Enhanced Security for Information Flow in VANET using Signcryption and Trust level

Sumitkumar Singh
Master of Technology in
Information Technology
School of Information Technology
and Engineering,
VIT University, Vellore-632014
India

Vijayan R
Assistant Professor (Senior),
School of Information Technology
and Engineering
VIT University, Vellore 632014
India

ABSTRACT
Security in Vehicular ad hoc network has always been a major research area. Reducing cost of computation, effective consumption of limited resources and providing uncompromised security has always been a challenge over VANET. Two levels of security have been proposed based on Signcryption and node trust. Using Signcryption the computation cost is reduced as compared to Sign-then-encryption and also the confidentially and integrity of the message is conserved. By assigning trust levels to every node the malicious nodes or misbehaving nodes are removed from the network. Providing Confidentiality, Integrity of the message, detecting and removing malicious and misbehaving nodes from VANET are the main focus of this paper.

General Terms
Confidentiality, Integrity, Misbehaving node, Trust Threshold value, Public Key, Private Key, Shared Key.

Keywords
Signcryption, Trust level, VANET Server, Single Transmission mode, Broadcast Transmission mode

1. INTRODUCTION
Vehicular ad hoc network are highly dynamic in nature and suffers from frequent path breakage due to the high velocity of the moving vehicle. Therefore providing security for such a high volatile network has always been a challenge for the researchers. The network has to be secured and mean while the current transmission should not be affected. Dedicated short Range Communication (DSRC) [5] will be used in this system. The detailed advantage of using DSRC over IEEE 802.11p has been given in [5]. To identify the location of the vehicle the Global positioning system [6] will be used. The GPS systems can be used effectively to determine the location of the vehicle as describe in [6]. Digital signature has been used in automobiles [1] which suggest preserving public and private key and using private key for signing the message. The drawback of this [1] technique is that the computation cost required is high and is not suitable if it is to be implemented over VANET. The security algorithm which is to be implemented in VANET should provide less computational cost, and should utilize limited resource effectively. Signature-then-encryption is the better public key encryption technique to achieve confidentiality and integrity of the message in transmission but when it is implemented over VANET it cannot be the efficient way to provide security due to its drawbacks. Therefore a technique which can be suitable for VANET and eliminate all the drawbacks arising from signature-then-encryption technique should be used. Signcryption proposed by *ZENGH* [2] provides an incomparable security technique which can be used over VANET. This technique provides authentication and confidentiality in one logical step hence reducing the computation cost by a great margin as compared to signature-then-encryption technique. Providing Confidentiality and integrity are not only the major challenges in VANET, Identifying malicious node and preserving privacy are also one of the major aspects of the VANET. This paper therefore has proposed a trust based model which can be used to identify misbehaving and malicious node thus providing with two levels of security in a single system. The initial transmission requires the sender to identify the destination node through on board unit (OBU) global positioning system by its unique serial number given to it during its registration. The request to send is passed to road side unit (RSU) and from RSU to VANET server which processes the request and generates public and private key through random number generator for sender and receiver and transmits them to source and destination. Before generating the Keys, the trust level of the source node is evaluated. If and only if the given trust level condition is satisfied, which is to be explained in proceeding section, the node is allowed to transmit. The same is the case with the node at the receiving end. This adds on to an additional level of security in the network. In this paper, the Roadside unit acts as an access point between nodes and VANET server and also exchange information amongst RSU's. The details of this process will be explained in further section. After getting the keys the source computes Signcryption over message using the key and transmits it to the destination, Where the destination unsigncrypt the message and verifies the authenticity of the message. The detailed processes are described in later section. Section 2 describes about the proposed network model Entities, Section 3 describes about the assumption that has been made, Section 4 describes about the basic idea for implementation, Section 5 describes the process of assigning trust values to node, Section 6 describes about the mode of transmission which are selected by the node. Section 7 gives the conclusion.

2. PROPOSED NETWORK MODEL AND ENTITIES
The proposed network model as in Fig: 1. consists of VANET server, Roadside Unit and nodes model. All the entities present within the model contribute equally in the network. The in detailed functions of the present entities in our model will be explained in the proceeding sections. Following are the entities used in our proposed network model along with their basic functions.

