ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

# Key Revocation for Secure Vehicular Ad Hoc Network

D. Sujeetha [1] , R. Saranya[2]

***Abstract*—Vehicular Ad hoc Networks are used for communication among vehicles and between vehicles and roadside equipment. The security of vehicular ad hoc networks should be considered in the field of wireless mobile networking because VANETs are exposed to cruel attacks. A number of secure authentication schemes based on asymmetric cryptography have been proposed to avoid those attacks. On the other handthese schemes not suitthe highly dynamic environments such as VANETs, because they cannot efficiently handle with the authentication procedure. Hence, we go for an efficient authentication scheme for VANETs. In this, a distributed lightweight authentication scheme called key revocation mechanism for vehicle-to-vehicle communication networks is implemented. KRM assumes the concept of transitive trust relationships to improve the performance of the authentication procedure. Moreover, KRM satisfies the following security requirements like privacy, location privacy, common authentication, imitation attack resistance, adaptation attack resistance, repetition attack resistance, perfect forward confidentiality, man-in-the-middle attack resistance.***

***Index Terms*—Authentication, key revocation mechanism(KRM), Law executor (LE),mistrust vehicle (MV), Trust vehicle (TV), vehicular ad hoc networks (VANETs).**

## I. INTRODUCTION

Recently, the security issue [1] in VANETs has become a hot topic, and then many researchers provide the V2I and V2V authentication mechanisms to protect valid users. However, the design for an efficient V2V authentication mechanism is more challenge than that for V2I authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in V2V communications. Therefore, we concentrate on V2V network locations and propose an efficient authentication scheme in this paper.The main components of a VANET are the wireless on-board unit (OBU), the roadside unit (RSU), and the authentication server (AS). OBUs are installed in vehicles to provide wireless communication capability, while RSUs are deployed on intersections as an infrastructure to provide information or to access the Internet for vehicles within their coverage. The AS is responsible for mounting the secure parameters in the OBU to authenticate the user. In IEEE 802.11p, the dedicated short range communication system(DSRCS) [2] has two kinds of communication environments: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications.We assume that each vehicle's OBU is furnished with security hardware, containing an event data recorder (EDR),and a tamper-proof device (TPD) [15]–[17] so that an invader cannot obtain information about the vehicle from the OBU. The EDR is responsible for recording important data about the vehicle, such as the location, time. The TPD provides the cryptographic processing capabilities. Finally, we assume that the time of every vehicle is synchronous via GPS device.To address the above need; we propose a decentralized authentication scheme, called KRM, for V2V communication networks. KRM is ainsubstantial authentication scheme because it only uses an XOR operation and a hash function. Although KRM needs low computation since we use Hash and XOR functions, it still satisfies the many security requirements. We use the NS-2 network simulator [19] to evaluate the performance of key revocation mechanism (KRM) the following section describes about in section. This paper is organized as follows. Section II contains previous work, Section III contains related work.Section IV contains algorithm of proposed scheme in detail. In Section V and VI we discuss about Security analysis and result and Section VII deals with conclusion and future work.

## II. PREVIOUS WORK

Raya and Hubaux [6] initially load each vehicle with a large number of unidentified public and private key pairs, and theirequivalent public key certificates. Each of the public key certificates has their pseudoidentity. Then, each traffic messages are signed with a Asymmetric cryptography scheme, and each pair of public and private key has a short lifetime for the purpose of privacy. Freudigeret al. [7] used the cryptographic MIX-zone to improve the location privacy, and Sampigethavaet al. provides location privacy by using the group navigation of vehicles. However, these approaches [6]–[8] do not work well in highly dynamic environments like VANETs because they use asymmetric cryptography or a digital signature verification scheme, which results in high computation costs, long authentication latency, and a large storage space. Based on related studies [6]–[14], the authentication scheme is susceptible to malicious attacks; our objective is to design a scheme that is strong to

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

such attacks.

