Improved Session Key based Certificate to Detect Sybil Attack in VANET

Ravi Prakash
PG Scholar, Computer Science and Engineering,
Galgotias University,
Greater Noida, U.P, India

Kamal Soni
PG Scholar, Computer Science and Engineering,
Galgotias University,
Greater Noida, U.P, India

***Abstract*- This paper is total explanation about the detection technique of Sybil attack in VANET. The paper uses the improved session key method that dynamically generates the local certificate for the vehicles to communicate within range of VANET server. In this scheme the session key is used to detect the ID of the vehicles so that they can be tracked easily and the attack could possibly avoid. This improved session key requires less number of arithmetic calculations so that the response time of the vehicles and the server is reduced. It provides privacy to the driver by using anonymous identity. It is reliable for the safety driving with reliable information.**

Keywords—session_key, VANET server, anonymous identity

INTRODUCTION

Today the wireless network has widely grown up and everyday the new technology is emerging, VANET is also an example of the new technology era. It is an ad-hoc network used by the vehicle's on the road. There are many application about this technology such and safety enhancement and traffic congession notification have been described earliar[1,2]. But still there are chance to improve the existing techniques. The VANET is vulnerable to many attack's like sybil attack, blackhole attack, DOS attack and so many more.

The sybil attack is one of the active attack for the VANET in which a driver creates multiple idintity for its own purpous. The sybil attacker uses its fake identity to misguide the other vehicles on road. The driver disobeys the basic assumptions of the VANET and does not support for the ideal behaviour of the network[3.4] .

In this paper we have used improvised session key to authenticate the different identity of the vehicles in the network. And this modification will provide more reliability to the network communication. Drivers can rely on the information provided by the other vehicles moving in the range. The information flowing in the network can be safely tranmitted within the range of communication.

RELATED WORK

A. *VANET AND ITS ARCHITECTURE*

In VANET there are usually two types of nodes that are On Board Units (OBU) and Road Side Units (RSU). The OBU's provides the hardware and the processing unit that provides the basic requirements for communication in ad-hoc architecture. There are sensors, storage and warning devices associated with this unit that are temper proof in nature. The second one is the equally important in behavior and that is the Road Side Units that provides the security messages and other traffic information for to the drivers on the road. The RSU's provides the information like parking lots, gas station and access of internet [4]. Vehicles can communicate with the RSU's and with the other vehicles too. This type of communication is called V-I and V-V communication.

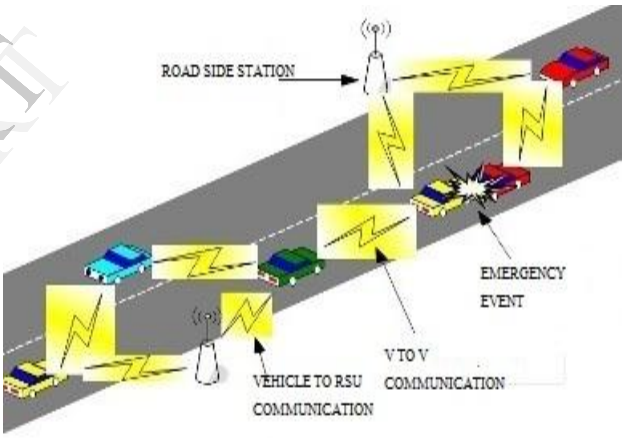

FIGURE1: COMMUNICATION IN VANET

The figure1 is a illustration of the VANET here the vehicles are equipped with the OBU's and with sensor devices and applications such as GPS that helps to find out the geographical position of the vehicle and sensors senses the speed, rotation and pressure of the vehicle on the road. There connectivity gateway is RSU's. The RSU's are connected with the VANET server that are called VANET main server in rest of the paper and the RSU's are called local VANET server. The main VANET server is govern by the legal persons or the legal authorities. That is much reliable in nature. The main server is having all the records about the vehicles identity and registration number in its own database. And it will help to authenticate the vehicles in the VANET. The RSUs are called local VANET server and it can directly communicate with the main VANET server to check whether a particular vehicle is having registered identity in the database of legal authority or not. Vehicles moving on the road are capable of sharing information within their own region and simultaneously the collect the other information like traffic condition, accident event, roadblock and more. They can forward these information to their neighbor vehicle so that the other vehicles can avoid such problems and could choose an alternate path to their destination. This type of communication is called V-V communication. For this security purpose the communication protocols must be satisfy the authentication, information integration, conditional anonymity of messages[5].

