A Survey on Effective Way of Message Authentication Using Proxy Vehicle in Vehicular Ad-Hoc Network

Punam R. Sathe[1], Ganesh N. Dhanokar[2]

[1]ME Student, Computer Department, G. H. Raisoni College of Engineering, Jalgaon, North Maharashtra University India

[2]Professor, Computer Department, G. H. Raisoni College of Engineering, Jalgaon, North Maharashtra University India

Abstract: ***Now a day's communication is the best medium to share the information from one place to another, like message sending, emails and vehicle communication. Vehicle communication is another new concept which plays the most important role in our daily life. Vehicle communication is based on V2V and V2I.Identifing the message sender and verifying the integrity of message is done with the help of PKI. Authentication of any message is performed by first checking if the sender's certificate is included in the current Certificate Revocation List. A PKI use in VANET for authentication .Superior vehicular communication is the necessity of regular life, because it provides reduction of message loss. This paper provides an effective message authentication using proxy vehicle in VANET. Proxy Vehicle is nothing but the vehicle which is used to verify the signature and result will be pushed into the RSU.***

Keywords: Message Authentication;Privacy Preservation;Proxy Vehicle;Vehicular adhoc network(VANET)

1. Introduction

Today's world is a world of connectivity and fast communication, without inter-connectivity world would come to stand still. Telephone, media(T.V/News world), Mobile, Internet are different media for connectivity from which Internet is one of the most effective way for establishing connectivity and carry out global communication. In recent times message authentication is the crucial issue regarding the data transmission through the wired/wireless networks. Vehicular ad hoc Network uses Public Key Infrastructure.PKI is used to verify integrity of message and identity of messages sender. VANET will enable both V2V and V2I communication[8].Authentication includes the level of security and efficiency in verification process. Existing system focus on security and privacy of VANET.

Our area of interest is about message authentication in proxy vehicle for VANET. The remnant of this paper is prepared as follows. Section2nd provides current research work done related to our topic of search. Section 3 proposes newer approach based on message authentication in VANET.The working of proxy vehicle is to authentication multiple message with verification function.The RSU is used to verify the output which is generated by proxy vehicles. The last section includes conclusion and future scope of the concept.

2. Related Study

We already know about the VANET are an emerging infrastructure that makes use of vehicles as the main objects within a network.

a) Expedite Message Authentication Protocol(EMAP)

This is protocol to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL.EMAP employs keyed Hash Message Authentication Code(HMAC) in the revocation checking process. The advantage of this is free from the false positive property which is common for lookup hash table [6].

b) Elliptic Cryptography Digital Signature Algorithm (ECDSA)

It is one of the Traditional public key infrastructure offers more efficient security standards, Hash Chain Protocol could potentially be deployed side by side to ECDSA when delays in the network are inevitable and faster processing is required by the system [7].

3. Related Techniques

Generally with the help of this section we can focus on the number of techniques which is used into VANET for the message authentication.

In [1], the writershave studied HMAC function is used in EMAP for authentication. Probabilistic random key distribution employing by Novel key sharing scheme. Replacing time consuming CRL checking process.SHA-256 is used for the purpose of fast revocation checking process and novel key sharing scheme.Public key infrastructure holds the authentication certificate.

In [2], an author explains in detail about HMAC function and novel key sharing scheme employing probabilistic random key distribution.ECDSA to check the authenticity of the certificate and signature of the sender, this digital signature method chooses by WAVE standard.

In [3], the creators of this paper describe the Message Authentication Protocol. Expedite message authentication protocol adopted in VANET.

a) EMAP protocol having some entities

- Trusted authority (TA):-

The main function of trusted authority is to provide an Anonymous certificate and distributing secret keys to all On Board Unit in the network.

- Road side Unit(RSU):-
  RSU is a static unit and it can be distributed all over the network.
- On-board unit(OBU):-
  Vehicle to vehicle and vehicle to infrastructure communication is done with the help of OBU.

b) V2V and V2I

Vehicle to vehicle and vehicle to infrastructure are the two basic mode used for communication.