2.1 VANET Server

VANET servers are responsible for evaluating, maintaining and storing the records of the registered vehicles in its database. These records include old ID's to new ID's issued, the trust level of a vehicle. ID will be used to verify the authenticity of the source and destination node whereas the trust level will determine whether the node is allowed to receive or transmit message within the network.

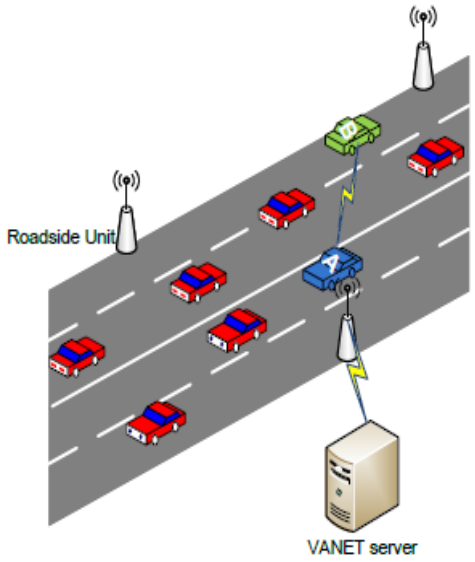

Fig 1: Represents Network Model. Node labeled as 'A' is the Source node and Node labeled as 'B' is the destination node. The nodes poses values like Ser_{no}: 809932UNLHxxxxx.,Loc_{des}: 12.936568,79.159638. Using these values the source node can detect the destination node and send request message to VANET server for transmission to particular destination node

2.2 Roadside Unit

The Roadside unit (RSU) acts as an access point between source node and VANET server and between VANET server and Destination node. The RSU in our system is not responsible for issuing key but are responsible for sending them to appropriate node. The RSU relay keys to neighboring RSU in the case when the transmitting node goes out of range of the current RSU.

2.3 Onboard Unit

Onboard unit (OBU) will use Global positioning system to track the vehicles based on their unique serial numbers. Only those vehicles will be allowed to track other vehicle who poses trust level more than '1'.

2.4 Source Node

The source node will initiate the transmission. The source node will be allowed to operate on Single mode or Broadcast mode of transmission by the VANET server based upon its trust level. To operate on Single mode the source node should have minimum trust level '1' and to operate on Broadcast mode the source node should have the minimum of trust level as '2'.

2.5 Destination Node

The destination node acts as the receiver. After receiving the message the destination node is required to provide a feedback depending upon the accuracy and reliability of the message to the VANET server. Based on the feedback received, the trust level of the source node will be increased or decreased by the VANET server.

3. DISCUSSION

- The VANET server is a trusted entity by all nodes participating in the network.
- The shared key used between nodes and VANET server cannot be compromised in any conditions.
- The public and private keys sent from VANET server to nodes are through secure channel and cannot be compromised by any means.
- The trust value assigned by the destination node is appropriate**.**

4. BASIC IDEA

VANET suffers from different type of attacks [3] and probably more than Mobile ad hoc networks due to their highly dynamic and volatile nature. The systems that are designed to provide security in VANET should be efficient and at the same time the computation cost for computing messages should be less. The proposed VANET system requires that, every node before entering into the network should be registered to the VANET server. The registered node will then be identified by its serial number. The serial number will be used only for identification and will not be used in data transmission. After registration, the VANET server will provide a unique ID to the node which will be used for the first transmission. For every new transmission the ID of the node will be changed hence making it difficult for the attacker to identify the sending node even if the old ID of the node is compromised hence providing message privacy [4]. Once the Transmitting node ID is found to be valid, the trust level of the node is evaluated, and only if both the conditions are satisfied, only then the Public key (PU) and Private Key (PK) for source node and destination node are created. In order to provide a fast and reliable encryption and signature technique; we have used Signcryption [2] which can be proved as an ideal technique in VANET. Advanced Encryption standard using 128 bit key has been used in the later stage of the Signcryption to provide encryption of the message. The detailed explanation of this process is given in proceeding sections. The contingency of an authorized node becoming a malicious node has always been a major problem in an ad hoc network. In order to circumvent such issues we have provided with a very efficient way to mark the trust level of every node that transmits within the network. This trust level is provided by the destination itself for the source from which it received the message and transmits it to the VANET server. The trust level is then stored in the VANET server database. The detailed explanation of assigning trust will be explained in Section 5. The basic idea of our system requires that the source operate in one of the two modes i.e. single mode or broadcast mode. The detailed explanations of these two modes are given in Section 6.

