AN ERGONOMIC METHOD OF CREDENTIALITY OF VARIOUS REQUESTS FROM EMERGENCY VEHICLE USING BATCH REQUEST AUTHENTICATION ALGORITHM

S.SILAMBARASAN*1,Mrs.M.MAHESWARI#2Mrs.K.REJINI#3,Mr.D.RAJINI GIRINATH*4

**1P.G Student, M.E CSE, Anand institute of higher technology, Chennai, T.N, India.*
#2Asst.prof, Dept of CSE, Anand institute of higher technology, Chennai, T.N, India
#3Asst.prof, Dept of CSE, Anand institute of higher technology, Chennai, T.N, India
#4Head of the, Dept of CSE, Anand institute of higher technology, Chennai, T.N, India

Abstract— **VANET is a form of Mobile Ad-Hoc Network which provides communication between vehicles and road-side base stations. The aim is to provide safety, traffic management, and infotainment services. The security of VANET is in concern state from early time. VANETs face several security threats and there are a number of attacks that can lead to human life loss. Existing VANET systems used detection algorithm to detect the attacks at the verification time in which delay overhead occurred. Batch authenticated and key agreement scheme is used to authenticate multiple requests sent from different vehicles. Yet it does not provide any priority to the requests from emergency vehicles and a malicious vehicle can send a false message by spoofing the identity of valid vehicles to other vehicles leading to Sybil attack. Batch Request Authentication Algorithm (BRAA) is used to classify the requests obtained from multiple vehicles in order to provide immediate response to emergency vehicles with less time delay. This system also to prevent Sybil attack by restricting timestamps provided by RSU at an early stage itself.**

Keywords— ***VANET; BRAA; Sybil Attack; Timestamp; Road Side Unit (RSU).***

I. INTRODUCTION

The need for transportation is increasing day by day because of this; number of vehicles can also increase dramatically. So it is necessary to regulate vehicle traffic and improve safety for vehicles and human lives on roads. This initiates the development of new kind of network called Vehicular Ad-hoc Network (VANETs) [9].Vehicular communication network is one of the developing technologies to provide safety for human lives, management of traffic in roads and also disseminates messages to drivers and passengers. In VANETs, vehicles are able to communicate with each other and Road Side Units (RSU).By using VANET we can avoid collision among vehicles and it also provides some important services, like unmanned driving of vehicles, navigation, safety for vehicles, reduce traffic and also allow access to internet and entertainment applications. VANET provides two types of applications [9],first is safety applications to send safety related information's like traffic alerts and to avoid collisions, at every 300ms each vehicles can transmit its current location, speed and directions which can be generated by the Global Positioning System (GPS). Second are non safety applications for internet surfing, chatting and toll payment services. The below figure 1 shows the system model of VANET.

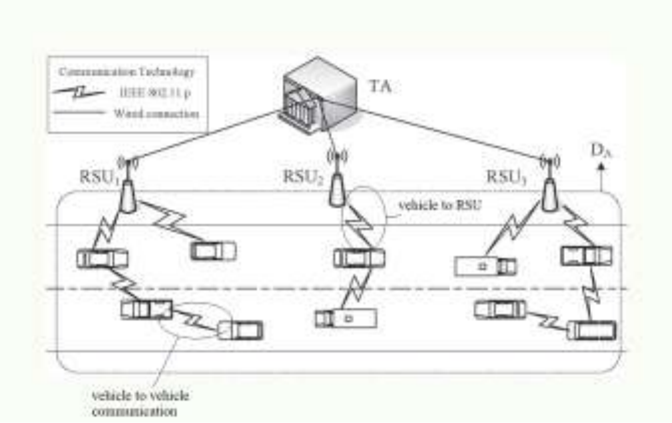

Fig 1. System Model of VANET

A. *Characteristics of VANET are as follows:*

- Network topology can be modified dynamically and quickly.
- Communication link lives for a short period of time.
- Authorized infrastructures such as RSUs are located at Important regions for provide extra services.
- Nodes in the network have high functionality (more power supply, able to perform computation quickly).

