World Engineering & Applied Sciences Journal 8 (1): 01-06, 2017
ISSN 2079-2204

DOI: 10.5829/idosi.weasj.2017.01.06

A Locked and Privacy Aided Navigation in Vehicular Adhoc Networks

A. Samydurai, B. Vanathi, C. Pabitha and D Sakthi suganya

Department of Computer Science and Engineering,
Valliammai Engineering College, SRM Nagar, Kattankulathur- 603203, India

Abstract: VANET has been a most important or hot research area in the last few years due to its unique characteristics. The characteristic that portrays VANET are high dynamic topology, predictable mobility. It grabs the interest on both academic and industry wise. VANET is an emerging technology that is aimed to achieve road safety, privacy preserving verifications, secure date dissemination, traffic status information will be provided regularly and it is shared among drivers. When a vehicle is involved in any event or accident zone of forewarning message, the certificate authority should recover the actual identity of this vehicle. To agreement with this concern, we propose a novel privacy-preserving authentication protocol with authority traceability.

Key words: VANET · LPP · Information dissemination · Private key distribution · Secure data

INTRODUCTION

At present cars and other private vehicles are used daily by many people. Due to increased use of private transport increases the accidents and thus there is increase in fatalities. VANET provides a wireless communication between vehicle to vehicle and vehicle to roadside unit. When it comes to vehicle to vehicle communication the VANET switches to MANET which allows the vehicle to share a reliable communication between them. The communication between the vehicles and road side unit will give the information on the accident prevention, post-accident investigation or traffic jams. A comprehensive survey on the vehicular ad-hoc network will provide us to know about the aspects and challenges related to this field (VANET) which covers issues like network architecture, communication domains, challenges, applications and simulation tools. VANET differs from MANET by its architecture, challenges, characteristics and applications. VANET improves road safety and travelers comfort. Thus, aspects related to VANET are being taught with referring other relevant papers to simulate VANET protocols and applications. The fig 1, the VANET architecture tells us about the performance of the overall simulation. The role of three major nodes are being explained, 1) the certificate authority, 2) On Board Unit (OBU) and 3) the Road Side Unit (RSU). However, the development of VANETs architecture varies from region to region, CAR-2-CAR communication consortium is little different from reference architecture. The CA holds the real identity of both the road side unit and on board unit where OBU's certificate information is reported to CA. Thus it is clear that CA plays the major role in authorization. After the registration is done by CA and the key is distributed to both RSU and OBU.CA tracks the information and sends to the OBU. RSU publishes the private key to the OBU so that it can be informed to the user that

The main aim of the proposed paper is to achieve a privacy-preserving authentication protocol with authority traceability 1) mutual and anonymous authentication for both vehicle-to-vehicle and vehicle-to-roadside communications, 2) vehicle unlink ability, 3) authority tracking capability and 4) high computational efficiency. For privacy preserving we use LPP (Long term evolution-Positioning Protocol) protocol which is only applicable for mobiles and on board units. This helps the RSU and OBU to communicate securely. The LPP protocol will inform the certificate authority to know the registered units on it and to give the authorization to get information requested for. We propose a secure vehicular network model with the types of network entities that are specified as follows: the certificate authority (CA), the fixed RSUs at the road side and the mobile OBUs equipped on the running vehicles.

Corresponding Author: A. Samydurai, Department of Computer Science and Engineering, Valliammai Engineering College, SRM Nagar, Kattankulathur- 603203, India.