5. ASSIGNING TRUST LEVEL

In order to remove malicious or compromised nodes from the system we have provided with a very effective and efficient method. The trust based system is proposed which will be helpful in identifying misbehaving node within the system. In our system, after the transmission between the source and the

destination is over the destination node evaluates the message and assigns a specific feedback value that is trust value in this case for the source and sends it to the VANET server. The maximum trust value that a node can preserve is '5' and the minimum is '1'. The nodes having trust level '5' will be regarded as the most trusted node in the system whereas nodes with less than '1' trust value will be regarded as least trusted node. The node having the trust value below '1' will be removed from the network by blocking every transmission through them and to them. Only should the VANET server receive the trust level for a particular node from three different vehicles the trust values of the node can be increased or decreased. By allowing three different vehicles to assign a trust value to a node which causes the increase or decrease in the trust value of the node, allows that particular node to operate in the network for fair amount of time. In our system there are two scenarios where the node can be discarded from the network.

5.1 Scenario 1

When the trust level of the node is below '1' the node will debarred from the network, hence blocking all transmission from it and to it. E.g. If the trust value received from two vehicles are negative whereas one vehicle gives a positive trust value, the trust value of the node remains unchanged. Similarly, if four vehicles provide a negative value for a source, then only trust value of '1' will be decrease for the source node not '2', had it been six then of course it will be decreased by '2'.

5.2 Scenario 2

Whenever the trust value is decreased, the number of times it has been decreased is stored by the VANET server. If the trust value has been decreased for '5' times; the node will be termed as an inappropriate node and will be debarred from the network this means that a node has been marked as an inappropriate node by '15' (3x5) different nodes.

6. MODE OF TRANSMISSION

The nodes having trust level between '2' and '5' will be allowed to operate on Single and Broadcast mode whereas nodes having trust level as '1' will be allowed to operate on single mode and will be discontinued to operate on broadcast mode. By providing such kind of provision, even if the node has become malicious it will not affect the entire network since it has been disallowed from broadcasting message. The detailed explanation has been provided in below section.

6.1 Single Transmission Mode

The single transmission mode as in fig 2 represents a single mode transmission between source and destination .An ideal source node in VANET first checks for the location of destination and then its range to destination to transmit system, the previous ID (ID_{old}) and the location of the destination (LC_d). This whole packet is encrypted by the shared key e.g. Sk_{av} where 'a' is the source node and 'v'

message. In our system the source can track the location of the destination node using the unique serial number through the onboard GPS unit. In single mode of operation the source node request for public key and private key and is generated randomly by the VANET server. The packets that are sent from the source node to the VANET server through RSU contain the single mode bit (SM bit) which is '1' in this

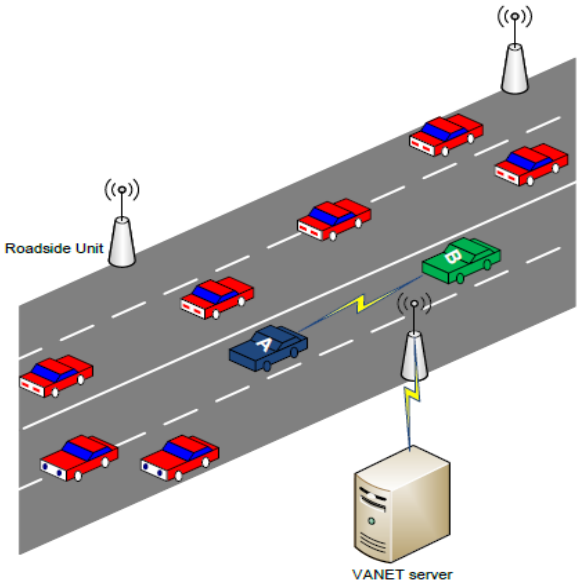

Fig 2: Represents Single mode transmission. Source node is Labeled as 'A' and Destination node is Labeled as 'B'. Node 'A' and Node 'B' receive keys from VANET server which are then used for Signcryption process.