From these we can separate VANET from other wireless networks.

B. *VANET Requirements:*

VANET requires authentication, availability, data verification, data integrity and privacy [7].

a) ***Authentication:*** To prove the message is obtained from the original vehicle, the received message must be authenticated. To perform authentication, vehicles incorporate its private keys and its certificate into every message it sends. On the receiver side, the message is verified by assuring its keys and certificates.

*b) **Availability:*** **Vehicular** Network must be ready to provide requested services at any time, even a small delay will cause many serious problems.

*c) **Data Verification:*** After the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

*d) **Data Integrity:*** It ensures that data or messages are not altered by attackers. Otherwise, users are directly affected by the altered emergency data.

*e) **Privacy:*** The information of a driver must be kept secure from the unauthorized observers, such as path, speed, identities etc. This can be done by temporary keys, these key can be changed frequently. It is used for one time and then it expires. All these keys are stored in TAMPER PROOF DEVICE and it can be retrieved when it is necessary.

II. TYPES OF VANET ATTACKS

VANET faces several security attacks [8], they are as follows;

A. Black Hole Attack

The Black Hole in the network is formed by the number of malicious vehicles .These vehicles deny to transmit the messages received from the legalized vehicles. This leads to heavy packet loss because no nodes or vehicles in that area will transmit the received message to other vehicles.

B. Denial of Service Attack (DOS)

Attackers make the resources unavailable to the legitimate user who is having all rights to use those resources and also they may transmit dummy messages to jam the channel and thus reduce the efficiency and performance of the network.

C. Masquerade

A vehicle modifies its identity and acts like another vehicle for its own purpose. This can be attained by message fabrication, alternation and replay. An attacker can act like an ambulance or any other emergency vehicles to deviate or slow down other vehicles.

D. Malware and spam

Viruses and spam can cause serious damage to the normal operation in VANET. When performing software updates of On Board Units (OBU) of vehicles and RSUs the inside attackers introduce the malware and spam attacks.

E. Timing Attack

When malicious vehicles or attackers receive any emergency message they do not forward it to the neighboring vehicles at the right time, but they add some timeslots to the original message to create some delays. Thus the neighboring vehicle receives the message after they actually require it.

F. Sybil Attack

It is an identity forging attack that a malicious node impersonates several other nodes in order to disrupt the proper functioning of VANET applications. A node that spoofs the identity of other vehicles is called a Sybil attacker.

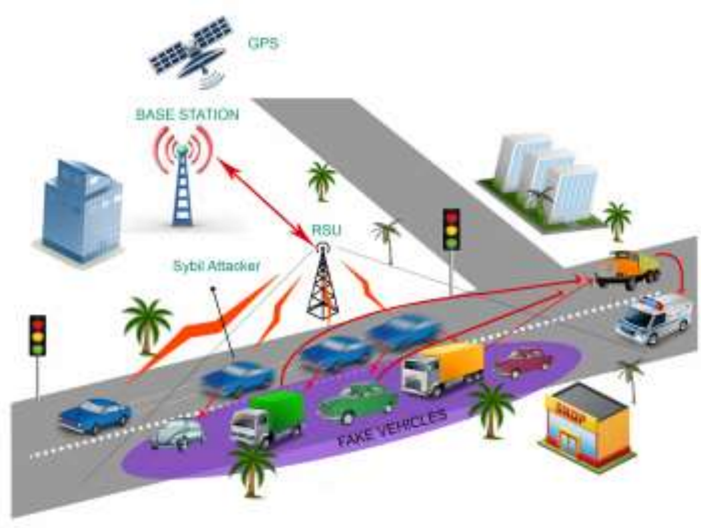

Fig 2. Sybil Attack Model

Figure 2, shows the model of Sybil attack. A node whose identity gets spoofed is called as Sybil node. A Sybil attacker creates an illusion of traffic on the road.

