International Journal of Pure and Applied Mathematics
Volume 118 No. 20 2018, 4813-4821
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Efficient Privacy Preserving Emergency Message Passing In VANET

G. Santhana Devi[1], M. Germanus Alex [2]

[1]Research & Development Center, Bharathiyar University, Coimbatore-641 046, Tamilnadu
[2]Kamarajar Government Arts College, Surandai 627859, Tirunelveli District, Tamilnadu

Abstract

In present-day, vehicular ad hoc networks (VANETs) provide spontaneous traffic associated messages to its users informing them with the road condition, road route, traffic signal and weather condition of the route thereby to enable them with the trouble-free driving. Most importantly VANETs broadcast emergency messages in times of exigencies that save people's lives from disaster. It has been a great challenge to ascertain the authentication and privacy of the messages that are broadcast in VANETs. In this paper to ensure privacy to the honest users we have recommended Trust Authority [TA] to provide a long term primary token to the vehicles and use this token for all its communication purpose. In addition it is necessary to receiving the short term secondary token from RSU at each interval of time. The authentication of the emergency message is verified with the help of short term pseudonymous. Since the emergency messages require secure, timely and factual communication our proposed Efficient Privacy Preserving Emergency Message Passing Protocol [EPPEMP] recommend the distribution of two different tokens, so that the privacy, security and the authentication of emergency messages are ensure to the VANET users.

Keywords: VANET, Privacy, Authentication, Protocol, emergency message

I.INTRODUCTION

Vehicular ad-hoc network provides a perfect transportation system to the world. It is one of the subclass of mobile ad-hoc network. Generally the VANET architecture has three major elements, namely the Trust Authority (TA), Road Side Units (RSUs) and Vehicles. In VANET each vehicle equipped with OBU [On Board Units], it has computation and communication capabilities [1]. RSUs placed on the road side at miscellaneous distance and the TA [Trust Authority] as well. The vehicular network has three type of communications namely vehicle to vehicle communication (V2V) communication, vehicle to RSU [Road Side Unit] communication (V2R) and RSU to RSU communication (R2R). The Vehicular ad hoc network applications are usually categorized into two main types that are safety applications and non safety applications. The safety applications is to provide early warning to the users such as [2] traffic signal warning, emergency break warning, crash warning, hazard notification and collision warning. In addition there are safety applications that are necessary after the assurance of a disaster or accident to send the emergency message to nearby emergency rescue team. These applications also facilitate the fast and secure message dissemination.

The rest of the paper is organized as follows: Section 2 discuss related work. Section 3 discusses proposed protocol. Next, performance analysis is described in Section 4. Section 5 discusses concluding remarks.

II.RELATED WORK

In [3] Raya et.al, have proposed of securing vehicular ad-hoc networks based on pseudonymous scheme, in which pseudonyms are used to hide the real identities of the vehicles. The pseudonyms have only a short life, so the vehicles should contain a large number of pseudonyms in the vehicle's OBU. In this paper, the author proposed [4] a Hierarchical Privacy Preserving Pseudonyms Authentication Protocol for VANET. In this paper, the author proposed [5] a TWO-Factor lightweight privacy preserving authentication scheme for VANET (2Flip) which utilize decentralized certificate and biological password based authentication. In this scheme use authentication code and one way hash operation for to improve the privacy preserving authentication. In this protocol hierarchy of pseudonyms based on the time period of their usage and does not require and maintaining a CRL. In [6] s.devi et.al, have provide fast emergency message dissemination routing protocol. In this paper [7], the author proposed a cloud-assisted conditional privacy preserving authentication protocol for VANET. This protocol is hybrid approach that utilizes both the concept of pseudonyms based approaches and group signature based approaches. In this paper [8], the author introduced location based CPPA scheme for VANETs without the bilinear pairing and tamper-proof device. In this paper [9], the author proposed efficient identity-based authentication scheme with conditional privacy preserving for VANETs by using Elliptic Curve Cryptography (ECC).

III.PROPOSED MODEL

This section explains our proposed efficient privacy preserving emergency message passing protocol, which is used for secure VANET emergency message communication.