represents VANET server. On receiving the request from the source node for the transmission to the desired destination the VANET server first checks the ID of the source node. If the ID is forged the node is immediately removed from the network. If the ID is found to be valid the trust level of the source node is then evaluated. The node is only allowed to transmit if the trust level is between '1' to '5' else it is discarded by the VANET server. After ID and trust level is found to be valid and satisfactory only then a new ID_{new} is assigned to source node and the ID_{old} is stored in VANET server database. By generating new ID's for every new session the privacy [4] of transmission is maintained. E.g. Even if the attacker has somehow got an access to the ID_{old} he

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

Algorithm 1:

1. $E(Sk_{av}[RQST(SM,ID_{old},Loc_{des},Ser_{no})])$ from source node 'a'
2. $Search(ID_{old==}ID_{old})$
3. **IF** found (ID_{old}==ID_{old}) **Then {**
4. **IF** (TL != 0) **Then** {
5. Generate ID_{new}
6. Generate PU_a,PR_a, PU_b, PR_b
7. $E(Sk_{av}[RPLY(ID_{new},PU_a,PR_a,SK_{ab})])$ to Source node
8. $E(Sk_{bv}[SEND(ID_{new},PU_b,PR_b,SK_{ab})])$ to Destination node
9. **}** **Else** DSPLY("Transmission Cannot be Granted")
10. **}** **Else** (Remove Source node from the network)

still cannot use it by any means since the ID_{new} has been generated and will be used in new session. The VANET server generates Public key and private key pairs for Source node and destination node , ID_{new} and Shared key SK_{ab} 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 VANET server are sent to source and destination by encrypting it with their respective secret key. A situation may arise where the current transmission may fail due path breakage, which if often seen in VANET. In such cases the source node can send a path break message to VANET server using ID_{new} as the parameter. On receiving this message the VANET server evaluates the time stamp when the ID_{new} was created and based on that either a new ID and keys are generated or same key and same ID are sent through the current RSU within the range of source and destination. However, Handoffs has been kept as the future scope and more emphasis will be given on providing security. The Algorithm 1 describes about the process at VANET server when it receives a message request for a particular destination. The Notations used during a message transmission are shown in TABLE – I

6.1.1 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. Following steps for Signcryption are carried out as described in [2] by the source node. The Signcryption process is then followed by the process of Unsigncryption as described in [2].

- 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.

6.1.2 Unsigncryption at Destination:

After receiving the message from source the destination now has to unsigncrypt to obtain the original message from the source. The following steps are performed at the destination side.

- The destination receives three values that are c, r and s. The destination now uses r, s, PU_a, PR_b, 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 (($PU_a * g^r)^s * PR_b$ mod p).

TABLE 1.

Notations used during the Signcryption and Unsigncryption Process

Symbol	Process
RQST	Request from source node
RPLY	Reply from VANET server
SEND	Send key from VANET server to destination
DSPLY	Display message
E (…)	Encryption of Message
D (…)	Decryption of Message
TL	Trust Level
SM	Single mode
BM	Broadcast mode
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'
Sk_{ab}	Shared Key between Source node 'a' and Destination node 'b'.
Sk_{av}	Shared key between source node 'a' and VANET server
Sk_{bv}	Shared key between source node 'b' and VANET server
Sk_{br}	Shared key between all nodes in broadcast mode of operation
ID_{old}	Previously issued Identification number to particular node
ID_{new}	Identification number issued for current session to node
Loc_{des}	Location of destination node
Ser_{no}	Serial number of the destination node

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]).

The message received by the destination node also contains the new ID of the source node. Based on the accuracy and reliability of the message the destination node sends the trust value for the source to the VANET server.

