ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Approach for Providing Security in Vehicular Adhoc Network Through Vehicles Present in the Network

Vijayan.R
Assistant Professor (senior grade)
School of Information Technology and Engineering
VIT University, Vellore, India
vijayan_ram@yahoo.com

Sumitkumar Singh*
Master of Technology
School of Information Technology and Engineering
VIT University, Vellore, India
research.sumit@yahoo.com

Abstract: Infrastructure based Vehicular ad hoc network has indeed increased the efficiency and accuracy of the network but at the same time it has also increased the cost required for the setup of such network. Therefore there exist needs wherein the nodes within the network itself provide security features hence eliminating the need for setting up of an expensive network. In this paper we have proposed a novel approach wherein the nodes itself can act as a central authority which will provide requesting nodes with public and private key. To improve the performance and at the same time to enhance the security and to provide confidentiality and integrity we have proposed the use of Signcryption [1, 2]. In order to take the performance of the network to next level we have proposed the use of improved Signcryption [2]. Providing improved Signcryption through nodes present within the network are the main focus of this paper.

Keywords: Signcryption, Current Coverage Area (CCA), CA node, Single hop Transmission, Multi hop transmission

I. INTRODUCTION

Security in Vehicular ad hoc network has always been the major research area. Infrastructure based network has indeed helped in increasing the security levels in VANET but meanwhile it has also led to some major drawbacks which include the cost involved for the setup of such network. Setting up of an infrastructure based network requires the services of Roadside units which act as an access point in the network. [4] Describes the usage of RSU and has been termed as Service Units (SU). These RSU can act as an access point or certificate granting authority or may be programmed for other relevant usage. These RSU are connected to a server which provides relevant features to the nodes present within the network. Such network becomes a very effective network but it increases the overall deploying cost. Therefore to reduce such drawbacks of the system a novel approach has been proposed wherein the security features will be provided by the node itself present within the system. Such nodes are considered as the trusted nodes which can be a government vehicle e.g. police vehicle, Government ambulance or vehicles assigned by the service providers .VANET suffers from many limitations which include availability of limited resource, frequent path breakage due to its dynamic nature. In such network it is required that the computation cost involved in the system should be less. In order to achieve such goals we have proposed the use of Signcryption [1]. Signcryption combines Digital signature and Encryption in logically single step unlike Digital signature than encryption which requires more machine cycle for processing than Signcryption. [3] Describes an approach wherein digital signatures are used in automobiles. The proposed model in [3] is effective but suffers from additional computational cost. A more enhanced feature has been proposed in [2] which have modified Signcryption to make it easier for computation. This paper has proposed the use of such [2] model which would help decreasing the computation cost and increase the performance level of VANET.

II. NETWORK MODEL

A. *CA Node*

Central authority (CA) nodes are responsible for assigning public and private keys to the requesting nodes in the network. These nodes are assigned by the service provider based on their type i.e. a CA node can be a government vehicle like police cars, ambulance or some private vehicle designated by the service provider itself. The fig 1. Shows a typical network model proposed in this paper.

B. *Source Nodes*

These are the nodes which requests available CA node for transmission with the destination node.

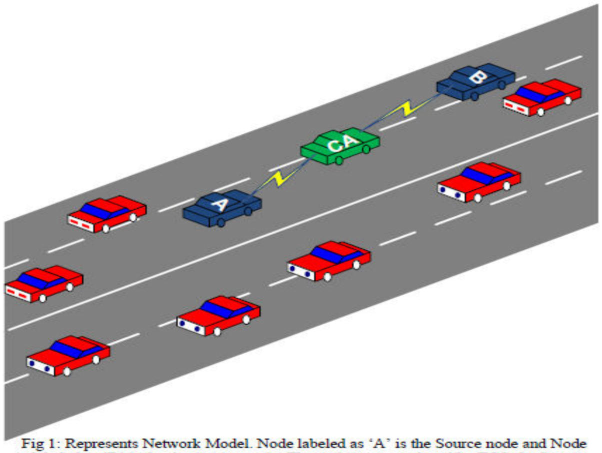

Fig 1: Represents Network Model. Node labeled as ‘A’ is the Source node and Node labeled as ‘B’ is the destination node. The nodes poses values like TOS: 2, Ser_{no}: 809932UNLHxxxxx. ,Loc_{des}: 12.936568,79.159638. The CA node is labeled as CA. It poses values like TOS: 1, Ser_{no}: 9384953UNLHxxxxx. ,Loc_{des}: 12.883568,79.133638. Source node and destination node are within the CCA of CA Node.

