An Effective and Secure User Authenticated Protocol for Location Services in Road Networks

Saima Kanwal

Department of Computer science Engineering

School of Optical, Electrical and Computer Engineering

University of Shanghai for Science and Technology

Shanghai, China

Chunxue Wu

Department of Computer science Engineering

School of Optical, Electrical and Computer Engineering

University of Shanghai for Science and Technology

Shanghai, China

Naixue Xiong

Department of Mathematics and Computer Science

Northeastern State University,

OK, USA

Abstract— **Road network is employed for exchanging the information among the vehicles where accidents and traffic information can be delivered, or receive services by an infrastructure. Although wireless communication systems yield an efficient traffic system and provide ease to the drivers, there is a chance of a traffic disturbance and risk to drivers through malicious information. So, there should be examined a way to limit the chance of an intermediate attack. This paper presents an efficient user based authentication protocol for location based services to secure address configuration for IPv6-based mix-zones over the road network. This protocol authenticates to inspect vehicles actions confidentially and have the following characteristics (1) Anonymous authentication: a message issuer can be authenticated. (2) Privacy: Communication content is confidential. The cost must be reduced through the address configuration scheme to improve the scalability. (3) Efficiency: it attains quick message verification, low storage requirements, and in case of a dispute, provides cost efficient identity tracking. Vehicles movement, the variation of velocity and distance are considered to maintain as many common users as possible by reducing the cost. The performance evaluation and cost analysis show that our framework can reduce the cost and gain outperformed results. This model can achieve reliability and efficiency with packet rate information. This user authenticated key establishment protocol has comparatively shorter time response, diminishes cost, less packet loss information and enhanced privacy preservation against malicious attacks compared with existing methods.**

Keywords—Location tracking, Authentication Key establishment protocols, security, LBSs

I. INTRODUCTION

The rapid development of vehicular technologies may apply new information and interconnection to improve the safety via vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [1]. Vehicular networks are also called Vehicular Ad Hoc Networks (VANETs), which are mostly used in Intelligent Transportation Systems (ITS) applications. In vehicular networks, the vehicles communicate with each other such as Inter-Vehicle Communication (IVC) and also with roadside base stations through a roadside unit. The vehicular networks provide safety for the users on the roads by providing timely information to the drivers. The vehicular network is a sub-class of mobile ad hoc networks (MANETs) and works on the same principle of mobile ad hoc networks (MANETs). In the early stage of 2000, MANET were one to one application but now a days VANETs have grown up in terms of inter-vehicle communication. VANET supports wide range of applications such as multi-hop message broadcasting over long distance and many other technologies that might uses UMTS, LTE, or WiMAX IEEE 802.16. For short range communication, it may use WLAN (either standard Wi-Fi), Bluetooth, Visible Light Communication and Infrared. Routing protocols in VANETs are significantly different from road networks, because various applications in VANET may have different QOS requirements for safe application. Broadcast routing in VANET is unlike from routing in road network due to various reasons such as rapidly changing network topology, wide range communication, and traffic pattern in different time and places. This may imply that conventional routing protocols for road network are not appropriate for most vehicular broadcast applications and they may also have different application requirements as compared to road network such as Infotainment applications, assistance co-operative awareness and Traffic efficiency management.

In VANETs each message need not to be verified and sent to the main server while on the other hand, in road networks every message must have to pass from main server and road side unit. These periodically broadcast messages are known as beacon messages. The content of beacon messages may include a vehicle's current position, velocity, and headway route. All the beacon messages have common requirements which are periodic broadcast and low latency. The beacon messages are useful for safety applications, for instance driver assistance, collision avoidance, and cruise control, etc. These applications require timely and correct information, and the typical beacon broadcast frequency, that might be in the range of 5-10 Hz [2]. The National Highway Trace Safety Administration (NHTSA) has identified and set down requirements for Intelligent Vehicle Safety Applications

Published by :

http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

[3]. Also, the work that would require V2V devices in latest vehicles in future has already   been started on a regulatory proposal. In contrast, in V2I architecture the mobile vehicles directly connect with infrastructures set up along roads for sending and disseminating packets [4].

In Mix-zone server, two classical address configuration protocols such as stateful protocol [5] and other is stateless and to achieve address configuration in the road networks is an important challenge. Various messages for road conditions, congestion avoidance and detour notification for road authorization can spread by VANETs [11-17]. The value-added services and traffic associated message delivered by road network are used to improve drivers' wayfaring capability, toll payment services and provide internet access navigation etc. To address above challenges, this manuscript has proposed an effective protocol and anonymous authentication scheme for road network. Our scheme has significant feature that may compared with existing methods; (i) An anonymous authentication, it provides content secrecy communication (ii) It accomplishes low storage requirements.

Following are our main contributions in this work:

(1)   We proposed location based routing protocol in road network to send data rapidly from the source vehicle to destination vehicle. A road network is an esteemed number of network gaps such as shortest paths, the average speed of the vehicles and the expected delay to transmit the data from one junction to another.

(2)   We establish a privacy preserving authentication protocol to verify the vehicle activities in a privacy preserving manner. We proposed a new method to adjust the vehicles speed which reduces the vehicle delay that might suffer from the network gap problem.

