Volume 5, No. 4, April 2014 (Special Issue)

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORTS

Available Online at www.ijarcs.info

Authentication techniques in VANETs-A Survey

Remyakrishnan.P[1], Tripti C
Department of Computer Science & Engineering
Rajagiri School of Engineering & Technology, Kochi, Kerala, India

Abstract: The motives behind vehicular communication are the safety and comfort on roads. Safety messages demands of high priority for it to be delivered to the nodes on time to prevent from accidents. There is an urgent need to provide an effective mechanism for authentication in VANETs. VANET includes vehicle to vehicle (V2V) and vehicle to infrastructure communication. VANET have wide applications Intelligent Transportation System (ITS) also. This paper does a detailed study on various user authentication techniques in VANETs.

Keywords: VANET; V2V; V2I; layered biometrics; templates

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are an emerging research area because of its great potential to improve road safety and increase passenger convenience in vehicles. VANET vehicles will be capable of storing and processing great amounts of information, including a driver's personal data and geo-location information. VANET vehicles will b equipped with processing, recording and positioning mechanisms with a potentially infinite power supply [1].

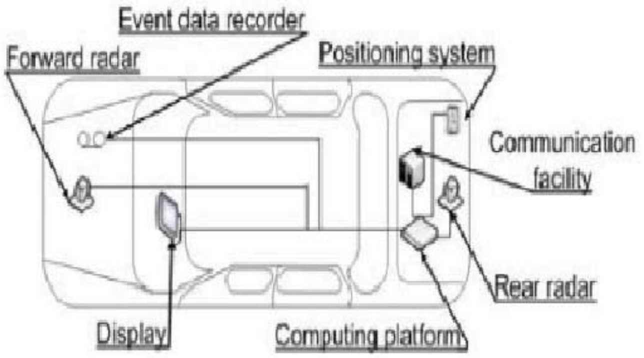

Figure. 1. A node in VANET

VANETs enable node-to-node and node-to infrastructure communication, thus communicating nodes are either vehicles or base stations that can exchange information. Mainly there are three types of messages been transmitted in
VANETs :

a. Warning messages which is used to prevent detected risky situations
b. Traffic management messages
c. Added value which provide Internet services

In a VANET the network can be accessed by all nodes, so messages sent by one node are available to all other nodes that have joined the network thus easing packets' eavesdropping. One of the most important challenges in VANETs is to enforce security and privacy. A VANET's vehicle can provide services to other vehicles as well as it can request any infrastructure service available. A vehicle must authorize other vehicles to access its information.

In this paper Section II classifies the different authentication techniques that exist now. Section III presents a detailed study of these schemes l. Section IV concludes the paper.

II. CLASSIFICATION OF AUTHENTICATION TECHNIQUES IN VANETS

The authentication techniques can be classified as those which are based on trust, digital signature and symmetric cryptography. Trust based authentication techniques are Trust Extended Authentication Mechanism (TEAM) and Chameleon Hashing for mutual and anonymous authentication. Authentication techniques based on digital signature are Elliptic Curve Digital Signature Algorithm (ECDSA) and Challenge Response Authentication using Digital Signatures. Finally authentication techniques based on symmetric cryptography are Timed Efficient Stream Loss-Tolerant authentication (TESLA) and TESLA++.

III. VARIOUS AUTHENTICATION TECHNIQUES IN VANETs

A. Trust Extended Authentication Mechanism (TEAM):

TEAM is a decentralized lightweight authentication scheme for vehicle-to-vehicle communication networks. It only uses an XOR operation and a hash function hence called as a lightweight authentication scheme. TEAM requires only a few storage spaces compared to other schemes because the vehicle does not need to store the authentication information (e.g., public key) of the entire vehicle. It classifies the vehicles into to the following types: a law executor (LE), a mistrustful vehicle (MV), and a trustful vehicle (TV).

A LE, can be a police car or public transportation vehicles (e.g., buses), which can act like a mobile Authentication Server. Th Law Executer can be trusted permanently. If a normal vehicle is authenticated successfully then it is trustful otherwise, it is considered as mistrustful. A Trustful Vehicle becomes the Mistrustful Vehicle when the key lifetime is over. To provide a secure communication environment, the On-Board Unit should be authenticated successfully before it can access the service. Hence any trustful OBU can authenticate the other mistrustful OBUs without necessarily finding an LE, and all vehicles in a VANET can complete the authentication procedure quickly TEAM focus on Transitive Trust Relationship as shown in the figure below [2].

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014

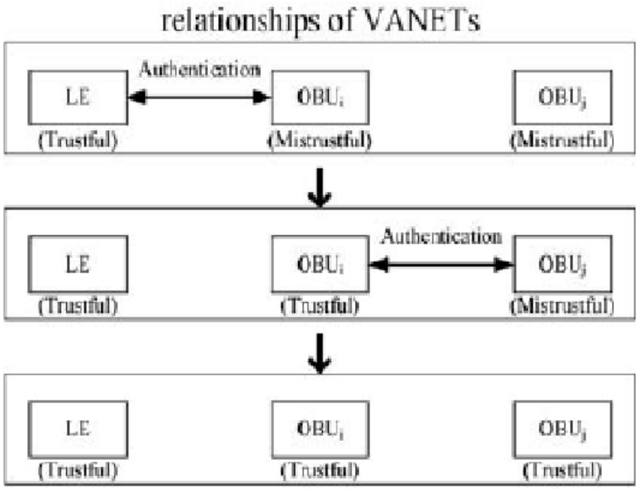

Figure. 2. Transitive trust relationships in a TEAM.