Figure: 1

C. *Destination Node*

These are nodes that receive messages from the source nodes.

III. ASSUMPTIONS

A. Source node and Destination node are present within the Current Coverage Area (CCA) of CA node.
B. The CA node is a trusted node by all the nodes within the network and cannot be compromised.
C. The current proposal is suitable for the use within the city perimeter whereas over higways it depends on above (A) condition.

IV. BASIC IDEA

The proposed model requires that every node participating in the network transmission should first register itself with the service provider. A unique serial number such as the chassis number of the vehicle or the number plate of the vehicle will be used to identify the vehicle. The serial number will used only during route updating process whereas for message transmission new ID will be used. A unique ID will be provided to such nodes which will be used during their first transmission. These ID will be changed for every new transmission Therefore even if the attacker has somehow gained access to the old ID it will still not be able to make out as to who the owner of the ID is and hence the privacy of the message is preserved. This paper proposes that the two nodes that are the Source node and destination node should be present within the current coverage area (CCA) of the CA node during the transmission. A proactive routing approach has been proposed. Every node in the network is required to send regular beacons which consists of its type which is displayed as ‘1’ in the route update message for the CA node whereas ‘2’ in the case of other nodes and its location. The serial numbers of the vehicles are also included within the route update message to identify the vehicle.

V. ROUTE DISCOVERY

A proactive routing approach has been used to update the routing information of the node present within the network as shown in fig 2. Every node in the network is required to maintain two different tables. One table is required to update the CA nodes position whereas the other is required to update neighboring nodes location. By using the routing information about the neighboring nodes neighbor, each node in the network can get a virtual picture of the network hence eliminating the usage of costly systems like the RSU, Server or GPS systems. Each node in the network is required to forward beacons at regular interval of ‘1sec’ which consist of its route updates along with the route updates of its neighboring nodes containing parameters like Type of node (TON), The ID of the node (ID), Serial number of the node (SER) and Location of the node (LOC). The TOS of the node describes the type of node. The ID and SERno is required by the CA node to verify the node. The location specifies the location of the node. The location can be obtained from the GPS system. . If the node who wishes to send a packet to a required destination, it will first check CA routing table for the available CA node. Depending upon the nearest located CA node the source selects the node and requests for transmission to destination node.

VI. MESSAGE TRANSMISSION

A source gets to know about the destinations location based on the updates received from the node. Consider node ‘A’ need to transmit message to node ‘B’ as shown in fig. The node A first checks its routing table and marks the destination node to which it needs to transmit message. It then checks for the latest arrived CA node in its CA routing table. After marking the CA node and respective destination the source sends a request message RQST (SER_{des}, LOC_{des}, ID_{old}) to CA node encrypting it with the shared key between CA node and Source node. On receiving this request the CA node decrypts the message and first checks whether the given parameters are valid. To do this the CA node first checks whether the given serial number matches the ID_{old} of the source node. If the ID_{old} is not the latest ID or found to be invalid, the node is removed from the network. Only if both the parameters are found to be valid, the source node is allowed to transmit. On receiving RQST from source node and finding the parameters to be valid, the source node now generates Public and Private Key for source and destination. The message also contains the randomly generated shared key that is to be used between source and destination for further transmission. These keys are encrypted using respective shared keys and sent to source and destination. The ID_{new} that are generated for source and destination are now sent to other CA within the network using multi hop technique explained in below section. This helps other CA to verify the nodes if the particular node has entered its CCA. After receiving the keys Signcryption is done over the message.