(3)   We proposed a novel vehicle orientated privacy preserving technique for road network services that is also proficient of protecting the Road side unit from attacks.

(4)   Vehicles moving trend, distance difference and velocity difference, are considered to maintain as many common users as possible to reduce the cost. The performance evaluation and cost analysis indicate that our framework can reduce the cost factor and gain good performance. With roadside unit server assistance, the proposed model can perform reliably.

II.   ADDRESS CONFIGURATION PROTOCOL

A.   Protocol's Structure

The road network consists of mobile vehicles and RSU (road side unit) in this protocol [19-26] communicating with Mix-zone server Internet over road side unit is shown in Fig. 1.

(5)   The road side unit can immediately decide which messages are trustworthy, and then send its opinion to neighbouring vehicles immediately. With the aid of road side unit server, vehicles can successfully increase decision accuracy while making decisions about the event messages.

(6)   The evaluation experiments based on NS-3 [18] to improve user's authenticated key establishment protocol , that have relatively shorter response time, reduce cost, less packet lost information and enhanced privacy preservation as compared with the proposed methods in [19] and [20].

Memon et al. [4] presented secure and effective Communication design with authenticated key establishment protocol for road networks. This proposed scheme is based on Mix-zone server (MZ$_s$) protocol and have achieved address configuration for users over the road network. Moreover, this scheme has achieved user communication security via authentication kind of road network. Considering some of these features; this work is totally different from our previous work [4] in terms of following aspects:

The system architectures are unlike the previous work. A road network is a special type of vehicular network, when a vehicle enters a new IP domain; its network prefix correspondingly changes. Therefore, the architecture in this scheme is based on multiple IP dynamics mix-zone server. In previous work, a road network is limited to one IP domain, so the network prefix of a mobile node keeps unchanged. The previous work based upon One IP domain.

The IPV6 address structure has changed. In this scheme, the network architecture is based on road segments and various junction concepts. In order to improve the performance and contribute to the hierarchical routing which is made up of RS ID and node ID. In previous work, the network architecture is based on the MIX-ZONE SERVER tree topology where a gateway node is the root. Correspondingly, an address consists of three parts that might be the global routing prefix, the gateway node ID and the node ID. This protocol simultaneously achieves the address configuration and address reclamation at the same time, therefore the extra cost and delay caused by the address reclamation is avoided.
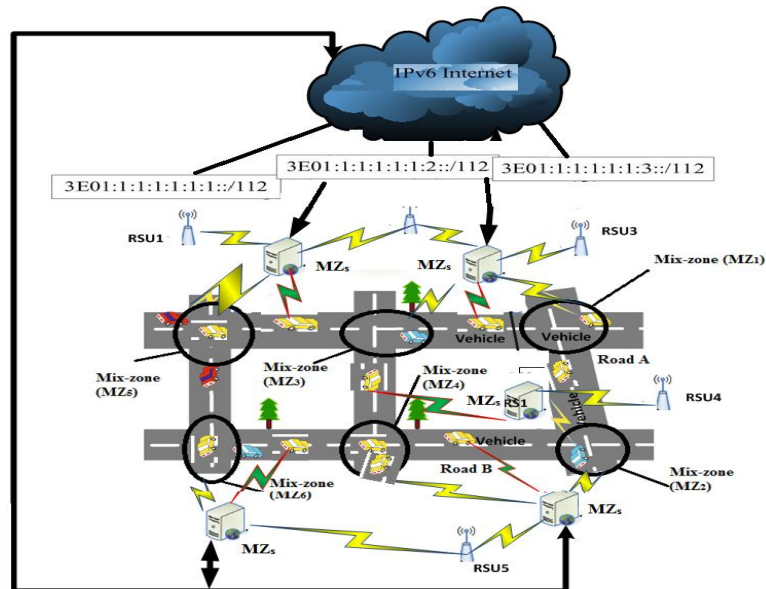
Fig. 1. Road network architecture.

B. Address Structure and address configuration algorithm

The address structure for road network based on the proposed architecture is presented in Table 1 and Table 2.

TABLE I. IPv6 address structure

(128-i)bits	i bits
RSU ID	Mobile vehicle ID

TABLE II. Notations

Notations	Descriptions	Notations	Descriptions
U_i	Mobile vehicle	p	a large prime
MZ_s	Mix zone server	‖	string concatenation
RSU_j	Road side unit	$\oplus$	XOR operation
ID_i	identity of mobile vehicle U_i	$\rightarrow$	message transmission
$RSUID_j$	identity of Road side unit	pw_i	password of U_i
r	master secret of MZ_s	$h()$	secure hash function
ST	Secret key between users and Mix-zones	s	server's secret key

1) Registration state

In registration state, as the user U_i wants to register with the MZ_s, it performs two steps with MZ_s.