III. EXISTING WORKS

The author [1] [6] tries to defend against the Sybil attack with only support of Road Side Unit (RSU). Whenever a vehicle passes the RSU it obtains a timestamp. If a vehicle wants to send a message to another vehicle, it incorporates the timestamp inside the message. The author finds it impossible for two vehicles to pass two or more RSUs at the same time, so there must be a small time difference between them.

According to the timestamp provided by the RSU, a new kind of timestamp series mechanism is developed. It is difficult for two vehicles to obtain the same timestamp while crossing multiple RSUs. From this a Sybil attack can be detected.

Due to providing multiple timestamps it is insecure for any attack. When a vehicle requests multiple timestamps from a single RSU, it means there is a chance that the vehicle may act as a Sybil attacker. Assume that the timestamp requesting vehicle is a Sybil attacker; by using the obtained timestamps the vehicle creates multiple Sybil nodes. By these Sybil nodes a false traffic message can be provided to the legitimate vehicles.

In order to detect the Sybil attack, two timestamps which are obtained from the last two RSUs passed by the vehicle must be enclosed with the traffic message sent to legitimate vehicles. The updating of timestamps is also known, instead of keeping the two timestamps in a message, a new aggregated timestamp has been created; it contains both the current and previous timestamps.

Secure batch verification [2] [3] is carried out to avoid the invalid or false message from the unauthenticated or even authenticated vehicles. By avoiding these false messages, road accidents and traffic jams can be prevented to continue the safe and secure transportation.

A digital signature is used to ensure the identity authentication and message integrity. A vehicle signs the message with digital signature and then sends it to the RSUs for verification. They improve the scheme to prevent replay attack and forgery attack. The scheme includes key generation and pre-distribution phase, pseudo identity generation and message signing phase, identity tracing and message verification phase.

Tracking of vehicle identity becomes difficult when the generation of pseudo identity for vehicle gets failed. There is also threat for replay and non reputation of digital signatures. The identity of vehicle can be lost.

An author presents a novel solution named Sybil attack detection based on signature vectors (SADSIV) [4] [6] in VANETs. Each node gathers the digital signatures in their moving; then the algorithm detects Sybil attack by analyzing and comparing vehicle nodes' signature vectors independently under the condition of inadequate infrastructures.

Proposed system present an algorithm to detect the Sybil attack detection based on signature vectors (SADSIV) in VANETs. There are some distributed authority units (AUs) in a VANET system. These AUs are comprised of authorized RSUs and some mobile nodes, including police or public transport vehicles. It is assumed that these authorized units can provide the digital signatures with timestamp for the vehicle nodes periodically. And all vehicle nodes will record these digital signatures for the detection. And these legal nodes gather and record the signature vectors from different AUs in their movement. In contrast, Sybil nodes have the same locations and motion trajectories all the time. They always get the signatures from same AUs because of their consistent trajectories. The authorized units provide signatures with timestamp every one minute. In an algorithm when a detector wants to detect Sybil attackers around, it gathers the neighboring nodes signature vectors

A signature vector is more robust and it is obtained based on the collaboration of neighboring nodes. Each vehicle can independently detect Sybil attack by comparing the differences of neighboring nodes digital signature vectors; this algorithm is more feasible even less infrastructure resources.

An author presents a new kind of Sybil detection approach, based on received signal strength variations, allowing a node to verify the authenticity of other communicating nodes, according to their localizations.

This paper provides Sybil attack detection [5] [6] approach based essentially on received signal strength variations. This approach allows a node to verify the authenticity of nodes with which it is communicating, via two complementary techniques, the verification of their geographical localizations and the evaluation of their distinguish ability degree.

IV. PROPOSED MODEL

Introduced the Batch Request Authentication Algorithm (BRAA) to provide an immediate response to the emergency vehicles. When an RSU receives multiple requests from different vehicles at a same time, time delay can occur to process all of them and it does not provide a quick response to emergency vehicles like ambulance, fire and police.