Algorithm used for evaluating the message at CA node

Algorithm 1:

```
A. E($Sk_{ac}$[RQST(TOS,,$ID_{old}$,$Loc_{des}$,$Ser_{no}$)]) from source node ‘a’ to CA node
B. Search($ID_{old==}ID_{old}$)
C. IF found ($ID_{old}$==$ID_{old}$) Then {
D.     Generate $ID_{new}$
E.     Generate $PU_a$,$PR_a$, $PU_b$, $PR_b$, $Sk_{ab}$
F.     E($Sk_{ca}$[RPLY($ID_{new}$,$PU_a$,$PR_a$,$SK_{ab}$)]) to Source node
G.     E($Sk_{cb}$[SEND($ID_{new}$,$PU_b$,$PR_b$,$SK_{ab}$)]) to Destination node
H.     E(Skcc[IDnew, SERno]) to other CA in network
I. } Else DSPLY(“Transmission Cannot be Granted”)
```

The algorithm 1 explains this process. The notations used in this paper are explained in TABLE 1. The detailed process of improved Signcryption will be explained in preceding section. After receiving the Signcrypted message the destination unsigncrypt the received message to get the original message.

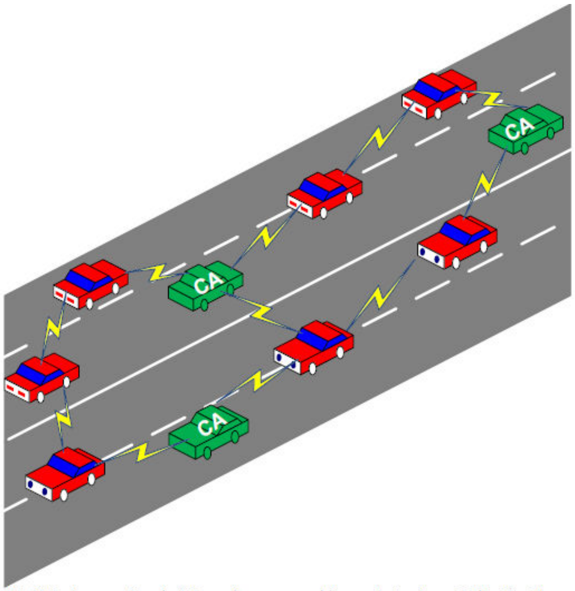

Fig 2:Exchange of route information amongst the node is shown in the fig. The node marked as CA are the CA nodes.

Figure: 2

The entire process of transmission has been categorized into two that is Single hop transmission and multi hop transmission. The details are provided in the below section.

VII. SINGLE HOP TRANSMISSION:

In single hop transmission it is required that all the node participating in message transmission that are source node, destination node and CA node remain in one hop distance from each other. A typical single hop scenario is shown in fig 3. After receiving the updates from the CA node and the destination node the source node check in the CA routing table selects the CA node. The further process is same as explained in section VI.

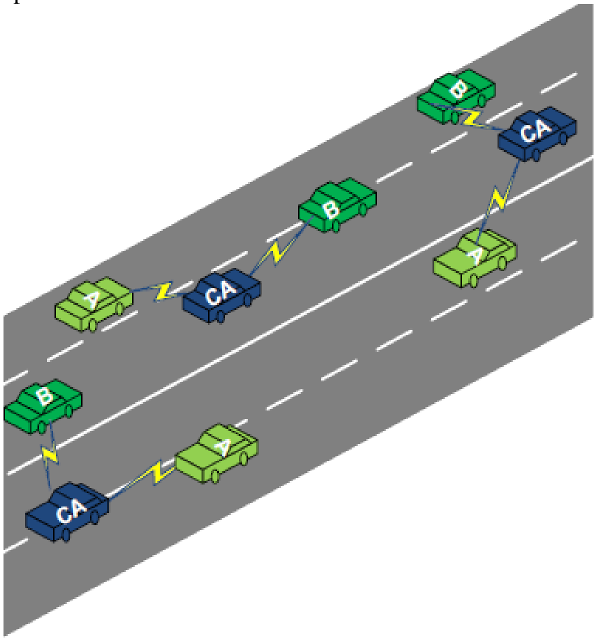

Fig 3: Shows a Single hop transmission mode. Here Source nodes are Labeled as 'A', The destination nodes are labeled as 'B' and the CA node are labeled as 'CA'. Every source node and destination node is one hop away from the CA node

Figure: 3

TABLE I: NOTATIONS USED DURING THE SIGNCRYPTION AND UNSIGNCRYPTION PROCESS

Symbol	Process
RQST	Request from source node
RPLY	Reply from CA node to source node
SEND	Send key from CA node to Destination node
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'
Sk_{ab}	Shared Key between Source node 'a' and Destination node 'b'.
Sk_{ca}	Shared key between source node 'a' and CA node
Sk_{cb}	Shared key between destination node 'b' and CA node
Sk_{cc}	Shared key between CA nodes
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 node

The algorithm explained in algorithm 1 applies for single hop transmission as well. After receiving the key, the source node Signcrypt the message.