Step:1 $\qquad U_i \circledR MZ_s : (IDi, h(PWi), h(\vartimes))$

The user U_i after freely choosing its password pw_i and identity ID_i performs an iris scan with a capture and generates a template MZ_s that describes the iris template of U_i. This protocol adopts iris as a characteristic since it is harder to be compromised in contrast to their characteristic information

such as fingerprint. Then, the user U_i selects a secure one-way hash function $h(\vartimes): \{0,1\}^* \circledR \{0,1\}^k$ and calculates $h(pwi)$, then it submits $\{ ID, ST, h(pwi), h(\vartimes) \}$ to the MZ_s through a secure channel.

Step:2 $\qquad MZ_s U_i \circledR U : (ID_i, h(PW_i), (\vartimes))$

After getting the information from the user U_i, MZ_s calculates the secret information and encrypts ID_i and ST via the server's secret key s to attain $T = E_s(ID P ST)$. Then, it conveys this smart card to the user U_i in a safe method in fig.2. The user U_i preserves the password pw_i, the identity ID and the smart card confidentially for the authentication manner Case 1. Logging in for the first time, as shown in Fig.3 and Fig.4. Case 2. On a following login, as shown in Fig.5 and Fig.6.

2) First time login state

Step:1
$$Qj1 = T_{rj}(x) \bmod p, \quad Qj2 = T_{rj}(Q) \bmod p,$$
$$Y1 = h(Qj2), \quad Y2 = h(Qj1 P Qj2 P Qi1 P Y1 P X2 // Bj).$$

Step:2 $\qquad MZ_s \circledR RSUj \ \{Qi1 \ X1, X2, Qj1, Y1, Y2\}$

$MZ_s \circledR sends \ \{Qi1, X1, X2, Qj1, Y1, Y2\} to the RSUj \ (RSUj).$

3) First-time login Authentication and key agreement state

Step:1 $\qquad \{Qi1, X1, X2, Qj1, Y1, Y2\},$

Published by :

http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

The MZ_s computes

$$Qi2*° \ T_r(Q_{i1})mod \ p, IDi* \ = h(Qi2*)\text{Å} \ X1, \ Ai* = h(IDi*//r),$$

$$Qj2* \equiv T_r(Q_{j1})mod \ p, RSUIDj* \ = h(Qj2*)\oplus Y1, \ Bj* = h(RSUIDj*),$$

Step 2:

The MZ_s checks if

$$X2 = h(Ai*\text{P}RSUIDjPQi1PQi2*\text{P}X1), Y2 = h(Qj1PQj2*PQi1PY1PX2//Bj*).$$

$$Zi = h(Qi1PQj1PRSUIDj*PAi*PX2), Zj \ = h(Bj*PQi1PQj1//Zi).$$

Step:3 $\qquad MZ_s \ ® \ RSUj : \ \{Zi, Zj \}$

Step:4 $\qquad RSUj \ ® \ MZ_s : \ \{Qj1, Rj, \ CIDi, t, R \}$

Step:5

The smart card first computes:

$$Zi* = h(Qi1PQj1PRSUIDjPAiPX2)$$

and checks whether

$$Rj = h(\ Zi*//T_{r_i}(Q_{j1}\ )PCIDiPtPR\ )$$

$$Ri \ = h(\ RSUIDjPQi1PQj1PVPT_{r_i}(Q_{j1}\ ), d = h(RSUIDj\ P \ pwiPIDi//t)\text{Å}V$$

and stores

$$\{RSUIDj, d, CIDi, t\}$$

$$SK = h(T_{r_i}(Q_{j1})PRSUIDj)$$

(1) Select a random number N
$d_0 = h \ (pw_i||ID_i) \oplus N$

(IDi, h(PWi), h(.))

(2) $\ c = h(ID_i||r) \oplus d_0$
Store $\{c, x, p, Q, h ()\}$ to
a smart card

Smart card

(3) $d_1 = c \oplus N$
$\quad d_2 = h(ID_i||pw_i)$
$\quad$ Replace c with
$\{d_1, d_2\}$

Fig. 2. Registration state.

(1) Check if $h(ID_i||pw_i) = d_2$

(2) $A_i = d_1 \oplus h(pw_i||ID_i)$
$Q_{i1} \equiv T_x(x) \ mod \ p$
$Q_{i2} \equiv T_r(Q) \ mod \ p$
$X_1 = h(Q_{i2}) \ominus ID_i$
$X_2 = h(A_i||RSUID||Q_{i1}||Q_{i2}||X_1)$

(3) $\{Q_{i1}, X_1, X_2\}$

(4) $Q_{j1} \equiv T_r(x) \ mod \ p$
$Q_{j2} \equiv T_r(Q) \ mod \ p$
$Y_1 = h(Q_{j2}) \ominus RSUID_j$
$Y_2 = h(Q_{j1}||Q_{j2}||Q_{i1}||Y_1||X_2||B_j)$

