'q' where 'q' is the prime factor of (p-1) to produce 'result' which is then divided by the random value 'x' which produces a value 's'

Now, three different values have been produced that are c, r and s. The source node can now encrypt these three values using Advanced Encryption Standard using Sk_{ab} and transmit them to the destination node.

B. Unsyncrption at destination

After the signcryption at the source is completed the destination node now possess c, r and s. using these values the destination now decrypts the message.

- After receiving the values c, r and s the destination node now decrypts the message to obtain the original message.
- The destination receives three values that are c, r and s. The destination now uses r, s, PUa, PRb, p and g to compute a hash to produce 128bit result where 'g' is an integer with the order q modulo p chosen randomly from (1,….p-1).
- The Hash function then produces Key K = H ((PUa * gr)s X PRb mod p). This Hash function now produces a key of 128bits. This 128 bit key is now divided into two halves to produce two 64 bit key and these are identical to the keys that are generated during Signcryption process by source node.
- Destination node now uses Key K1 to decrypt Cipher 'c' to get the original message m = D(K1[c]).

TABLE I. NOTATIONS USED DURING THE SIGNCRYPTION AND UNSIGNCRYPTION PROCESS

Symbol	*Process*
REQUEST	Request from source node
RPLY	Reply from CS to source node
SEND	Send key from CS to
DSPLY	Display message
E (…)	Encryption of Message
D (…)	Decryption of Message
PU_a	Public key for source node 'a'
PR_a	Private Key for source node 'a'
PU_b	Public Key for destination node 'b'
PR_b	Private Key for destination node 'b'
SKN	Shared Key between Source node 'a' and Destination node 'b'.
SKC	Shared key between source node 'a' and CS
LID	Location ID
VID	Vehicle Identity
T	Time

ACKNOWLEDGMENT

I owe a great many thanks to a great many people who helped and supported me during the writing of this paper. My deepest thanks to Lecturer, **Vijayan R** the Guide and author of this paper for guiding and correcting various documents of mine with attention and care. He has taken pain to go through the paper and make necessary correction as and when needed.

REFERENCES

[1] Yuliang Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption)<<Cost(Signature) + Cost(Encryption)" 1997 in CRYPTO '97 Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology

[2] Dr. iur.Lutz Gollan, Prof. Dr. sc. Christoph Meinel "Digital Signature in Automobiles" 2002 in Systemics, Cybernetics and Informatics (SCI)

[3] Arijit Khan, Shatrugna Sadhu, and Muralikrishna Yeleswarapu, "A comparative analysis of DSRC and 802.11 over Vehicular Ad hoc Networks" http://www.cs.ucsb.edu/~arijitkhan/cs276.pdf

[4] J.T. Isaac1 S. Zeadally J.S. Ca´mara, "Security attacks and solutions for vehicular ad hoc networks" 2010 in IEEE-Communications IET ,Volume 4 issue 7, 1751-8628

[5] Maxim Raya and Jean-Pierre Hubaux,"Securing vehicular ad hoc networks" 2005 3rd ACM workshop on Security of ad hoc and sensor networks (SASN)

[6] Jason Chao, Yong-qi Chen, Wu Chen, Xiaoli Ding, **Zhilin Li**, Nganying Wong and Meng Yu**, 2001.** An Experimental Investigation into the Performance of GPS-based Vehicle Positioning in Very Dense Urban Areas, Journal of Geospatial Engineering, 3(1): 59._-66.

[7] Journal, I., Science, A. C., & Hod, M. (2011). A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 2(3), 7-12.

[8] Suri, P. K. (2011). A Novel Approach to Implement Fixed to Mobile Convergence in Mobile Adhoc Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 2(1).

[9] Suri, P. K. (2011). Simulation of Packet Telephony in Mobile Adhoc Networks Using Network Simulator. International Journal of Advanced Computer Science and Applications - IJACSA, 2(1), 87-92.

[10] Indukuri, R. K. R. (2011). Dominating Sets and Spanning Tree based Clustering Algorithms for Mobile Ad hoc Networks. International Journal of Advanced Computer Science and Applications - IJACSA, 2(2).

AUTHORS PROFILE

Prof. Vijayan R: An Assistant Professor (senior) at SITE, VIT University, Vellore, India is a Research scholar and currently pursuing his research work on network and Information security systems. He has published number of papers in various different journals and presented number of papers in International conference.

Mr.Sumitkumar Singh is currently pursuing his Master of Technology in Information Technology Specializing in Networking from SITE, VIT University, Vellore, India. His current research work involves security over Vehicular Ad Hoc Network. Sumitkumar has published number of papers and presented papers in different conferences.