Notation	Description
V_i	Sender Vehicle
P_{TK}	Primary Token
S_{TK}	Secondary Token
$M_{REQ}[S_{TK}]$	Secondary Token Request Message
$M_{VERIFY}[V_i [P_{TK}]]$	Primary Token Verification Message of Vehicle Vi

Table –I Notation

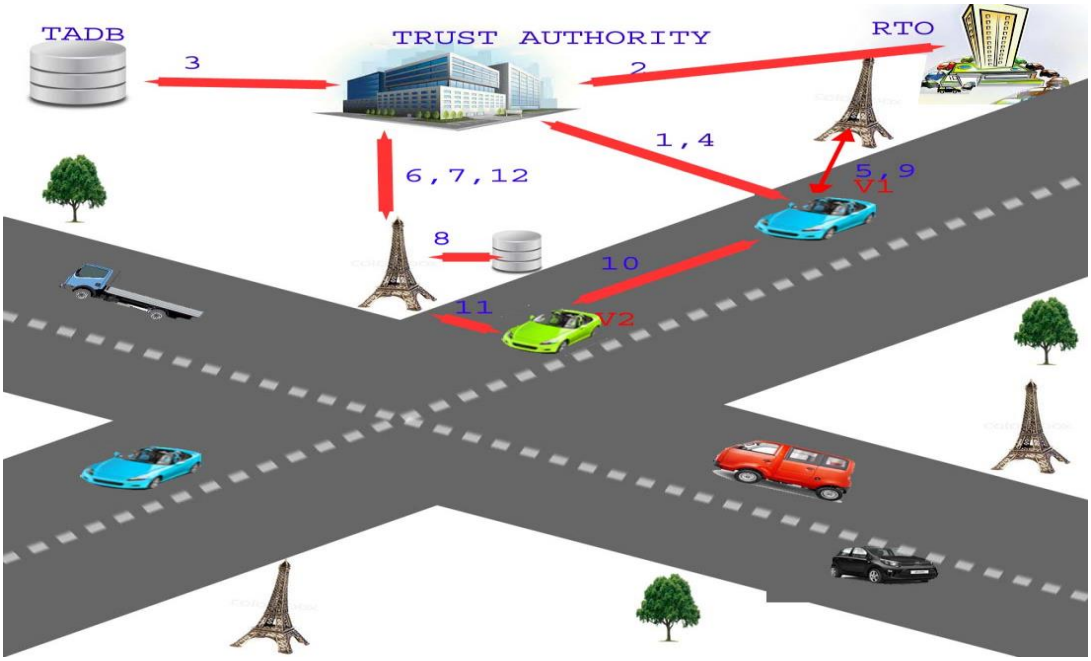

Fig:1 The Proposed System Model

A. System initialization

Boneh and Franklin [10] established the ID-based encryption scheme based on bilinear pairings on elliptic curves. P is the generator of G and $e(P, Q)$ is the generator of G_T

Let $\hat{e}: G \times G \rightarrow G_T$ is bilinear map between these two groups .The map must satisfy the following three properties:

i) *Bi-linearity*: $e(aP, bQ) = e(P,P)^{a\,b,}$ Such that, $\forall (P,Q) \in G$ and $\forall (a,b) \in Z^*_n$

Such that Z^*_n is a multiplicative group of Z_n, n is the integer modulo. In particular,

$Z^*_n = \{x / 1 \leq x \leq p-1\}$ since p is prime.

ii)Non-degeneracy: $\forall P,Q \in G$, such that $e(P,Q) \neq 1$

iii)Computability : e is efficiently computable. Compute $e(P,Q), \forall P,Q \in G$

B. Vehicle Registration and Primary token allocation

During the registration process vehicle V_i sends its Vehicle Register Number, and the owner details to the trust authority TA. The trust authority verifies the vehicle V_i details and its owner details with the Vehicle's Manufacturer department. If the details are correct, TA generate primary token $V_i[P_{TK}]$ for vehicle Vi and the expiry time $V_i[P_{TK\_EXP}]$ to the vehicle V_i. . The primary token generation procedure is explained as follows

The TA selects an arbitrary $P \in G^*$, and selects a random integer $k \in Z^*_n$.

$V_i[P_{TK}] = e(P,P)^k$

After generating primary token, the Trust authority saves the vehicle register number and Primary token in the trust authority database [TADB], which is trust worthy.

C. Secondary Token allocation

When the Vehicle V_i enters a new RSU coverage, it sends a secondary token request $[S_{TK\_REQ}]$ message along with the P_{TK} to the RSU. The secondary token is valid in short time (ex: one day). As the RSU Receives the secondary token request message from the vehicle V_i . It sends P_{TK} of the requesting vehicle to the Trust authority for verification.

After receiving the verification message, TA verifies the vehicle V_i 's $P_{TK,}$ and current location with TADB database .During the verification, if the vehicle Vi 's P_{TK} is correct and if its current location is closely associated with the most recently updated TADB location, then the TA sends an approval message to RSU otherwise TA sends a invalid message of its disapproval to RSU.