(5) $\{Q_{i1}, X_1, X_2, Q_{j1}, Y_1, Y_2\}$
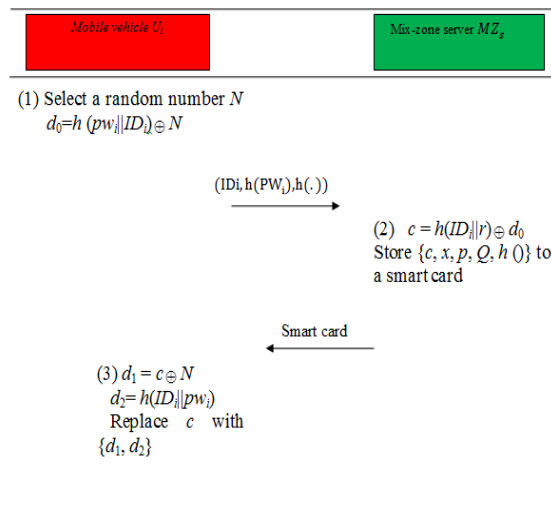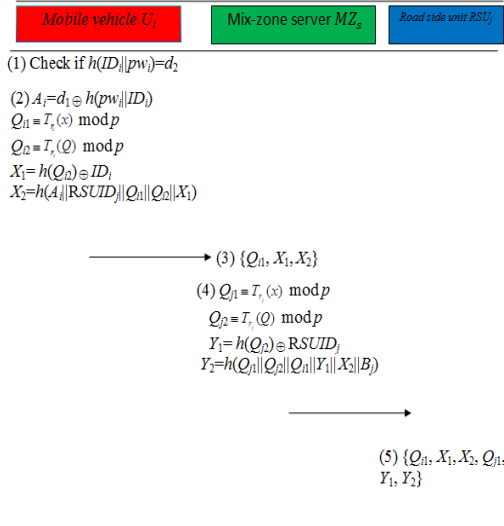
Fig. 3. First time login state.

Step:7 $\qquad U_i \ ® \ MZ_s : \{MZ_s \}$

The card sends

$\qquad \{ MZ_s \}$ to the $RSUj$.

Step:8 $\quad Ri = h\big(RUSIDjPQi1PQj1Ph(CIDiPBj//t)//T_{r_j}(Q_{i1})\big)$

(1) $Q_{i2}* \equiv_{T_r(Q_{i1})} mod \ p$
$ID_i* = h(Q_{i2}*) \oplus X_1$
$A_i* = h(ID_i*||r)$
$Q_{j2}* \equiv_{T_r(Q_{j1})} mod \ p$
$SID_j* = h(Q_{j2}*) \oplus Y_1$
$B_j* = h(r||SID_j*)$

(2) $X_2 = h(A_i*||RSUID_j*||Q_{i1}||Q_{j2}*||X_1)$
$Y_2 = h(Q_{j1}||Q_{j2}*||Q_{i1}||Y_1||X_3||B_j*)$
$Z_i = h(Q_{i1}||Q_{i1}||SID_j*||A_i*||X_2)$
$Z_j = h(B_j*||Q_{i1}||Q_{i1}||Z_i)$

(3) $\{Z_i, Z_j\}$

(4) $Z_j = h(B_j||Q_{i1}||Q_{i1}||Z_i)$
$R = h(CID_i||B_j||t) \oplus h(T_{r_j}(Q_{i1}))$
$R_j = h(Z_i||T_{r_j}(Q_{i1})||CID_i||t||R)$

(5) $\{Q_{j1}, R_j, CID_i, t, R\}$

(6) $Z_i* = h(Q_{i1}||Q_{i1}||RSUID_j||A_i||X_2)$
$R_j = h(Z_i*||T_{r_i}(Q_{j1})||CID_i||t||R)$
$V = R \oplus T_{r_i}(Q_{j1})$
$R_i = h(SID_j||Q_{i1}||Q_{i1}||V||T_{r_i}(Q_{j1}))$
$d = h(SID_j||pw_i||ID_i||t) \oplus V$
$SK = h(T_{r_i}(Q_{j1})||SID_j)$

(7) $\{R_i\} = h(T_{r_i}(Q_{i1})||SID_j)$

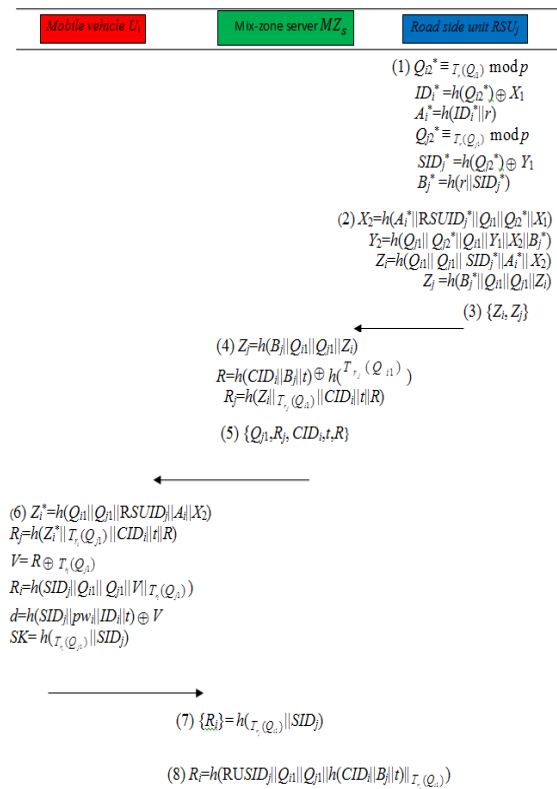(8) $R_i = h(RUSID_j||Q_{i1}||Q_{i1}||h(CID_i||B_j||t)||T_{r_j}(Q_{i1}))$