B. *SYBIL ATTACK*

In VANET there are many security threats that cause the serious danger to the safety of the vehicles. The Sybil attack is one of the active attacks for the vehicles. Here the malicious node disguise itself by using different identity and sends wrong messages to the neighbor vehicles in its communication range for its own benefits. The basic goal is to make other vehicles change their route for the personal benefit of the malicious node. Sometimes it causes serious danger to the life of other drivers of the network.

In this paper the improvement in the session key makes it possible for the other drivers to rely on the messages coming from the other vehicles of the same network. It also provides warning messages that detects the suspicious nodes in the network.

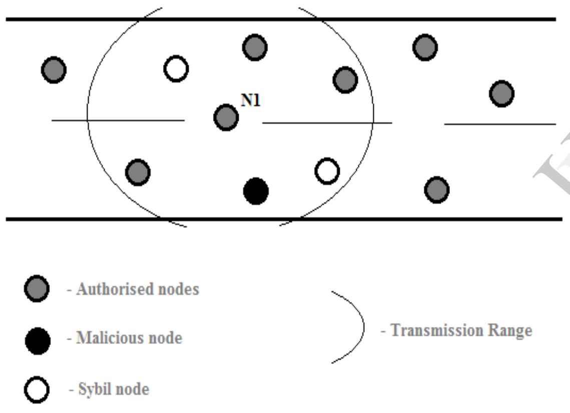

Fig2: Sybil node in the network

As illustrated in the figure2 the Sybil node can cause serious threat to the network this may give illusion of the traffic congestion, they can broadcast the false data into network that will impact the data consistency in the network [6]. The Sybil node can claim to be at different location at the same time to produce problem in geographical routing [7]. And the improved scheme will have following steps.

C. DESIGN OF SCHEME

The proposed design assumes that all the nodes having a master key, hash function, ECC, AES and a unique identity called UID [8]. This proposed method has following steps in its design that are listed below and having almost the same protocol against Sybil attack on VANET [9].

First the vehicle's UID is and its Master Key is registered in the main VANET server.

Second vehicle A will generate anonymous identity and send it to local VANET server to which vehicle A belongs to.

Third the local VANET server will validate the anonymous identity of the vehicle A in the main VANET server.

Fourth the local VANET server will generate a session key and local certificate for the vehicle A and will store this in its database then send this local certificate to the vehicle A.

Fifth, vehicle A will use this local certificate, road number, message and the message hash value to the other vehicle B.

Sixth, the vehicle B will check the local certificate of vehicle A by requesting the local certificate of vehicle A to a local VANET server and if it is found mismatched then it is assumed that a Sybil node has attacked on vehicle B and it is using vehicle A's identity.

Seventh, if the identity is validated then vehicle B will go for the message integrity checking and then read the message.

Eighth, vehicle B will check the validation of road number provided by the vehicle A and vehicle B will check that the sender vehicle A is having the same road number on which vehicle B is moving. The road number is always chosen in the direction where the front light of the vehicle is.

D. GENERATION OF SESSION KEY BASED CERTIFICAT

The improved session key based certificate generation procedure is explained below as in this method we are using each vehicle's unique identity (UID), session expiration time (T), a master key(MasterKey) and two keys that are private key and public key. The complete procedure will complete in four steps. Let us explain the complete procedure of generation of local certificate of any vehicle A.

1. *Authentication*

First, the vehicle which wants to broadcast any traffic information like roadblock or any accident event must concatenates its master key (Master Key) with its identity (ID) and will generate its own commitment identity (CID) [8] by using a hash function.

$$\mathrm{CID_A{=}HASH(MasterKey_{\,A} \,||\, Identity_{\,A})}$$

Second, the local VANET server will authenticate vehicle's CID with the VANET main server. If the CID is found in the main server database as a registered user then proceed to the next step otherwise access is denied. And session creation process is closed and all request from that vehicle is rejected.

2. *Session creation*

Now the third step, after the successful authentication of vehicle identity the vehicle will generate a public key based upon its own private key using an ECC algorithm as given below.

$$\mathbf{PublicKey}_{(A)}\mathbf{=PrivateKey}_{(A)}\mathbf{X\ P\ mod\ N}$$

This public key is send to the local VANET server and the local server will now generate its own public key using the same algorithm as

$$\mathbf{PublicKey}_{(LVANET)}\mathbf{=PrivateKey}_{(LVANET)}\mathbf{\ X\ P\ mod\ N}$$

After this the local VANET server XORs the both public keys then it will hash the certification expire date (T) with local certificate of local VANET server and the private key of local server after concatenating all these. Now this value is called the Hash Value for local VANET server.

$$\mathbf{HashValue}_{(LVANET)}\mathbf{= HASH(LCert}_{(LVANET)}\ \mathbf{||T||PrivateKey}_{(LVANET)}\ \mathbf{)}$$

Now the local server would generate the local certificate based on session key by multiplying the session key with the hash value and then adding the certificate of local server to the result.

$$\mathbf{LCert_A= [\ (SessionKey\ x\ HashValue}_{(LVANET)}\mathbf{)\ +\ LCert}_{(LVANET)}\mathbf{]\ mod\ N}$$

This local certificate is send to the vehicle A as its legal proof through which any other vehicle can validate whether the information sender vehicle is reliable or not. After sending this certificate the local VANET server will save the commitment identity, expiration date and the issued certificate in its database for future use. And this certificate is valid till the expiration time (T) after this the certificate is no longer in use.