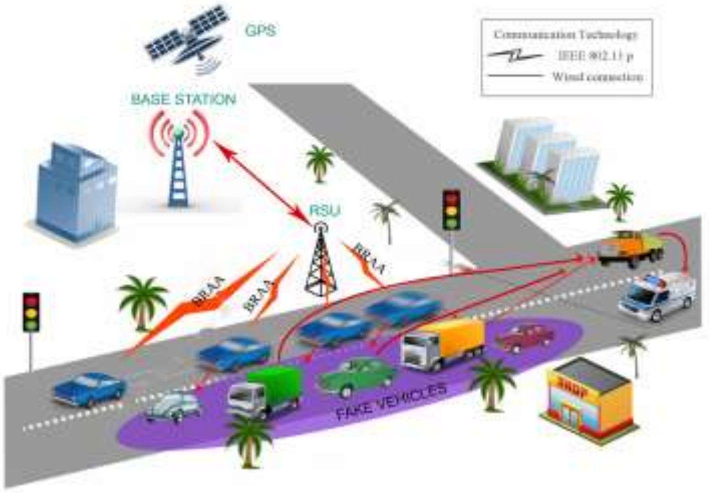

Fig 3. Proposed Model of Batch Request Authentication Alg

A. *Hash Function, Hash Chain, and HMAC*

A one-way hash function $h(\cdot)$ is said to be secure if the following properties are satisfied [18].

1) $h(\cdot)$ can take a message of arbitrary length as input and produce a message digest of a fixed-length output.
2) Given x, it is easy to compute $h(x) = y$. However, it is hard to compute $h^{-1}(y) = x$ given y.
3) Given x, it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$.

Furthermore, a hash chain is defined as in Fig. 2, where $S_k = h(S_{k-1})$, $k = 1,2,...,i$, and $S_0 = SD$, where SD is the initial seed value. According to the definition of the hash function, it is obvious that, given S_k, it is easy to compute $S_{k+1}, S_{k+2}, ..., S_i$ but infeasible to compute any one of $SD, S_1, ..., S_{k-1}$.

HMAC is used to authenticate the source of a message and its integrity by attaching a message authentication code (MAC) to the message, which is accomplished by a cryptographic keyed hash function (such as MD5, SHA-256). In this paper, we use HMAC for two purposes: 1) ensuring the validity of senders' identities, since only valid users can generate correct HMACs; and 2) checking the integrity of messages before batch verification, thus achieving the efficiency of batch verification. The detailed algorithm process of HMAC can be found in [19]

B. *Proposed Model of Priority Batch Verification Algorithm*

It is common multiple vehicles send request to single RSU at same time. Generally RSU perform operation on those received request by using batch verification algorithm and provide needed services to the vehicles. But it does not assign any priority and provide response to the request from emergency vehicles [2] [3]. It is very important to provide immediate services to emergency vehicles.

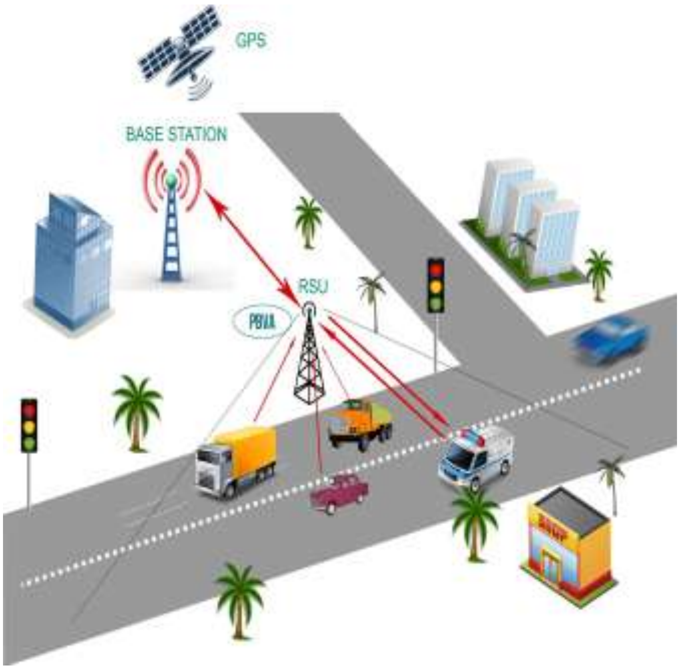

Fig 4. Proposed Model of PBVA

The above Figure 4, shows the proposed model of PBVA Mechanism.