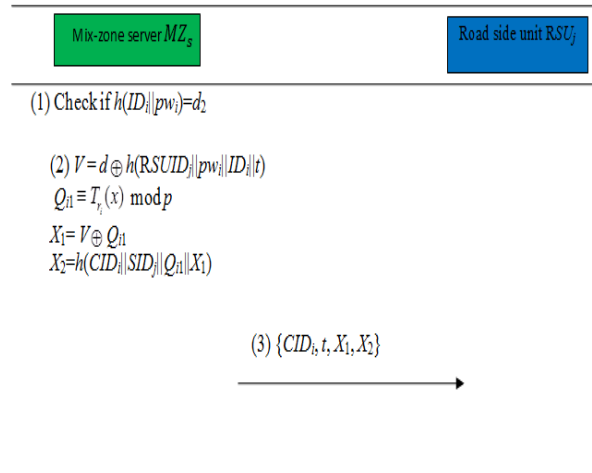Fig. 4. First-time login Authentication and key agreement state
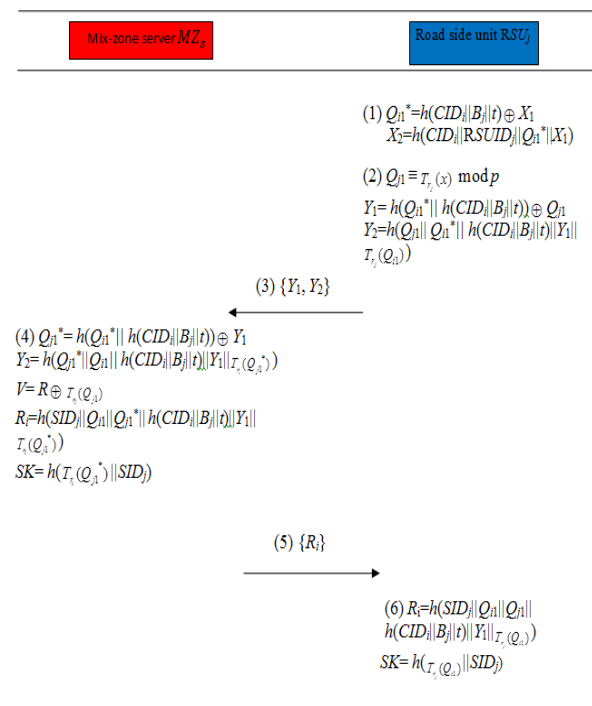
Fig. 5. Consequent login state

Fig. 6. Consequent login Authentication and key agreement state

4) Consequent login Authentication and key agreement state

Step 1. On the reception of request message $\{CID_i, t, X_1, X_2\}, MZ_s$ primarily checks if t is valid. Then, if it is valid, MZ_s computes $Q_{i1}^* = h(CID_i \,//\, B_j \,//\, t) \text{\AA} X_1$. Then RSU_j checks whether

$$X_2 = h(\, CID_i \,//\, RSUID_j \,//\, Q_{i1}^* \,//\, X_1\,).$$

Step:2 $Q_{j1} \circ T_{r_j}(x) \bmod p, Y_1 = h(Q_{i1}^* \,//\, h(CID_i \,//\, B_j \,//\, t)) \text{\AA} Q_{j1},$

$$Y_2 = h(\, Q_{j1} \,//\, Q_{i1}^* \,//\, h(CID_i \,//\, B_j \,//\, t)) \,//\, Y_1 \,//\, T_{r_j}(Q_{i1})\,).$$

Step:3 $RSU_j \circledR_i MZ_s i : \{Y_1, Y_2\}$

Step:4 The smart card initially calculates

$$Q_{j1}^* = h(Q_{i1}^* \,//\, h(CID_i \,//\, B_j \,//\, t)) \text{\AA} Y_1$$

and checks whether

$$Y_2 = h(\, Q_{j1}^* \,//\, Q_{i1} \,//\, h(CID_i \,//\, B_j \,//\, t)) \,//\, Y_1 \,//\, T_{r_i}(Q_{j1}^*)\,)$$

If case of above equality, the smart card calculates

$$V = R \text{\AA} T_{r_i}(Q_{j1}),$$

$$R_i = h(\, RSUID_j \, P Q_{i1} \, P Q_{j1} * P h(CID_i \, P B_j \, P t) PY_1 \, PT_{r_i}(Q_{j1}^*)).$$

Lastly, the card calculates the session key

$$SK = h(T_{r_i}(Q_{j1}^*)) \, P RSUID_j\,)$$

Step:5 $MZ_s \circledR RSU_j : \{R_i\}$

Step: 6 the service MZ_s checks whether the equality holds

$$R_i = h(\, RSUID_j \,//\, Q_{i1} \, P Q_{j1} \, P h(CID_i \,//\, B_j \,//\, t)) \,//\, Y_1 \, P T_{r_j}(Q_{i1}) \, JT_{r_j}(Q_{i1})\,)$$

5) Password Change Phase

Then the smart card computes

$$d_1^{new} = d_1 \text{\AA} h(pw_i \,//\, ID_i) \text{\AA} h(pw_i^{new} \,//\, ID_i), d_2^{new} = h(ID_i \,//\, pw_i^{new})$$

and replaces

$\{d_1, d_2\}$ with $\{d_1^{new}, d_2^{new}\}$.