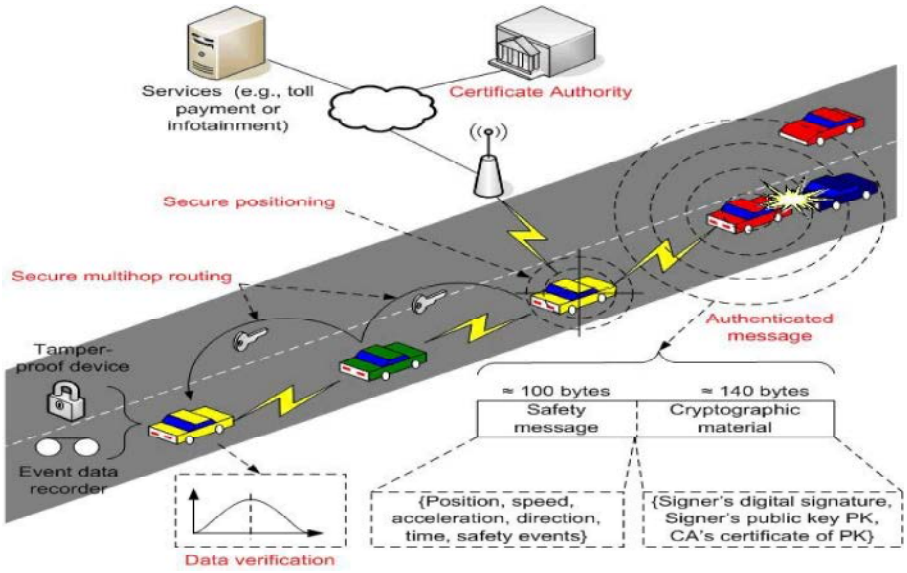

Fig. 1: VANET Architecture

The CA acts as registration and certification center for both RSUs and OBUs with unlimited computation and storage capability. Only the CA can have the real identity of an OBU from its certificate. RSU works as an intermediary between OBU and CA in a semi-trusted way. They are responsible for filtering fake messages from malicious or revoked vehicles and reporting OBU's certificate information to CA. OBUs regularly broadcast routine traffic-related status information to help users with a better awareness of their vehicular movement environment.

Related Works: The author has proposed a new routing approach namely RAR (Roadside-Aided Routing) which is the first to exploit the affiliation method on roadside units based on road constraints [1]. Today's communication via wireless mode in vehicular environment consists of safe communication that cannot tolerate long connection establishment delays. Mainly before establishing a connection with other vehicles. It also consists of another application namely road map update to track a car in the particular locality [2]. In this paper, the author puts forth the idea of an efficient conditional privacy preservation protocol. This protocol provides secure messages with authorized traceability to overcome issues on anonymous authentication. This protocol is attributed with on-the-fly short short-board units (OBUs) and roadside units (RSUs) to enable fast anonymous authentication and privacy tracking [3]. In this paper, the author has discussed security of the vehicular networks with detailed threat analysis and security architecture. A security protocol has been provided to ensure privacy, robustness and efficiency [4]. In this paper, the author has adopted a new scheme to settle issues on large parking lots. a real-time parking navigation service, intelligent anti-theft protection and friendly parking information dissemination has been provided to drivers in order to provide an efficient service[5]. In this paper, the author has proposed a technique called mutual authentication and key agreement scheme for V2I communications with increased security and privacy protection from a common driver's view. This scheme is useful in analyzing security and performance to enhance practical use[6]. The author has addressed certain challenges such as large overhead and latency. A hybrid scheme HASVC has been used to address the authentication issue and performance evaluation in order to meet the requirements of vehicular communication [7]. The author has discussed two countermeasures on signature flooding, namely, Fast Authentication (FastAuth) and Selective Authentication (SelAuth), FastAuth secures periodic single-hop beacon messages thereby enabling faster verification through Elliptic curve Digital Signature Algorithm. Wherein, SelAuth secures multi-hop applications[8]. The traffic-related status information with be provided periodically to the drivers to enhance driver's safety. In order to ensure security and privacy guarantee, the author has proposed a new privacy-preserving authentication protocol using elliptic curve based chameleon hashing. Hence mutual and anonymous authentication, unlinkability, authority tracking capability and high efficiency[9]. The author had

introduced a concept called chameleon signature where the privacy of the contents of the signed information is concealed from the third party including the recipient. Hence chameleon hash functions are made use of. Chameleon hashing is constructed based on standard cryptographic assumptions wherein chameleon signatures use digital signatures[10]. In this paper, The author has proposed the first identity- based chameleon hash functions based on hash-and-sign paradigm. In this scheme, the owner of the public key need not necessarily acquire the associated secret key wherein a id-based chameleon signature and a novel sealed-bid auction scheme is used[11]. The author has proposed an innovative technique to improve road safety and motor traffic efficiency through Intelligent Transport Systems(ITS). Various improvements have been made in the field of wireless communication through various VANET application areas like vehicle crash warning and traffic information spreading. Furthermore applications of VANETs have also been discussed [12]. The author has proposed a handover authentication scheme using credentials based on chameleon hashing with the main aim of providing robust security and efficiency. In this scheme, an authenticated ephemeral Diffie-Hellman key exchange occurs between a mobile node and an access point without any communication with the authentication server[13].