The Proposed model Priority Batch Verification Algorithm (PBVA) is installed in each RSU. When RSU receives multiple requests at the same time, PBVA processes these requests in order to detect any request received from emergency vehicles.RSU classify the obtained requests by using the vehicle identifier found in the received requests. Each vehicle in the VANET has unique identifier by this only RSU identifies whether it is an emergency vehicles or other general vehicles.

If RSU obtains requests from emergency vehicles our mechanism PBVA immediately processes these requests and sends necessary services to that vehicle without time delay.

a) *Algorithm*

```
Begin
RSU received BR={req1,req2,…,reqn}
V1,….vn=req1,req2,…reqn
V[n]=req[n]
For (i=0;i<n;i++)
Classify the requests
If (req[id]==vr1)
Return “AMBULANCE”
Return “provide service to the request”
Else if (req[id]==vr2)
Return “FIRE AND POLICE VEHICLE”
Return “provide service to the request”
Else
Return “GENERAL VEHICLE”
Return “safety and non safety services”
End if
End
```

Above code explains the proposed mechanism of Priority batch verification algorithm.

TABLE I. NOTATIONS

Notations	**Description**
T	Timer
ID	Identifier
TS	Timestamp
REQ	Requests
ACK	Acknowledgement
VR	Vehicle Request identifier

Fig 5. Tables

The above table shows the notations used in this paper.

V. CONCLUSION AND FUTURE WORKS

Our proposed system PBVA algorithm is used process multiple request at a single time and also to provide immediate response to the request from emergency vehicles. By attack prevention mechanism we can prevent Sybil attack in early stages itself through restricting the timestamps. In future, we are going to prevent attack by without restrict the provision of timestamps to vehicles and minimize the computation work of algorithm.

REFERENCES

[1] Soyoung Park,Baber Aslam,DamlaTurgut,Cliff C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit", IEEE conference Paper ID 900042,2009.

[2] Zhang Jianhong, Xu Min and Liu Liying, "On the Security of a secure Batch verification with Group Testing for VANET", International Journal of Networks, Vol.16, No.4, PP.313- 320,2014.

[3] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien," ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" IEEE Transaction On Vehicular Technology, VOL. 60, NO. 1, Janauary 2011.

[4] Chen Chen, Weili Han and Xin Wang, "Sybil attack detection based on signature vectors in VANETs", Int. J. Critical Computer-Based Systems, Vol. 2, PP 455,2011.

[5] Mohamed Salah Bouassida,Gilles Guette,Mohamed Shawky And Bertrand Ducourthial, "Sybil Node Detection Based on Received Signal Strength Variation" International Journal of Network Security, Vol.9, No.1, 2009.

[6] Karamjeet Kaur , Sanjay Batish & Arvind Kakaria, "Survey of Various Approaches To Countermeasure Sybil Attack", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Iss-4.,2012.

[7] Mohammed Saeed Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Network (VANETs)", IEEE. 978-1-4673-2393-2,2012

[8] Ghassan Samara , Wafaa A.H. Al-Salihy , R. Sures "Security Issues and Challenges of Vehicular Ad Hoc Networks(VANET)", IEEE Xplore,2012

[9] Wikipedia "Vehicular Ad-Hoc Network"http://en.wikipedia.org/wiki/Vehicular_ad-hoc_network thispage was this page was last modified on 15 December 2013.

[10] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET,"IJNSA, Vol.3, No.6, November 2011.

.