III. SECURITY ANALYSIS

This protocol restrains the malicious attacks associated to the dynamic address configuration and hold the security.

A. Address forgery Attack

Using this protocol, a mobile vehicle attains a unique address with no replicate address detection. If any malicious mobile vehicle takeoffs the address of a real mobile vehicle to spread a wrong message (for instance, a replicate location detection message), firstly the message will be delivered to its nearby mobile vehicles. As the malicious mobile vehicle is not authenticated by the nearby vehicles, they reject the wrong message. Hence, the wrong message is restricted. Similarly, if a malicious mobile vehicle try to interact with a real mobile vehicle by taking an address, then the real mobile vehicle will obstruct the interaction with that vehicle since the malicious mobile vehicle is not authenticated [20].

B. Address Exhaustion Attack

When a malicious mobile vehicle request for an address from a nearby mobile vehicle or roadside, its request is declined as the malicious mobile vehicle or roadside is not authenticated.

1) Fake address conflict attack

If an address conflict message is broadcasted by any malicious mobile vehicle, then this message is firstly received by the nearby mobile vehicles and they abandon this address conflict message as they cannot authenticate the malicious

mobile vehicle. Furthermore, this protocol gains the address configuration with no replicate address detection, so to certify an assigned address' distinctiveness, it does not apply an address conflict message. So, this could be easily authenticated by any mobile vehicle that the received address conflict message is from a malicious mobile vehicle. Hence the streaming of a fake address message is avoided.

2) Replay Attack

When a good vehicle X, sends an encrypted address request message, a malicious node interrupts it and again sends the same message to a vehicle Y to ask for an address to exhaust the address resources and occupy network resources. After Y receives the encrypted address request message, it can abandon this message as in this message the time stamp is expired. A malicious node interrupts the encrypted address response message from a good vehicle Y and again sends the same encrypted address response message to another node X and causes the address conflict. When X receives this encrypted address response message, it can discard this message because it cannot decrypt the encrypted address response message through its secret key. Hence, the replay attack is prevented.

IV. PERFORMANCE EVALUATION

The previous methods [19, 21-26] are designated to make a comparison with our method because of the following reasons in Table 3, Table 4 and

TABLE III.   Compare reasons

Methods	Storage overhead	Anonymity	Traceability	Authentication	Confidentiality	RSU-aided	Assumption
X.wang [19]	Low	✓	✓	✓	✓	✗	Normal
B.J Chang [21]	Low	✓	✓	✓	✗	✗	Normal
Chen, Y.-S [22]	High	✓	✓	✓	✓	✗	Normal
T.hwang,P. Gope[23]	Low	✓	✗	✓	✗	✗	Normal
R. Kumar, M. Dave [24]	Low	✓	✓	✓	✗	✗	Strong
Xiaonan [25]	High	✓	✓	✓	✗	✗	Normal
B. Ying [26]	Low	✓	✓	✓	✗	✓	Normal
Our proposed protocol	Low	✓	✓	✓	✓	✓	Normal

TABLE IV.   Efficiency comparisons of our scheme and the other related schemes [19, 22]

	Our Scheme	X. Wang [19]	Chen, Y.-S[22]
Authorization phase	$4T_{xor}+3T_{hash}+2T_{asym}+2$ random number	$4T_{xor}+4T_{sym}+13T_{exp}+6$ random number	$2T_{asym}+1T_{hash}+2$ random numbers
Access service phase	$5T_{xor}+6T_{hash}+3T_{asym}+3$ random number	$4T_{exp}+4T_{sym}+4$ random numbers	$4T_{asym}+4T_{hash}+2T_{sym}+6$ random numbers
Computational cost	$\approx 500\ T_{sym}$	$\approx 1028T_{sym}$	$\approx 602T_{sym}$
Computational time	4.35	6.42	5.7