## III. RELATED WORK

### *A. TRANSITIVE TRUST RELATIONSHIPS*

In VANETs, vehicles are classified as: a law executor (LE), a mistrustful vehicle (MV), and a trustful vehicle (TV) is shown inFIGURE. 1 .The LE is always trustful which may be a police car. It also act as a mobile Authentication server AS. A normal vehicle may be TV or MV. It is trustful when it isauthenticated successfully. Otherwise, it is considered to be MV. And also, the TV becomes MV when the key lifetime expires. In V2V communication network, as the number of LE is finite, the user should wait for the nearest LE to perform authentication. In this paper, we propose a Transitive Trust relationship to improve the performance of the authentication procedure in V2V communication networks. Transitive Trust relationship is shown in FIGURE. 2. Initially there are three vehicles in which one is trustful LE and others are mistrust vehicle with $OBU_i$and$OBU_j$. The first mistrust $OBU_i$becomes trustful and obtains the sufficient authorized parameter to authorize the other mistrustful.

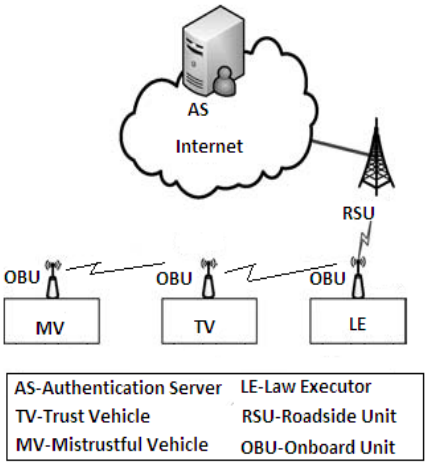


**Fig 1. Transitive Trust Relationship**

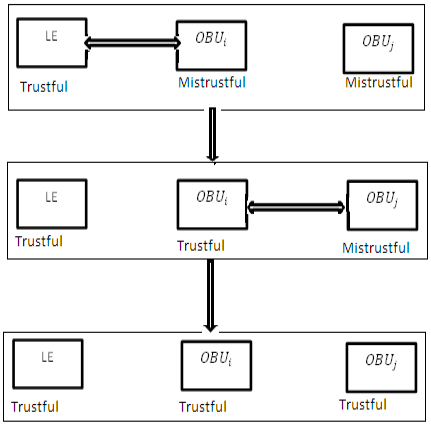


**Fig 2. Transitive Trust Relationship of KRM**

## IV. ALGORITHM

### *A. KEY REVOCATION MECHANISM*

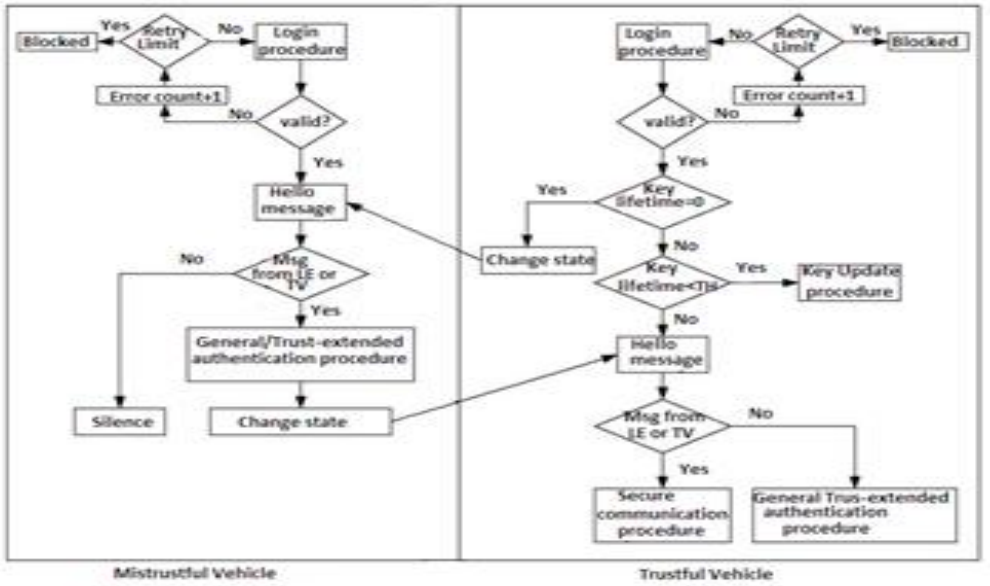


**Fig 3. Operations of the mistrustful/trustful vehicle in a KRM**

In this section, we describe the proposed scheme in detail. A KRM is a decentralized authentication scheme, and

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

the LEs need not to keep the authentication information of the entire vehicles. The proposed scheme involves eight procedures. Before a vehicle can join a VANET, its OBU must register with the AS.FIGURE. 3 show the operations of the mistrustful/trustful vehicle in KRM. The state of the LE does not change because the LE is always trustful.