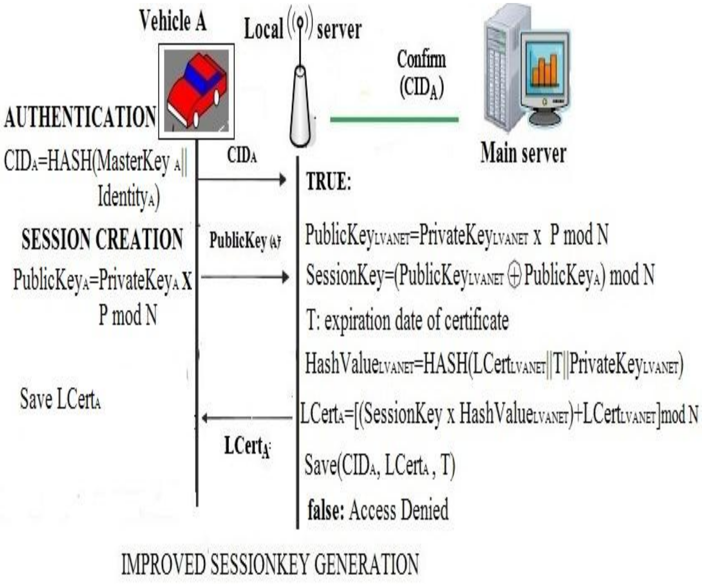
Vehicle A
Local server
Confirm
(CID$_A$)
Main server
AUTHENTICATION
CID$_A$=HASH(MasterKey $_A$|| Identity$_A$)
CID$_A$
TRUE:
SESSION CREATION
PublicKey$_{(A)}$
PublicKey$_A$=PrivateKey$_A$ X P mod N
PublicKey$_{LVANET}$=PrivateKey$_{LVANET}$ x P mod N
SessionKey=(PublicKey$_{LVANET}$ ⊕ PublicKey$_A$) mod N
T: expiration date of certificate
HashValue$_{LVANET}$=HASH(LCert$_{LVANET}$||T||PrivateKey$_{LVANET}$)
Save LCert$_A$
LCert$_A$=[(SessionKey x HashValue$_{LVANET}$)+LCert$_{LVANET}$]mod N
LCert$_A$
Save(CID$_A$, LCert$_A$, T)
false: Access Denied
IMPROVED SESSIONKEY GENERATION

Fig3: Detail view of Authentication and session creation

Figure 3 shows the detail view of above two procedure authentication and session creation. Both the step is visually described in this figure.

3. *Validation*

In this step of the proposed scheme we are going to explain the validation process of vehicle A by the vehicle B. At the start of communication after the successful authentication process vehicle A will send the commitment identity and the local certificate to the vehicle B now vehicle B which receive such message will concatenate the local certificate and the commitment identity and then simply send it to the local VANET server now the local server will check for the validation of commitment identity of vehicle A from the MAIN VANET server and if such commitment identity is found in the database then the main server will acknowledge the local server. After this successful acknowledgement the local server will find the commitment identity in its own database called DB then checks the expiration time of certificate and get the local certificate of vehicle A associated with the commitment identity and temporarily saves it and compare this certificate of vehicle A with the local certificate of vehicle A send by vehicle B and if all goes well then local server will acknowledge the vehicle B and now vehicle B can rely on vehicle A as a trustworthy node. Now vehicle A can send the security messages to vehicle B after then the message processing step will take place.