We have given a brief comparison of our scheme and the other prevailing schemes in terms of performance metrics which are important in road network authentication protocol, i.e., Authorization phase, Access service phase, computational cost, and computational time as shown (Table 4). In our experiments, to simulate a practical situation, the mobile vehicle are installed on two PCs in a local area network. In the registration phase, the presented scheme needs one hash operation to calculate $d_0=h(pw_i||ID_i) \oplus N$ on user side, needs one road side unit point multiplication operation and one modular inversion operation to obtain $d_1=c \oplus N$, $d_2=h(ID_i||pw_i)$, and needs one symmetric encryption operation to calculates $A_i=h(ID_i||r)$, $c=A_i \oplus d_0$ on the road side unit. While in authentication phase user side requires four scalar point multiplication operations to compute $Vrh(PW)P$ and $W=rR$; three hash operations to calculate $h(ST)$, u $Auth$ and SK; one symmetric encryption operation to find Z and one symmetric decryption operation to decrypt message $Auths$. The MIX-ZONE SERVER requires two symmetric decryption operations to decrypt message $\{R_i\}$ and [1], one symmetric encryption operation to calculate $Auths$; one elliptic curve scalar point multiplication operations to calculate V; and two hash operations to get $Authu$ and SK. Thus, the whole execution time of the computational time (s) is calculated as 4.35. As an evident of Table 4, our protocol has outperformed other protocols. It is renowned evidence that the symmetric encryption/decryption operation and the hash function operation hold the same computational cost. Consequently, the Computational cost of our proposed protocol, regarding the hash function operations, is more efficient as compared to other protocols.

V. CONCLUSION AND FUTURE WORK

In this paper, we put forward an Improved User's Authenticated Key Establishment Protocol for Road Networks. We establish a privacy preserving authentication protocol to verify the vehicle activities in a privacy preserving manner. We proposed a new method to adjust the vehicles speed which reduces the vehicle delay which might suffers from the network gap problem. We proposed a novel vehicle orientated privacy preserving technique for road network services that is also proficient of protecting the Road side unit from attacks. The road side unit can immediately decide which messages are trustworthy, and then send its opinion to neighbouring vehicles immediately. With the aid of road side unit server, vehicles can successfully increase decision accuracy while making decisions about the event messages.

The evaluation experiments based on NS-3 [18] to improve user's authenticated key establishment protocol have proved that our protocol has comparatively shorter response time, diminish cost, less packet lost information and better privacy preservation as related to those proposed in [19] and [20].

In future work, we will propose authentication with handover process using IPV6 protocol for 4G LTE cellular networks to reduce the computational cost, faster process, less steps (it is implementable with IPv6 protocol probably the quickest way is a listing of command, it will shows crypto)

scheme by the future proposed scheme, the overall system complexity is able to be reduced.

ACKNOWLEDGMENTS

CONFLICT OF INTEREST

The author declares that there is no conflict of interest regarding the publication of this paper.

REFERENCES

[1] J. C. Mukherjee, S. Agarwal, and A. Gupta, "Distributed event notification in VANET with multiple service providers," in *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems*, 2014, pp. 334-337.

[2] Z. Chen, Y. Liu, R. C.-W. Wong, J. Xiong, G. Mai, and C. Long, "Efficient algorithms for optimal location queries in road networks," in *Proceedings of the 2014 ACM SIGMOD international conference on Management of data*, 2014, pp. 123-134.

[3] I. Memon, K. Domenic, H. Memon, R. Akhtar, W. Yong, and F. Zhang, "Rumor riding: An anonymity approach for decentralized peer to peer systems," *Wireless personal communications,* vol. 79, pp. 647-660, 2014.

[4] M. Alsabaan, W. Alasmary, A. Albasir, and K. Naik, "Vehicular Networks for a Greener Environment: A Survey," *IEEE Communications Surveys and Tutorials,* vol. 15, pp. 1372-1388, 2013.

[5] N. Moore, "Optimistic duplicate address detection (DAD) for IPv6," 2006.

[6] A. K. Das, "A secure and effective biometric- based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *International Journal of Communication Systems,* 2015.

[7] U. Ghosh and R. Datta, "A secure dynamic IP configuration scheme for mobile ad hoc networks," *Ad Hoc Networks,* vol. 9, pp. 1327-1342, 2011.

[8] A. X. Liu and A. R. Khakpour, "Quantifying and verifying reachability for access controlled networks," *IEEE/ACM Transactions on Networking (TON),* vol. 21, pp. 551-565, 2013.

[9] I. Memon, M. R. Mohammed, R. Akhtar, H. Memon, M. H. Memon, and R. A. Shaikh, "Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC)," *Wireless personal communications,* vol. 79, pp. 661-686, 2014.

[10] X. Wang and Y. Mu, "A secure IPv6 address configuration scheme for a MANET," *Security and communication networks,* vol. 6, pp. 777-789, 2013.

[11] Y. S. Jeong, J. S. Park, and J. H. Park, "An efficient authentication system of smart device using multi factors in mobile cloud service architecture," *International Journal of Communication Systems,* vol. 28, pp. 659-674, 2015.

[12] I. Memon, L. Chen, A. Majid, M. Lv, I. Hussain, and G. Chen, "Travel recommendation using geo-tagged photos in social media for tourist," *Wireless Personal Communications,* vol. 80, pp. 1347-1362, 2015.

[13] H. Shin, E. Talipov, and H. Cha, "Spectrum: lightweight hybrid address autoconfiguration protocol based on virtual coordinates for 6LoWPAN," *IEEE Transactions on mobile computing,* vol. 11, pp. 1749-1762, 2012.

[14] N. Škoberne, O. Maennel, I. Phillips, R. Bush, J. Zorz, and M. Ciglaric, "IPv4 address sharing mechanism classification and tradeoff analysis," *IEEE/ACM Transactions on Networking,* vol. 22, pp. 391-404, 2014.