### *B. NOTATIONS*

Before describing the proposed scheme, the notations used throughout this paper are listed in Table I.

***TABLE I NOTATIONS***

| SYMBOLS | DESCRIPTION |
|---|---|
| $\oplus$ | The XOR operator |
| $\|\|$ | The combination of strings |
| $AID_i$ | The alias of entity i |
| h( ) | A collision-free one-way hash function |
| $ID_i$ | The public identification of entity i |
| $MSG_{KU}$ | A key update message |
| $N_i$ | A nonce or random number i |
| PSK | A secure key set that is preshared among LEs and the AS |
| $PW_i$ | The password of user i |
| $SK_{i-J}$ | A session key between entity i and j, where $SK_{i-j} = SK_{j-i}$ |
| X | A secret key protected by the AS |
| X→Y | User X sends a message to user Y through a secure channel |

### *C. PERIODIC HELLO MESSAGE*

In VANETs, the vehicles broadcast the hello message every so often with the authentication state (i.e., trust or mistrust). To ensure the network security, the secure communication procedure (i.e., Section IV-I) is executed only by the trust vehicle. On the contrary, the MV must complete the authentication procedure (i.e., Sections IV-E and IV-F) in early payment to communicate with other vehicles.

### *D. INITIAL REGISTRATION PROCEDURE*

**1) LE REGISTRATION:** First, the LE executes the LE registration procedure with the AS through the industrialist. The AS calculates the secure key set $\{PSK_i, i = 1, \ldots, n\}$ based on the hash-chain method (e.g., $h^2(x) = h(h(x))$) and drives this key set to the LE. Note thatthe LE only needs to hold a secure key set that is put in storage in the security hardware and it does not need to store any authentication information of the user. Moreover, each $PSK_i$ has a short lifetime for strong security. Each trustful vehicle performs the key update procedure with the LE (i.e., Section IV-K) when the key lifetime is going to end. We can see that the new PSK (e.g., $PSK_2$) cannot be concluded from the old PSK (e.g., $PSK_1$) since the key generation scheme has a one-way feature of the hash function.

**2) NORMAL VEHICLE REGISTRATION:**Other vehicles need to perform the normal vehicle registration procedure with the AS through the industrialist. This initial registration procedure is only performed once.

Step 1) $User_i \rightarrow AS$: A user sends the public identification $ID_i$ and his selected password $PW_i$ to the AS via the industrialist or a secure channel.

Step 2) After getting the user's ID and password, the AS calculates the following secret authentication parameters for the user: $A_i = h(ID_i||x)$, $B_i = h^2(ID_i||x) = h(A_i)$,$C_i = h(PW_i) \oplus B_i$, and $D_i = PSK \oplus A_i$. Thegoal of $A_i$ is to construct the relation between the user's ID and AS. Moreover, the goal of $C_i$ is to construct the relation between user's password, user's ID, and AS. Therefore, the user only answers in the correct personal information (i.e., $ID_i$ and $PW_i$) in the login procedure. Otherwise, the $OBU_i$discards this login request.

Step 3) AS→ $User_i$: The AS stores the parameters (i.e., $ID_i$, $B_i$,$C_i$,$D_i$,h( )) in the OBU's security hardware viathe industrialist or a secure channel.Note that the AS does not need to store the user's information (e.g., the user's password). Therefore, an antagonist cannot obtain the information to launch a stolen-verified attack.In addition, the registered user cannot imitate to another valid user successfully when the user obtains the following parameters. Because the user is not aware of the AS's secret (i.e., x).

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

### *E. LOGIN PROCEDURE*

The login procedure is the gateway. The OBU will find out an error action immediately if the user has wicked intentions.