If the RSU receives an approval message from the TA, then it generates secondary token $V_i(S_{TK})$ and sent to the vehicle V_i .same time this details are saved in RSU Database.

As when the vehicle enters new RSU_i coverage, at this time if the vehicle has an valid secondary token of RSU_i , it continues with the same secondary token otherwise requests for a new secondary token from RSU_i.

Algorithm:
Vehicle Registration and Primary token allocation

1) *$V_i \rightarrow TA$: Send V_i [Register number], V_i [owner details]*

2) *TA*	:	*If (V_i [Register number], V_i [owner details] are true)*
		Compute P_{TK}. Using V_i [P_{TK}] $=e(P,P)^K$
		End if
3) *TA→TADB*		*Save V_i [Register number], V_i [P_{TK}] in TA DB*
4) *TA→ V_i*	:	*Send V_i [P_{TK}]*
Secondary Token allocation		
5) *V_i→RSU*	:	*Send V_i [P_{TK}] and M_{REQ}[S_{TK}]*
6) *RSU→TA*	:	*Send M_{VERIFY}[V_i [P_{TK}]]*
7) *TA→RSU*	:	*Reply valid/invalid*
RSU	:	*If (M is valid)*
		Compute S_{TK}
		End if
8) *RSU→TADB*	:	*Save V_i [S_{TK}], V_i [P_{TK}] in RSU DB*
9) *RSU→ V_i*	:	*send V_i [S_{TK}]*
Message Broadcast		
10)*V_i*	:	*If (Disaster Event)*
		Broadcast emergency message to nearest RSU with V_i [S_{TK}]
		End if
11)*RSU*	:	*Receive message with V_i [S_{TK}]*
		If (V_i [S_{TK}] is valid)
12)*RSU→TA*		*Send emergency message to TA*
		Else
		Discard emergency message
		End if

D. Message Broadcast

In case any disaster event occurs, the affected vehicle or nearest vehicles send emergency message to nearest RSU using intermediate vehicles.

RSU receive emergency message, it verify the message sender by secondary token. If it is valid, then the RSU forwards the emergency message to the TA otherwise the RSU discard the message. After receiving emergency message the TA take rescue action immediately for save people life.

IV PERFORMANCE EVALUATION

In this section we analysis and compare message delay, message delivery ratio, throughput and message overhead of the unsecure emergency message dissemination protocol FEMDRP with the secure emergency message of proposed protocol EPPEMP.

Parameters	Values

Network Area	3Km X 3 Km
Node Density	20 to 150
No of RSU	3
MAC Protocol	IEEE 802_15.4
Beacon Interval	500 Sec
Packet Size	Dynamic
Simulator	NS2