Vanet Methodologies: Now a days due to increase in private vehicles on road, accidents are increased which leads to increase in fatalities. Thus to reduce this big problem VANET is used to communicate with the user on the traffic status,vehicular and object movement that informs on the event of forewarning or post-warning too. The modeling of the application is mainly based on three units they are Certificate Authority (CA), Road Side Unit (RSU) And On Board Unit (OBU). Road safety and travellers comfort are enhanced by providing this model of communication dissemination. The on board unit will receive the information on the status of drive, traffic and event that may happen or that had happened to the user. The information is provided by the provider RSU and the information is used by the user OBU where the information is displayed to the user by OBU and got from RSU.

Here CA is the registration and certification center for RSU and OBU which gives virtually unlimited computation and storage capabilities.RSU works as an intermediary for OBU and CA thus filters the fake messages from malicious or revoked vehicles.OBU gives the information about the vehicular, traffic and object oriented movements to the user. RSU works as an intermediary in a semi-trusted way. The CA will hold all information of OBU and RSU thus it gives unlimited computation virtually and even storage capabilities. The real identity of both RSU and OBU is taken over by CA as well. OBU's certificate information is reported to CA. CA takes advantage on RSU and OBU. OBU uses the services provided and broadcasts the routine traffic status to help the users.

In the fig 2, use case diagram is used in representing the vehicle link ability by showing the four actors OBU, RSU, CA and neighbor node (optional) and the process it does. The report of the OBU is obtained by the CA with the help of RSU. RSU and OBU registers on CA where registration is done by CA and the key is distributed to both. CA tracks the information and forwards it to OBU. RSU publishes the private key to the OBU so that it can inform the user about the traffic status, vehicular and object movement. The private key which holds the information about the traffic analysis is spread to the neighbor nodes by exchanging private key. The coverage of traffic and vehicular movement information are done by RSU and thus it is disseminated to both OBU as well as neighbor node and thus they communicate

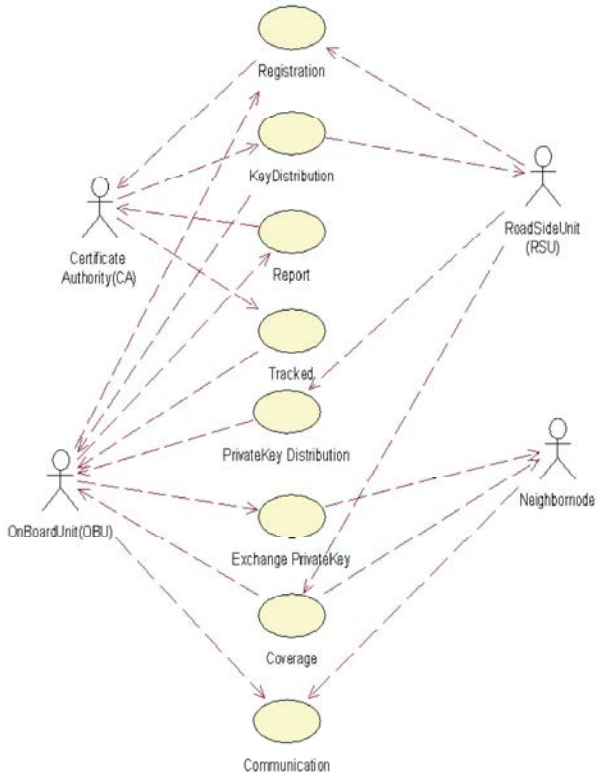

Fig. 2: Vehicle Link Ability Diagram

Simulation Results: As shown in fig 3, information on RSU and OBU are stored, tracked and shared. Certificate authority is the page where all information about RSU and OBU are registered and provided. The real identity of the RSU and OBU are illustrated. In this page certificate authorization for both OBU and RSU are maintained and thus certified. In OBU the vehicle number, node id, node name are stored to know about the particular vehicle or the neighbor nodes too. In RSU the node id, node name, node imp and distance are specified and noted to get the traffic status, vehicle and object movement information. Thus the certificate authority works. Here both on board unit and roadside unit are tracked with the help of the sensor that has a particular range analysis to indicate the activities that happens during boarding. It not only intimates only one on board unit but also intimates all the other neighbor nodes to be aware of the event happened or happening. The LPP protocol that we use gives the authorized and secured way of communication between the three important terminals. They behave as the access list specified for the certificate authority which has the real identity of the nodes that are communicating on board. The inappropriate spread of beacon messages are limited to have a safe and secure communication between the providers and users with the help of Long term evolution-positioning protocol (LPP). We use Computational Daffier Hellman (CDH) technique which is harder to break. This CDH algorithm is used to have the private key securely with only the authenticated units. The OBU and RSU exchanges the private key for authentication purpose and these even are monitored by the LPP protocol where the LPP protocol is mainly runs on the basis of computational daffier Hellman technique, the computational daffier Hellman technique is mainly used to have the secured interaction and to preserve private keys from eavesdroppers. From the consideration of the cyclic group C of order q the C^{row} can be calculated by accessing the generator C and the random ones C^r and C^o, C^{row} will be obtained as in case of CDH the private key can not be obtained due to prolonged cyclic groups of nodes and there communications.