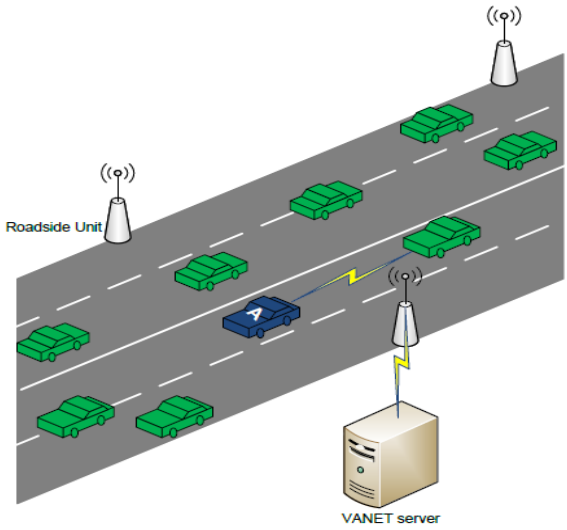

Fig 3: Represents Broadcast mode transmission. The node labeled as 'A' is the Source node whereas reset of the nodes are the destination nodes.

6.2 Broadcast Transmission Mode

The broadcast mode as in Fig: 3 are selected by the Source node when it needs to broadcast the message to the entire zone or region. In order to limit the computation cost a single pair of private key and public key are generated and distributed across the region. Again, here the trust level will be checked and only those nodes having trust level more than '1' will be permitted to broadcast. As described in the algorithm 1, the parameter within the request message doesn't contain parameters like location of the destination, the serial number of the destination as used in the single mode. In broadcast mode the message is transmitted to all the nodes present within the coverage area of the current RSU. If the source node happens to moves away from the coverage range of the current RSU, the source node can send a path breakage message to VANET server and VANET server will evaluate the ID of the source. Based on the ID, the VANET server will determine the Timestamp and the type of message that was created for that ID. Accordingly, the ID and Keys would be generated or same ID and keys will be distributed. The Algorithm 2 provides the evaluation process at VANET server when a request for broadcast message is received from the source. Handoff in this paper has been taken as the future scope. After receiving the keys the source node follows the same Signcryption process as was in Single mode transmission. The only difference is that the source node will now use Sk_{br} that the common shared key to encrypt the message and transmit it throughout the region. The decryption process followed at the destination node is the same as done in the single mode transmission.

Algorithm for Evaluating Message at VANET Server sent by Source Node in Broadcast mode of Transmission :

Algorithm 2:

1. Receive $E(Sk_{av}[RQST(BM,ID_{old})])$ from source node 'a'
2. Search($ID_{old==}ID_{old}$)
3. **IF** found ($ID_{old}==ID_{old}$) **Then {**
4. **IF** (TL != 0) **Then** {
5. Generate ID_{new}
6. Generate PU_a,PR_a, PU_b,Sk_{br}
7. $E(Sk_{av}[RPLY(PU_a,PR_a,Sk_{br})])$ to Source node
8. $E(Sk_{bv}[SEND(PU_{a,}Sk_{br})])$ to all nodes within region
9. **}** **Else** DSPLY("Transmission Cannot be Granted")
10. **}** **Else** (Remove Source node from the network)

7. CONCLUSION

The system model that we have proposed can be used as an ideal system to be implemented over VANET based on central authority which was VANET server in our system. Infrastructure based system always posses an added advantage over self organizing network where frequent path breakage during transmission is the major problem. Our system should provide better efficiency, low computation cost as compared to signature then encryption process and at the same time prevent path breaking by allowing the RSU to forward keys to neighbouring RSU. The future work of our paper would be to enhance the handoffs and provide an effective and efficient model which can provide two levels of security and can transmit message to the required destination even if the current message transmission has suffered loss due to path breakage. Also the trust model needs to be improved by making it more stringent. We need to consider situation where the trust provided by the first destination node is valid or not and at the same time to enhance the security level up to great extent.

8. REFERENCE

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

[2] 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

[3] 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

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

[5] 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

[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.