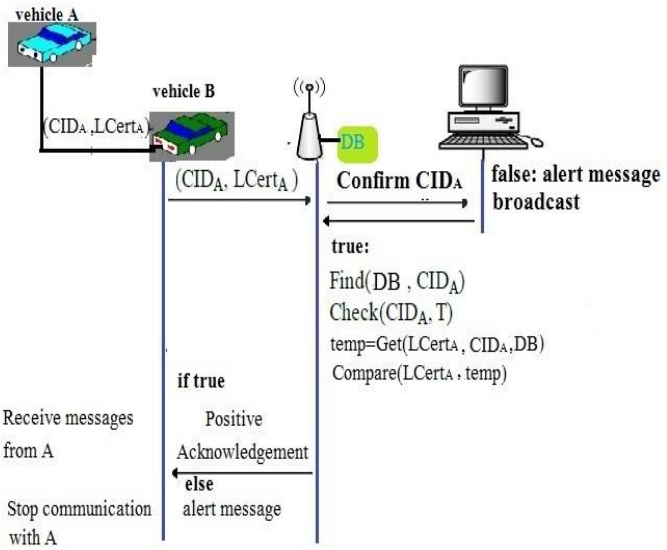

Fig4: Detail view of validation process

Figure 4 is a visualization of validation process in which detail view is shown.

4. *Message processing*

The third step involve into this scheme is message validation as this paper deals with reliability and much attention towards to the safety of the drivers, so the message sent by vehicle A should be validate at the receiver end that is another driver B. the driver B will check the message tempering at its own end. The method for validation of received message is done by comparing the original message with hash message at the vehicle B's end.

Vehicle A will concatenate the message and its own commitment identity and then hashes it [8].

$$HM_A = \mathrm{HASH}\ (Message \mid\mid CID_A)$$

It will now simply send the message packet which consist commitment identity, hash value and the message to vehicle B.

$$\text{Message Packet}\ (CID_A,\ HM_A,\ Message)$$

Now the vehicle B will hash the message with the received commitment id at its own end and calculate the HM_B after this it will compare HM_B with HM_A if both found equal then it is assumed that there is no tempering with the original message.

E. CONCLUSION AND FUTURE WORK

This improvised scheme provides very much support to the safety and reliability to the drivers. The privacy and the reliability is our main objective same time this scheme provides increment in response time in comparison to the earlier DTSA mechanism [8] because it requires less number of calculations at the sender's end. The generation of session key is all at local server's end and this certificate is simply delivering to the sender vehicle. It is not worth to calculate the same certificate at the sender's end so finally it will increase the response from the sender's end. And for the future work we are going to implement this whole scenario on network simulator and will be comparing our improved scheme with the previous scheme. So finally the reduction in response time and improvement in performance of the vehicles can be assured.

REFERENCES

[1] I.-H Bae, "Design and Evaluaiton of a Hybrid Intelligent Broadcast Algorithm for Alert Message Dissemination in VANETs", Int'l Journal of Grid and Distributed Computing, vol. 4, no. 4, (2011), pp. 1-10.

[2] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad and M. Usman, "Security Enhancement for Authentication of nodes in MANET by checking the CRL status of Servers", International Journal of Advanced Science and Technology, vol. 22, **(2010)**, pp. 49-58.

[3] S. Park, B. Aslam, C. Zou and D. Turgut, "Defense against Sybil Attack in Vehicular Ad hoc Network based on Roadside Units Support", Proceedings of Military Communications Conference (MILCOM'09), Boston, MA, USA, **(2009)** October 18-21.

[4] B. K. Chaurasia and S. Verma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering, vol. 6, no. 2, **(2011)**, pp. 41-54.

[5] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET", IEEE J. Select. Areas Communication, vol. 25, no. 8, **(2007)**, pp. 1569-1589.

[6] Bin Xiao, Bo Yu, Chuanshan Gao, ―Detection And Localization Of Sybil Nodes In VANETs‖, Diwans'06, September 26, 2006.

[7]] Maria Elsa Mathew and Arun Raj Kumar P **"**Threat Analysis and Defense Mechanisms in VANET" IJARCSSE Volume 3, Issue 1,January 2013

[8] Byung Kwan Lee, Eun Hee Jeong and Ina Jung "A DTSA(Detection Technique against a Sybil Attack) Protocol Using SKC (Session Key based Certificate) on VANET" International Journal Of Security and Its Applications Vol. 7, No. 3, May, 2013

[9] B. K. Lee, E. H. Jeong and S. H. Yang, "A SAP (Safe Authentication Protocol) design against a Sybil Attack on VANET", International Conference on Computer and Applications (CCA 2012), Proceedings, Seoul, Korea, (2012) March 30-31.

[10] Q. Huang, J. Cukier, H. Kobayashi, B. Liu and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks", WSNA'03 Proceedings of the 2nd ACM International conference on Wireless Sensor Networks and Applications, San Diego, CA, USA, **(2003)** September 19-19.

[11] M. Aydos, T. Yantk and C. K. Koc, "An High-Speed ECC-based Wireless Authentication Protocol on an ARM Microprocessor", The 16th Annual Computer Security Applications Conference, New Orleans, LA, **(2000)** December 11-15.