In [4], introduces the proxy base authentication scheme. Algorithm having the number of phases such as

a) System initialization phase
   This is the first phase of algorithm; it represents the initial stage of algorithm. The system parameters are registered in VANET.
b) Message Signing Phase
   The integrity of message and the validity of the originator are ensured, vehicle send a message and that should be signed with private key.
c) Batch verification by proxy vehicle
   Message send by vehicle then after that message can be verify with the help of proxy vehicle.
d) Verification by RSU

This phase having the task such as the originator of the message is real proxy vehicle, guarantees of correct verification and the proxy vehicle when the RSU finds it fails the process.

In[5],the worker explain the Hash Message Authentication Code checking process to replace the certificate revocation list checking process, the message loss ratio still remains zero.

4. Framework Design and Proposed System

The proposed technique provides:

a) System Structure

The system’s structure [8] is divided into three major steps.

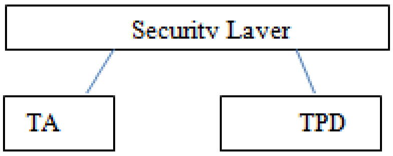

Figure a: Security Layer

- Trusted Authority(TA)
  It is a management center of the network. Registration and certificate for RSU and OBU are easily provided by TA.TA is powerful enough in terms of communication, computation, storage.
- Tamper Proof Device (TPD)
  This device is installed in Vehical.The main function of this device is to store all security related materials.

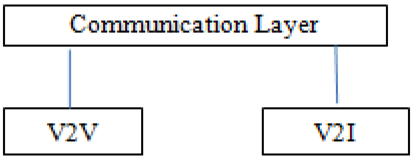

Figure b: Communication Layer

- Vehicle To Vehicle(V2V)
  This communication allows vehicle object to communicate together and exchange information.
- Vehicle To Infrastructure(V2I)
  This mode of communication allowOn Board Unit to communicate with the infrastructure.

5. Conclusion

This paper presents a novel multivariate correlational analysis based approach of detecting Denial of service attacks which differentiates both known as well as unknown DOS attacks from valid network traffic records. Important geometrical correlational features are extracted from individual pairs of two distinct features, the triangle are map approach helps to speed up the process. The future scope of this approach is real time implementation of the system over real world data and checking its performance practically and implement more optimized and sophisticated traffic characterization technique to reduce the false-positive detection rate.

6. Acknowledgment

Authors would like to Special thanks many of the people who helped me while presenting this paper. First of all preparation of this paper would not have been possible without the endless contribution of time, effect and valuable guidance. G.H. Raisoni College of Engineering forproviding all the necessary facilities. The author is highly grateful to Prof. G. N. Dhanokar for his valuable guidance throughout the work.

References

[1] Mrs.M.R.ajalakshmi,R.Kasthuti,J.Nivesha,J.Varalakshmi”Secured Expedite Message Authentication protocol For Vehicular Ad Hoc Network”IJREAT ,Volume 2,Issue 2,Apr-May,2014.

[2] R.Rajkumar ,S.Shahul Hammed(2014)“Accelerated Message authentication Protocol For Vehicular ad-hoc Networks” Volume 2issue 1,2014.

[3] Ranganathan,(2014),“Precipite message manifest protocol for vehicular ad hoc networks”(IJCSMC) International Journal of Computer Science and Mobile Computing,vol-3,issue 2,pg476-482.

[4] Yiliang Liu,Liangmin Wang,Hsiao-Hwa Chen,Fellow “Message authentication using proxy vehicles in Vehicular ad-hoc Network”,Member,IEEE,Vol-64,No-8,August 2015.

[5] Xiaoyan Zhu,Shunrong Jiang,Liangmin Wang ,and hui Li”Efficient Privacy – Preserving Authentication For Vehical Ad Hoc Networks”IEEE Transaction on Vehicular Technology ,Vol 63,No.2,February 2014.

[6] Albert Wasef and Xuemin (sherman) Shen, IEEE, Fellow" Expedite Message Authentication Protocol For Vehicular Ad Hoc Networks"IEEE Transaction On Mobile Computing ,Volume 12,No.1,January 2013.

[7] Jesse Lacroix,Khalil El-Khatib"Vehicular Ad Hoc Network Security and Privacy: A Second Look"The Third International Conference on Avances in Vehicular Systems,Technology And Applications,Vehicular 2014.

[8] M.Ravichandran,D.Raju,G.Sujatha"Hasten Message Authentication Protocol For Vehicular Ad Hoc Networks"International Research journal of infinite innovationsin Engineering And Technology,Volume 1,Issue 3,July 2014.