Consider a cyclic group *C* of order *q*. The CDH assumption states that, given

(C, C^r, C^o)

For a randomly chosen generator *C* and random C^r and C^o.

r, o å {0,…, q-1},

It is computationally intractable to compute the value

C^{ro}.

One could efficiently compute C^{ro} in the following way:

- compute C^{ro} by taking the discrete log of C^r to base C;
- compute C^{ro} by exponentiation: $C^{ro} = (C^o)^r$;

When compared to decisional diffei Hellman (DDH) computational diffie Hellman is the weaker assumption, when it comes to group of cyclic group of nodes then it is difficult to solve the problem. Thus CDH is used in our proposed system.

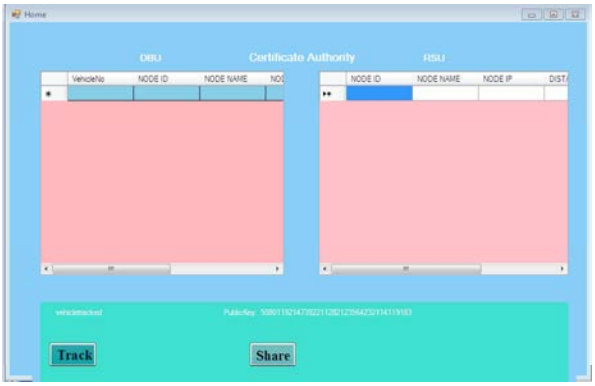

Fig. 3: Certificate Authority

Fig. 4: Creation of RSU

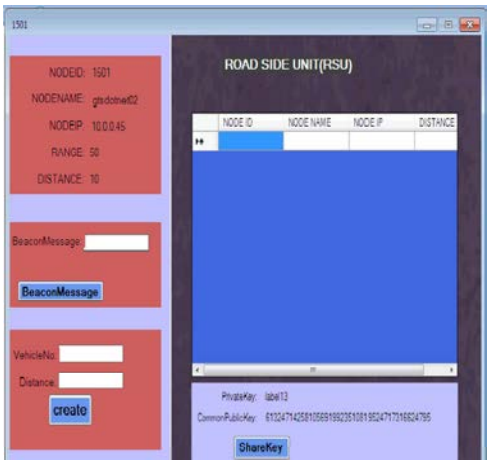

Fig. 5: RSU Key Publishing

From fig 4, it is clear that the creation on analysis of traffic and vehicular movement are done. As RSU is an intermediary for both OBU and CA. It should report on the analysis of traffic status, vehicular and object movement by with the help of OBU to the road side unit which has the information search of range, distance. If the range and distance are specified then the creation starts while the create button is pressed. After this event of pressing the create button with specified range and distance the alerts are provided to the OBU. The RANGE specifies the radius of particular distance in circumference to indicate the happening around the particular on board unit. Thus the objet in this range and distance are identified, checked for threat and then provided the alerts to the OBU. The OBU's communicates with the roadside station and thus horizons. The OBU's communicate with vehicle to vehicles using MANET and by exchanging the private key that is provided by Ruskin the fig 5, the final creation of both the CA and RSU are done. The CA holding the RSU's and OBU's information is provided. The beacon messages such as those that indicate about the traffic status, vehicular and object movement of the range and distance that are specified during creation of RSU. Beacon message is that which spreads to the range set. The neighbor node can be shared with the private key that is provided by RSU with entering the vehicle number and the distance needed. Thus the check is being processed and the neighbor node that is paired will be receiving the private and common public key by communicating with both OBU and RSU. Thus the communication extends while it is extended using OBU's then the MANET will be activated between vehicles.

Table 1: Traffic Analysis

Sly No	Time in Sacs	Number of Vehicle	Cumulative Vehicle
1	0-15	28	28
2	16-30	30	58
3	31-45	15	73
5	46-60	35	108

Table 1.1 informs on the time in which number of vehicles by pass.each time slot is in the measurement of 15 seconds. For each 15 seconds the numbers of vehicles by passed are monitored to know the traffic status in the particular locality. The series of time slots are measured with cumulative number of vehicles.