Table II: Simulation Setup

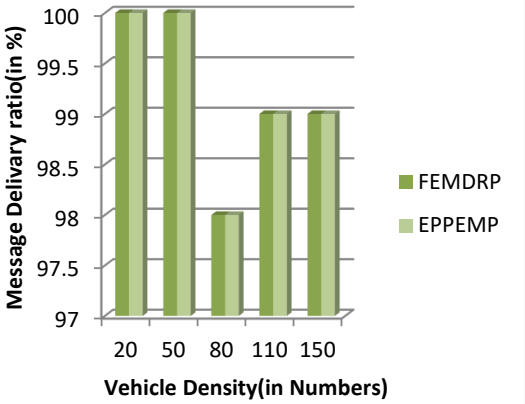

Fig:2Message Delivery ratio

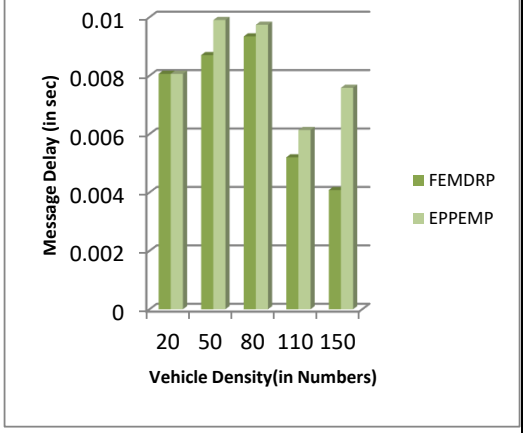

Fig : 3 Message Delay

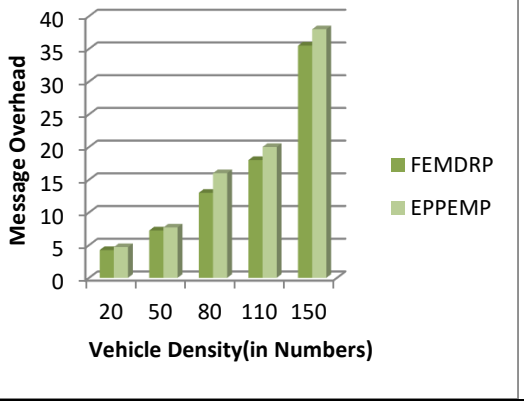

Fig:4 Message overhead

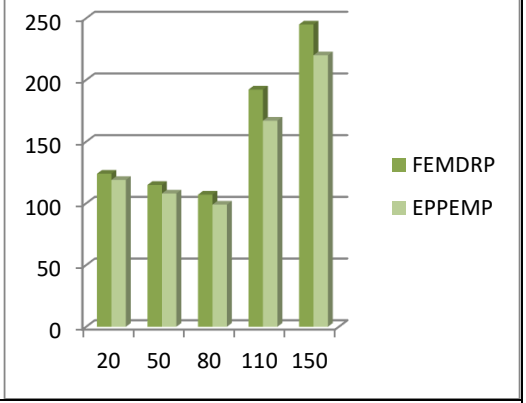

Fig :5 Message Throughput

Simulation Result

The message delivery ratio is the ratio of message delivered successfully to the total number of messages sent. The delivery ratio is obtained for different number of vehicles. The obtained results are shown in Fig 2. In this figure we observe that nearly 100% message delivery. End to end Message delay means the time taken by the message to reach the destination from the sender. The obtained results are compared with the FEMDRP which is shown in Fig 3.The

message overhead is the ratio of the number of emergency messages received by the node to the total number of emergency messages sent. The data obtained is compared with FEMDRP as shown in Fig 4.The Message throughput is total number of message received to the total time taken for simulation. The result obtained on secure messaging is compared with the throughput of the unsecure messaging in Fig 5.In the result, message delay and message overhead are increase compare to unsecure message. But it is permissible since it enables the emergency messages to be sent secure as encrypted messages.

V. CONCLUSION

In this paper, we have proposed Efficient Privacy Preserving Emergency Message Passing Protocol [EPPEMP] Our proposed protocol has two diverse tokens with different life time and it provides privacy to emergency message. In future this protocol improves; the tokens updates, in case of any vehicle involving in malicious activity. Moreover, RSU updates the secondary tokens of the involved vehicles. In addition it also improve location security to vehicles and users.

REFERENCE

1. M.Azees,P.Vijayakumar.and L.J.Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks,"IET Intelligent Transport systems,vol.10,no.6,pp.379-388,2016
2. Vishal Kumar, Shailendra Mishra, Narottam Chand, "Applications of VANETs: Present & Future ", Communications and Network 2013, 5,PP 12-15 .L. Yang and F. Wang,"Driving into intelligent spaces with pervasive communications," IEEE Trans. Intell. Syst., vol. 22, no. 1, , Jan. 2007,pp. 12–15.
3. U.Rajput, F.abbas and Heekuck oh," a Hierarchical Privacy Preserving Pseudonymous authentication Protocol for VANET",IEEE Access,2016,PP.1-13
4. F.Wang,Y.Xu,H.Zhang,Y.zhang and L.Zhu, " 2FLIP: A Two Factor Lightweight Privacy Preserving Authentication scheme for VANET" IEEE,2015, Pp. 1- 17
5. G.Santhana Devi, M.Germanus Alex " Fast Emergency message dissemination routing protocol in VANET" Journal of Network Communications and Emerging Technologies (JNCET) Volume 7, Issue 2, February(2017)
6. U.Rajput, F.abbas , J.Wang, H.Eun and Heekuck oh," CACPPA:A Cloud-Assisted Conditional Privacy Preserving authentication Protocol for VANET",IEEE/ACM International symposium on Cluster, Cloud and Grid computing Access,2016,PP.434-442.
7. Libing Wu,Jing Fan, Y.xie,J.wang and Q,Liu,"Efficient location-based conditional Privacy Preserving authentication scheme for VANET",International Journal of Distributed sensor Networks,2017,Pp.1-13.

8. Yong xie,Libing Wu,Jian Shenand Abdulhameed Alelaiwi,"EIAS-CP:new efficient identity-based authentication scheme with conditional privacy-preserving for VANETS",telecommunication system,2016,PP.1-12.
9. D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairings," Advances in Cryptology-Asiacrypt 2001, pp. 514-532, Springer-Verlag, 2001.