Step 1) $User_i \rightarrow OBU_i$: When a user wants to access the service, they should provide $ID_i$ and $PW_i$ to the $OBU_i$.
Step 2) The $OBU_i$ checks the $ID_i$ and verifies whether $h(PW_i) \oplus C_i$ is equal to $B_i$, where $B_i$ and $C_i$ are achieved from the initial registration process. When the information is correct, the $OBU_i$ performs the general authentication procedure. Note that $h(PW_i) \oplus C_i$ should match $B_i$. If not then it means that the user provided the wrong $ID_i$ or $PW_i$, resulting in rejection of the login request.

### *F. GENERAL AUTHENTICATION PROCEDURE*

The OBU carry outs the general authentication procedure after the user finishes the login procedure. Note that the OBU never uses the real identity of the user to perform the authentication procedure so no one can obtain the user's original identity (i.e., $ID_i$) via the interrupted message.

Step 1) The $OBU_i$ creates a random number $N_1$ and calculates the message $M_1$ as $h(B_i) \oplus N_1$. Then, it calculates the alias $AID_i$ as $h(N_1) \oplus ID_i$, and creates the message $M_2$ as $h(N_1||AID_i||D_i)$.
Step 2) $OBU_i \rightarrow LE_j$ : The $OBU_i$ sends an authentication request$(AID_i, M_1, M_2, D_i)$ to the $LE_j$.
Step 3) The $LE_j$ checks that the $OBU_i$ is trustful: on reception of the authentication request, the $LE_j$ uses a secure preshared key (PSK) to obtain $A_i$ (i.e., $A_i = D_i \oplus PSK$).The LE recovers the value of $N_1$ (i.e., $N_1 = M_1 \oplus h^2(A_i)$)and then checks whether $h(N_1||AID_i||D_i)$ is equal to $M_2$. It rejects the authentication request if$h(N_1||AID_i||D_i)$ and $M_2$ not equal, which means the authentication message has been modified. Next, the $LE_j$ calculates $ID_i$ as$AID_i \oplus h(N_1)$, creates a random number $N_2$, calculates$AID_j$ as $ID_j \oplus N_2$, and calculates a session key $SK_{ij}$as $h(N_1||N_2)$. Finally, the $LE_j$calculates the authentication reply message (i.e., $AID_j$, $M_3$, $M_4$, $M_5$),where $M_3$ is $N_2 \oplus h^2(N_1)$, $M_4$ is $A_i \oplus h^2(ID_i)$, and $M_5$ is $h(M_4||N_2||AID_j)$.
Step 4) $LE_j \rightarrow OBU_i$ : The $LE_j$ returns the authentication reply message (i.e., $AID_j$, $M_3$, $M_4$, $M_5$) to the $OBU_i$.
Step 5) The OBU verifies that the LE is trustful: The $OBU_i$ calculates the value of $h^2(N_1)$, retrieves the random number $N_2$(i.e., $N_2 = M_3 \oplus h^2(N_1)$), and checks whether $h(M_4||N_2||AID_j)$ is equal to $M_5$. If the information is correct, the $OBU_i$ calculates the value of $A_i$ (i.e., $A_i = M_4 \oplus h(ID_i)$), calculates the session key (i.e., $SK_{ij} = h(N_1||N_2)$), and stores $A_i$ in the security hardware.
Step 6) $OBU_i \rightarrow LE_j$ : The $OBU_i$ sends the message (i.e., $SK_{iji} \oplus h(N_2)$) to the $LE_j$ .
Step 7) The LE uses the session key $SK_{ij}$ to retrieve the value (i.e., $h(N_2)$). Then, it checks this value to prevent an invalid OBU from executing a replay attack.

### *G. TRUST-EXTENDED AUTHENTICATION PROCEDURE*

Trust-extended mechanism is based on the concept of transitive trust relationships that improves the performance of the authentication procedure. The state of a mistrustful OBU becomes trustful and then obtains an authorized parameter (i.e., PSK) when the OBU is authenticated successfully. Then, the trustful OBU plays the role of LE temporarily to assist with the authentication procedure of a mistrustful OBU. In this procedure, the trustful vehicle performs the authentication procedure and works as an LE. As a result, all vehicles in a VANET can complete the authentication procedure quickly.