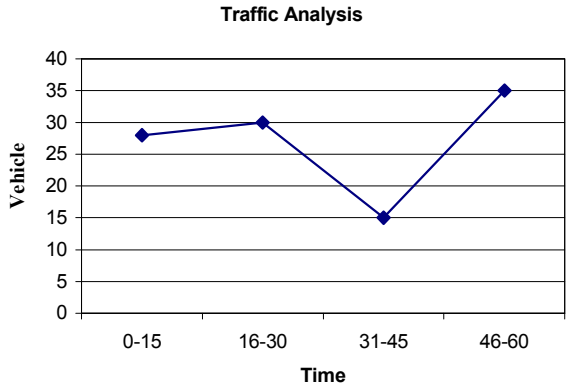

Fig. 6: Graph indicating traffic analysis

From the Fig 6 it is clear that the series1 indicates the number of vehicles that are in movement during the time slots. The series2 indicates the cumulative vehicles that are bypassed during the total time measured. The time is measured by 15 seconds for each slot and thus it is noted for 60 seconds according to the graph. In this graph it is shown that the traffic is normal and the speed of vehicle movement is normal. If the number of vehicles that is moved per 15 seconds is more then, it is said to be a traffic free day. While the number of vehicles bypassed each time slot is less then, it is said to be traffic jam. Thus the graphical information goes.

CONCLUSION

In this paper, we present a novel LPP protocol for VANETs. Through theoretical analysis, we show that LPP satisfies many desired properties for secure and privacy-preserving vehicular communications. We also demonstrate high efficiency of the proposed protocol in a number of representative vehicular communication scenarios by extensive ns2-based simulation. Compared to existing schemes, our proposed protocol can achieve mutual authentication for both V2R and V2V traffics with much lower computational cost and hence is highly suitable in a realistic vehicular environment

REFERENCES

1. Peng, Y., Z. Abichar and J. Chang, 2006. Roadside Aided Routing (RAR) in Vehicular Networks, in Proc. IEEE ICC, 8: 3602-3607.

2. Jiang, D. and L. Delgrossi, 2008. IEEE 802.11p: Towards an International Standard forWireless Access in Vehicular Environments,In Proc. IEEE VTC-Spring, pp: 2036-2040.
3. Lu, R., X. Lin, H. Zhu, P.H. Ho and X. Shen, 2008. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications, in Proc. 27th IEEE INFOCOM, pp: 1229-1237.
4. Raya, M. and J.P. Hubaux, 2007. Securing Vehicular Ad HocNetworks, J. Comput. Security, 15(1): 39-68.
5. Lu, R., X. Lin, H. Zhu and X. Shen, 2009. SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots, in Proc. 29th IEEE INFOCOM, pp: 1413-1421.
6. Kim, J.Y., H.K. Choi and J. Copeland, 2010. An Efficient Authentication Scheme for Security And Privacy Preservation in V2I Communications, in Proc. 72nd IEEE VTC-Fall, pp: 1-6.
7. Guo, H., F. Yu, Z. Zhang, W.C. Wong, M. Ma and Y. Wu, 2011. HASVC: An Efficient Hybrid Authentication Scheme for Vehicular Comm., in Proc. IEEE ICC, pp: 1-5.
8. Hsiao, H.C., A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur and A. Iyer, 2011. Flooding-Resilient Broadcast Authentication for VANETs, in Proc. 17th Annu. Int'l Conf. MobiCom Netw, pp: 193-204.
9. Shen, A.N., S. Guo, D. Zeng and M. Guizani, 2012. A Lightweight Privacy-Preserving Protocol Using Chameleon Hashing for Secure Vehicular Communications,in Proc. IEEE WCNC, pp: 2543-2548.
10. Krawczyk, H. and T. Rabin, 2000. Chameleon Signatures,in Proc. Netw. Distrib. Syst. Security Symp, pp: 143-154.
11. Ateniese, G. and B. de Medeiros, 2004. Identity-Based Chameleon Hash and Applications, in Proc. Financial Cryptogr. pp: 164-180.
12. Ezek, E.C., Sijing Zhang and Enjie Liu, 2014. Smart, Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward, in Pro. International Conference on Automation and Computing, pp: 176-181.
13. Choi J. and S. Jung, 2010. A Handover Authentication Using Credentials Based on Chameleon Hashing, IEEE Commun. Lett., 14(1): 54-56.