[15] H.-M. Sun, C.-H. Chen, C.-W. Yeh, and Y.-H. Chen, "A collaborative routing protocol against routing disruptions in MANETs," *Personal and ubiquitous computing,* vol. 17, pp. 865-874, 2013.

[16] E. Talipov, H. Shin, S. Han, and H. Cha, "A lightweight stateful address autoconfiguration for 6LoWPAN," *Wireless Networks,* vol. 17, pp. 183-197, 2011.

[17] M. Won and R. Stoleru, "A low-stretch-guaranteed and lightweight geographic routing protocol for large-scale wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 11, p. 18, 2014.

[18] D. Mishra, A. Chaturvedi, and S. Mukhopadhyay, "Design of a lightweight two-factor authentication scheme with smart card revocation," *Journal of Information Security and Applications,* vol. 23, pp. 44-53, 2015.

[19] X. Wang, Y. Mu, G. Han, and D. Le, "A secure IPv6 address configuration protocol for vehicular networks," *Wireless personal communications,* vol. 79, pp. 721-744, 2014.

[20] X. Wu, K. N. Brown, C. J. Sreenan, P. Alvarez, M. Ruffini, N. Marchetti, *et al.*, "An XG-PON module for the NS-3 network simulator," in *Proceedings of the 6th International ICST Conference on Simulation Tools and Techniques*, 2013, pp. 195-202.

[21] B.-J. Chang, Y.-H. Liang, and H.-J. Yang, "Performance analysis with traffic accident for cooperative active safety driving in VANET/ITS," *Wireless personal communications,* vol. 74, pp. 731-755, 2014.

[22] Y.-S. Chen, C.-S. Hsu, and W.-H. Yi, "An IP passing protocol for vehicular ad hoc networks with network fragmentation," *Computers & Mathematics with Applications,* vol. 63, pp. 407-426, 2012.

[23] T. Hwang and P. Gope, "Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time Secrets," *Wireless Personal Communications,* vol. 77, pp. 197-224, 2014.

[24] R. Kumar and M. Dave, "A framework for handling local broadcast storm using probabilistic data aggregation in VANET," *Wireless personal communications,* vol. 72, pp. 315-341, 2013.

[25] W. Xiaonan and Z. Shan, "An IPv6 address configuration scheme for wireless sensor networks based on location information," *Telecommunication Systems,* pp. 1-10, 2013.

[26] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *Journal of Network and Computer Applications,* vol. 36, pp. 1352-1364, 2013.

Saima Kanwal received the B.E. degree in Electronic Engineering from Islamia University of Bahawalpur, Pakistan, in 2012. Now she is working toward the Master's degree in the computer application technology, The University of Shanghai for science and technology, Shanghai, China. Her research interests include wireless sensor networks, and fiber optics.

Chunxue Wu (1964-) received the Ph.D. degree in Control Theory and Control Engineering from China University of mining and technology, Beijing, China, in 2006.He is a Professor with the Computer Science and Engineering and software engineering Division, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, China. His research interests include, wireless sensor networks, distributed and embedded systems, wireless and mobile systems, networked control systems.

Neal N. Xiong is current an Associate Professor (3rd year) at Department of Mathematics and Computer Science, Northeastern State University, OK, USA. He received his both PhD degrees in Wuhan University (about sensor system engineering), and Japan Advanced Institute of Science and Technology (about dependable sensor networks), respectively. Before he attended Northeastern State University, he worked in Georgia State University, Wentworth Technology Institution, and Colorado Technical University (full professor about 5 years) about 10 years. His research interests include Cloud Computing, Security and Dependability, Parallel and Distributed Computing, Networks, and Optimization Theory.

Dr. Xiong published over 280 international journal papers and over 120 international conference papers. Some of his works were published in IEEE JSAC, IEEE or ACM transactions, ACM Sigcomm workshop, IEEE INFOCOM, ICDCS, and IPDPS. He has been a General Chair, Program Chair, Publicity Chair, PC member and OC member of over 100 international conferences, and as a reviewer of about 100 international journals, including IEEE JSAC, IEEE SMC (Park: A/B/C), IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, IEEE Trans. on Parallel and Distributed Systems. He is serving as an Editor-in-Chief, Associate editor or Editor member for over 10 international journals (including Associate Editor for IEEE Tran. on Systems, Man & Cybernetics: Systems, Associate Editor for Information Science, Editor-in-Chief for Journal of Internet Technology (JIT), and Editor-in-Chief for Journal of Parallel & Cloud Computing (PCC)), and a guest editor for over 10 international journals, including Sensor Journal, WINET and MONET. He has received the Best Paper Award in the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08) and the Best student Paper Award in the 28th North American Fuzzy Information Processing Society Annual Conference (NAFIPS2009).

Dr. Xiong is the Chair of "Trusted Cloud Computing" Task Force, IEEE Computational Intelligence Society (CIS), http://www.cs.gsu.edu/~cscnxx/index-TF.html, and the Industry System Applications Technical Committee, http://ieee-cis.org/technical/isatc/; He is a Senior member of IEEE Computer Society,