### *H. PASSWORD CHANGE PROCEDURE*

Although the password change procedure is optional. This procedure is raised when a user wants to change his password. It can be completed without any support from the AS since the security hardware of the OBU stores the parameters $B_i$ and $C_i$
Step 1) The user provides his $ID_i$ and $PW_i$ an input.
Step 2) The OBU checks the $ID_i$ and confirms that $h(PW_i) \oplus C_i$ and $B_i$ is same. If the information is correct, the user can enters in with the new password $PW^*_i$. The OBU then calculates $C_i^* = C_i \oplus h(PW_i) \oplus h(PW^*_i) = B_i \oplus h(PW^*_i)$ as the password and replaces $C_i$ with $C_i^*$

### *I. SECURE COMMUNICATION PROCEDURE*

The secure communication procedure is performed by two trustful vehicles when they want to communicate.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

Step 1) The login procedure is completed and then OBUi creates an alias AIDi and the messages M1, M2, N3 another random number, AIDi is N3⊕IDi, M1 is PSK⊕N3, and M2 is PSK⊕h(AIDi||N3). PSK is identified from the general/trust-extended authentication procedure.
Step 2) OBUi→OBUj : The OBUi sends AIDi, M1, M2 to the OBUj .
Step 3) The OBUj checks that the OBUi is trustful: the request is received and the OBUj uses PSK to find N3 from M1 and then checks the value of h(AIDi||N3). If the obtained value is not correct, then we conclude the message has been modified, and the OBUj discards the request. After that, the OBUj creates a random number N4, calculates AIDj, and session key SKij as h(N3||N4||PSK). Then, the OBUj finds the reply message (i.e., M3, M4), where M3, M4 is PSK ⊕N4 and PSK ⊕h(AIDi||N4||h(N3)) respectively.
Step 4) OBUj →OBUi: The OBUj returns AIDj, M3, M4 to the OBUi.
Step 5) The OBUi checks that the OBUj is trustful: the OBUi finds the value of h(N3), uses PSK to recovers the N4, and checks the value of h(AIDj||N4||h(N3)). When the information is correct, the OBUi calculates the session key SKij = h(N3||N4||PSK ) for this communication.
Step 6) OBUi→OBUj : the OBUi sends the message SKij⊕h(N4) to the OBUj.
Step 7) The OBUj recover the value (i.e., h(N4)) by using SKij.Then,two trustful vehicles uses this session key to communicate.

### *J. KEY REVOCATION PROCEDURE*

In this scheme, the key revocation is based on timer which treats as the lifetime of the key. The authentication state of a mistrust vehicle becomes trustful when it is authenticated successfully. Then, the authentication state is changed into trust in the hello message and the secure hardware sets up a timer to count down. When the lifetime of the key is over, the state of the vehicle is changed to mistrust.

### *K. KEY UPDATE PROCEDURE*

The key update procedure is performed when the key lifetime of the TV will terminate. The TV extends its state of trustfulness after it finishes the key update procedure.

Step 1) The key update procedure is triggered when the key lifetime is below the predefined threshold (i.e., TH). The OBUi prepares to send a key update message to the LE. The OBUicreates a random number N5, and then it calculates the messages M1 as PSKold⊕N5, M2as PSKold⊕MSGKU, and M3as h(M1||M2).
Step 2) OBUi→LEj : The OBUi sends a key update request (i.e., M1, M2, M3) to the LEj .
Step 3)The LEj uses the current PSK (i.e., PSKold) to retrieve N5 and MSGKU. It rejects the key update request if the value of h(M1||M2) and M3 do not match, which means the message has been modified. Next, the LEjcreates a random number N6 and calculates the key update reply messages (i.e., M4,M5, M6), where M4is N6⊕h(N5), M5is PSKnew⊕N6, and M6 is h(M4||M5). Note that the key set of PSK is generated by the hash-chain method. Therefore, the OBU cannot use the current PSK to infer the new PSK. Finally, the LEj calculates the session key (i.e.,SKij ) as h(N5||N6||PSKnew).
Step 4) LEj→OBUi: The LEj returns the reply message (i.e., M4, M5,M6) to the OBUi
Step 5) On receipt of the key update reply message, the OBU icalculates the value of h(N5), retrieves the random number N6 (i.e., N6=M4⊕h(N5)), and obtains the new PSK. Next, the OBUi
Checks the value of h(M4||M5). Then, the OBUi checks whether h(PSKnew) and PSKold is same or not. If the value is equal, the OBUi updates the PSK and calculates the session key SKij ash (N5||N6||PSKnew).
Step 6) OBUi→LEj: The OBUi sends the message (i.e., SKij⊕h(N6)) to the LEj .
Step 7) The LEj uses the session key SKij to retrieve the value (i.e., h(N6)). It then checks this value to prevent an invalid OBU from executing a replay attack. Then, two trustful vehicles can use this session key to communicate securely.