An improved Signcryption proposed by [2] has been proposed in this paper. The following steps are carried out in this process.

A. *Signcryption:*

[a] Source node selects random value 'x' where x is in the range of (1,…,q-1)

[b] The source now selects PU_b and random value x to compute Hash function out of it. This creates a 128bit string. K = H (PUb mod p) where 'p' is a large prime number.

[c] The 128 bit key obtained is divided into two halves K1 and K2.

[d] Source now uses AES encryption technique and encrypts the message using Key K1 to produce Cipher C=E(K1[m])

[e] It is now followed by one-way keyed Hash function over message 'm' with Key K2 to produce 'r' where r = KH(m).

[f] 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'.

B. *Unsigncryption:*

[a] After receiving the values c, r and s the destination node now decrypts the message to obtain the original message.

[b] 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).

[c] The Hash function then produces Key K = H ((PU_a * g^r)^s X PR_b 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.

[d] Destination node now uses Key K1 to decrypt Cipher 'c' to get the original message m = D(K1[c]).

VIII.MULTI HOP TRANSMISSION

In multi hop transmission the node selects the destination node from the routing table and CA node from the CA routing table. If the destination node and CA node is not present within the CCA of the source node the source node forwards the message based on the routing table to the nodes between the source and the CA node, destination node. The fig 4 Shows a typical multi hop scenario.

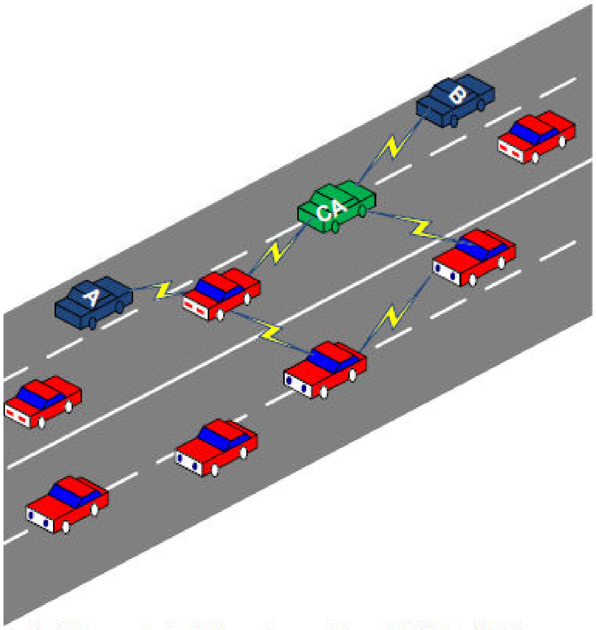

Fig 4:Shows a typical multi hop environment. The node labeled as 'A' is the source node, Destination is the node labeled as 'B' whereas CA node is the node labeled as 'CA'

Figure: 4

In this mode of transmission the CA node transmits keys encrypted with the shared key of the source node hence preserving confidentiality and integrity of the message. As explained in the above section the CA node transmits Public key, private key and shared key between source node and destination node. This shared key is then used between source and destination node to encrypt the message. Since the shared key is known only to Source and destination and hence the confidentiality and integrity of the message is maintained. The algorithm used in multi hop transmission is the same as explained in algorithm 1.

IX. CONCLUSION

In this paper the use of node which offers security features to other nodes within the network itself is explained. The use of costly equipments like the Road side units, Servers or Onboard GPS system have been avoided hence eliminating the additional cost required to setup such network. The future work in this paper involves more enhancements with respect to security features and adding up an additional security level by forming trust levels within the nodes participating in the network.

X. REFERENCES

[1] Yuliang Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption)<<Cost(Signature) + Cost(Encryption)".

[2] "A Signcryption Scheme with Signature Directly Verifiable by Public Key", Feng Bao and Robert H.Deng

[3] *Dr. iur.Lutz Gollan, Prof. Dr. sc. Christoph Meinel ,"Digital Signature in Automobiles",*

[4] "Data Aggregation and Roadside Unit Placement for a VANET Traffic Information System", Christian Lochert, Björn Scheuermann, Christian Wewetzer, Andreas Luebke, Martin Mauve