## V. SECURITY ANALYSIS

Due to the page limit, we only discuss the security features of KRM. The detailed cryptanalysis of KRM is listed in our future work.

1) Location confidentiality: Even if an adversary intercepts a number of messages during a definite period, he cannot track the user's physical position because the system's ambiguity mechanism uses a dynamic identification process, and the session key is generated based on a nonce.

2) Common authentication: A common authentication process is essential. The LE needs to confirm the OBU is a authorized user, and the OBU needs to make sure that the LE is valid. In the general authentication

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

procedure, the LE authenticates the OBU in Step 3, and the OBU authenticates the LE in Step 5, respectively. If the assailant intercept the messages and wants to fake a valid OBU/LE, it must generate a legal message to LE/OBU. However, the assailant cannot find the valid message because he does not know the secure key and random number. In addition, the secure communication procedure also achieves the mutual authentication (i.e., in Step3, the OBUj authenticates the OBUi, and the OBUi authenticates the OBUj in Step 5).

3) Resists repeat attacks: To protect the proposed scheme from play again attacks, in the authentication message we add random number. If an adversary intercepted the message and tried to pretend to be a valid OBU by replaying the message immediately, the LE would reject the request because the nonce in the replayed messages would be unacceptable. Furthermore the OBU also checks the random number sent by the LE to prevent play again attacks.

4) Resists adaptation attacks: An opponent can tries to vary the authentication and reply messages. Conversely, we use a one-way hash function to ensure that information cannot be altered. Therefore, this attack will be detected because an attacker has no way to obtain the value of the random number to generate the genuine message. If an attacker transmits a modified packet to the LE/vehicle, the packet can be easily identified by checking the hash values.

5) Resists fake attacks: If an invalid OBU tries to counterfeit another valid OBU's ID (i.e., $AID^*_i$), but they fails during authentication process. Although the attacker forges an alias ID (i.e., $AID^*_i = h(N_1) \oplus ID_i^*$ ), it cannot establish the valid authentication parameter (i.e., $D_i^*$ ) required to obtain authentication. Because the OBU does not know the AS's secret key
(i.e., x), so it cannot work out the value of $A_i$ correctly. In addition, the secret key is confined by the one-way hash function.

6) Decide and change password: Users can choose or change their passwords without the AS's assistance, so that it is easy for them to remember their passwords.

7) Resistance to man-in-the-middle attack: The man-in-middle attack can be prevented in this scheme since we are using the password and the secret key. The attacker cannot act as if to be trustful vehicle or LE to authenticate other MVs since the password (i.e., $PW_i$) or the secret key (i.e., x) is unknown to them.

## VI. RESULT

The performance of authentication procedure of the trust-extended and non-trust-extended schemes via NS-2 simulator [19]. The simulation area is 4500 X 1000 and we use 113 nodes for the performance analysis.FIGURE. 4, 5and 6 shows the graphs, in which trust extended and non-trust-extended scheme are compared in each graph.

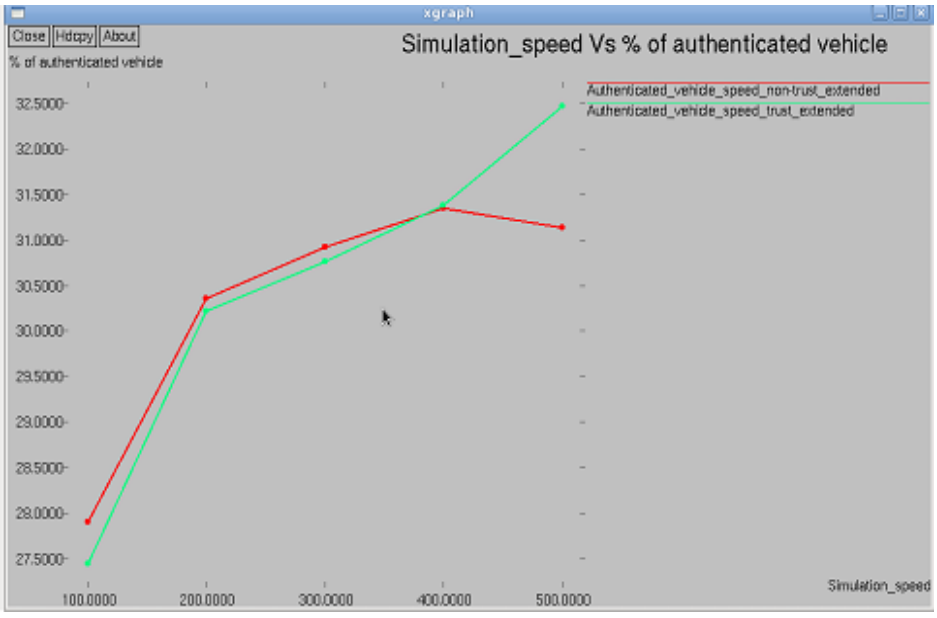


**Fig 4. Simulation Speed Vs. Percentage of Authenticated Vehicle**

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

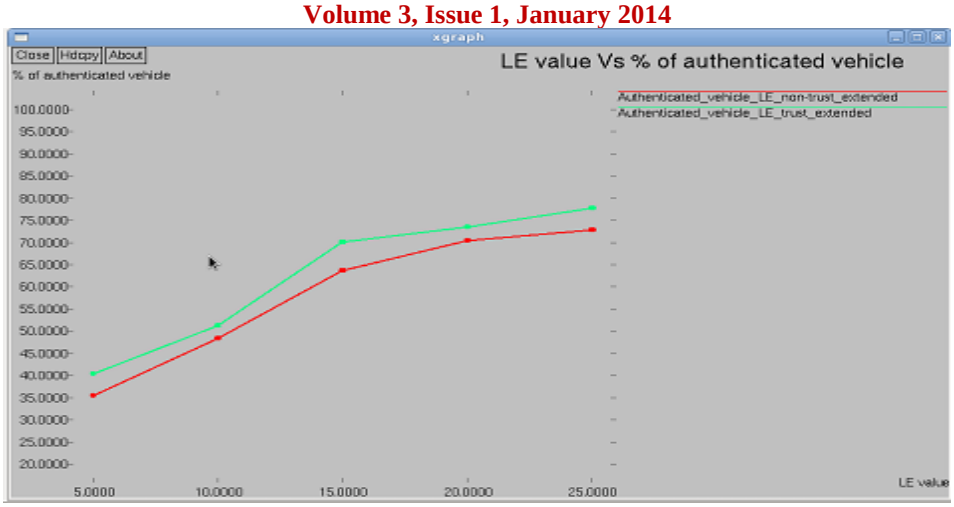


**Fig 5. LE Value vs. Percentage of Authenticated Vehicle**

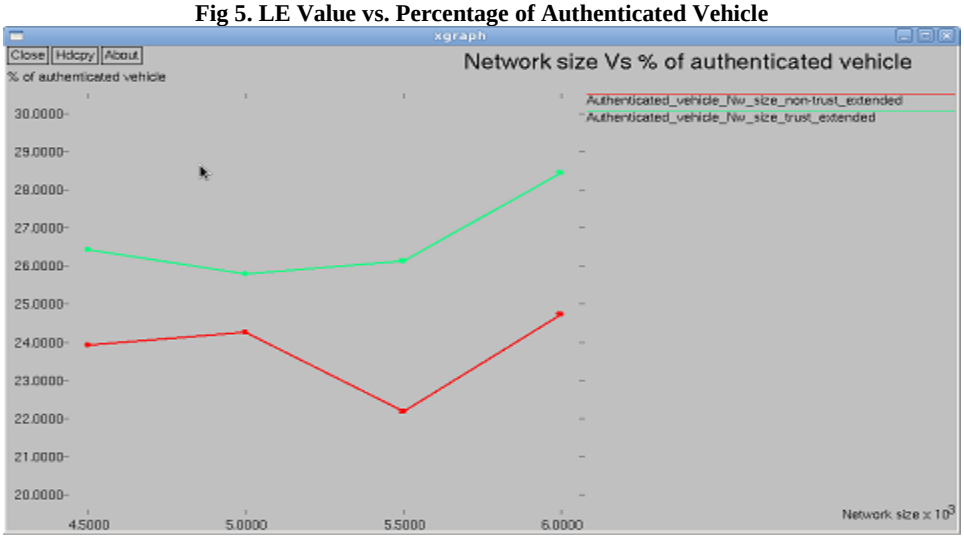


**Fig 6. Simulation Speed vs. Percentage of Authenticated Vehicle**

## VII. CONCLUSION

A distributed insubstantial authentication scheme called KRM protects valid users in VANETs from cruel attacks. In KRM, algorithm is designed by using XOR function and Hash Function that provides authentication. The amount of cryptographic calculation under KRM is less because it only uses an XOR operation and a hash function. It uses the concept of Trust and Mistrust vehicle that strengthens the authentication process. Furthermore, KRM is based on the concept of transitive trust relationships between vehicles that improves the performance of the authentication procedure. In future the performance of Trust Extended Authentication Mechanism can be improved by using a secure routing protocol for vehicular ad hoc networks by solving the inside attack.

## REFERENCES

[1] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security Privacy Mag., vol. 2, no. 3, pp. 49–55, May– Jun. 2004.

[2] Dedicated Short Range Communications (DSRC) [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[3] M. Nekovee and B. B. Bogason, "Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks," in Proc. IEEE Vehicular Technol. Conf., Apr. 2007, pp. 2486–2490.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 3, Issue 1, January 2014

[4] J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: A new data dissemination paradigm for vehicular ad hoc networks," IEEE Trans. Vehicular Technol., vol. 56, no. 6, pp. 3266–3277, Nov.2007.

[5] J.-F. Lee, C.-S. Wang, and M.-C. Chuang, "Fast and reliable emergency message dissemination mechanism in vehicular ad hoc networks," in Proc. IEEE Wireless Commun.Netw. Conf., Apr. 2010, pp. 1–6.

[6] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J.Comput. Security, vol. 15, no. 1, pp. 39–68, 2007.

[7] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proc. First Int. Workshop Wireless Netw. Intell. Transp. Syst., Aug. 2007, pp. 1–7.

[8] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Selected Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[9] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in Proc. IEEE Int. Conf. Commun., May 2008, pp. 1451–1457.

[10] M.-C. Chuang and J.-F. Lee, "KRM: Trust-extended authentication mechanism for vehicular ad hoc networks," in Proc. IEEE Int. Conf. Consumer Electron., Commun. Netw., Apr. 2011, pp. 1758–1761.

[11] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Provids location privacy for VANET," in Proc.ACM VANET, Sep. 2006, pp. 1–15.

[12] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, Apr. 2008, pp. 246–250.

[13] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, Apr. 2008, pp. 1229–1237.

[14] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," IEEE Wireless Commun., vol. 16, no. 4, pp. 16–22, Aug. 2009.

[15] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun.Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.

[16] G. Guette and C. Bryce, "Using TPMs to secure vehicular ad-hoc networks (VANETs)," in Proc. Int. Federation Informat. Process. May 2008, pp. 106–116.

[17] A. A. Wagan, B. M. Mughal, and H. Hasbullah, "VANET security framework for trusted grouping using TPM hardware," in Proc. IEEE Int. Conf. Commun. Software Netw., Feb. 2010, pp. 309–3012.

[18] NIST, U.S. Department of Commerce, "Secure Hash Standard," U.S.Federal Information Processing Standard (FIPS), Aug. 2002.

[19] The Network Simulator 2 (NS2) [Online]. Available: http://www.isi.edu/nsnam/ns.