The major advantages of TEAM are Anonymity, location privacy, mutual authentication, forgery and modification attack resistance, replay attack resistance etc. It has no clock synchronization problem. But in addition it has got two major drawbacks also such as authentication is only on the basis of trust and how to prolong the trustful state of the Trustful Vehicle.

B. Chameleon Hashing for Mutual and Anonymous Authentication(CHMAA):

It is a security model for vehicular networks defines three types of network entities: A certification authority (CA), the fixed Road Side Units(RSUs), and the mobile On Board Units equipped on the running vehicles [3]. RSUs and OBUs have to register and get certified by the certification authority (CA) which has unlimited computation and storage capability. The real identity of an OBU can be recovered from its certificate only by the CA. RSUs work in a semi-trusted way as an intermediaries between OBU. RSUs can filter the fake messages from a malicious vehicles. It can also report the OBUs certificate information to CA. OBUs broadcast the traffic status information such as speed, location and acceleration etc that make the drivers aware of their driving environment. Chameleon signature, first introduced in [4] is the basis of proposed authentication algorithm.

Chameleon signature algorithms has a unique characteristic that it is non-interactive, that means the signature is generated without interacting with the intended receiver. Hence the performance of authentication is improved. CHMAA known for the following merits such that it can achieve mutual authentication for both V2R and V2V traffics. It has got much lower computational cost and is highly suitable in a realistic vehicular environment. Demerits considered for CHMAA are each OBU needs to store a large number of anonymous pair-wise keys. And longer reception delays are experienced in high traffic density.

C. Timed Efficient Stream Loss-Tolerant Authen ticaton (TESLA):

TESLA is an efficient authentication techniques that can be used instead of Digital signatures in VANETs. In order to ensure that the sender is an authenticated source of message TESLA uses symmetric cryptography with delayed key disclosure. It can be used as an authentication mechanism for broadcast and multicast network communications. Since symmetric cryptography is much faster than signatures delay can be avoided. Hence TESLA can be used to overcome Delay of Service(DoS) attacks. In TESLA, the receiver stores the information send by the source until the corresponding key is disclosed. TESLA requires loosely synchronized clocks between the sender and the receivers. Each receiver must be loosely time-synchronized with the source in order to verify messages, but otherwise receivers do not have to send any messages. TESLA also needs an efficient mechanism to authenticate keys at the receiver and mainly use one-way chains for this purpose. The functioning of TESLA system can be understood from [5].

TESLA got wide acceptance due the following merits that it requires no trust between receivers and it uses low-cost operations per packet at both sender and receiver. In addition it can tolerate any level of loss without retransmission and requires no per-receiver state at the sender. TESLA can protect receivers against denial of service attacks in certain circumstances. Also it can reduce the overhead associated with user authentication. Even though it has got such major advantages there are some demerits also because TESLA is vulnerable to storage based Denial of Service attacks and TESLA signatures will require a clock source for synchronizing their local clocks. It fails to prevent the occurrence of repudiation and vulnerable to storage based Denial of Service attacks.

D. TESLA++:

TESLA++ is a more efficient and advanced form of Timed Efficient Stream Loss-Tolerant Authentication(TESLA). TESLA++ is functionally more efficient and more secure than TESLA. The complete procedure of authenticating the validity of user in TESLA++ has been concisely provided in [5].

Merits of TESLA++ over TESLA is that the cryptographic techniques used by TESLA++ are easier to manage and control than those used in TESLA.TESLA++ prevents the memory based Denial of Service (DoS) attacks as well as computation-based Denial of Service(DoS) attacks. TESLA++ reduces the memory requirements at receivers end without affecting the efficiency of its broadcast authentication mechanism. It offers a more secure User Authentication mechanism than TESLA. Also it is an efficient means of Information. Broadcasting in case of very high computational load. In addition the drawbacks of TESLA++ is that it cannot provide multi-hop authentication and does not offer non-repudiation. To prevent Flooding condition older messages are discarded.

E. The Elliptic Curve Digital Signature Algorithm (ECDSA):

VANET systems use Asymmetric ECDSA key pair to provide User Authentication [8]. The asymmetric key pair consists of a public key and a private key. Where the public key is a random multiple of the base point, and the private key is the integer used to generate the multiple. Signatures can be generated and verified using ECDSA. User Authentication using both the public keys and the private keys of ECDSA as explained by Don Johnson and others. User validation includes two steps:

a. The public key of sender is validated.

b. Authentication of user by validating his private key.

To increase the reliability, the sender is asked to sign the message using his private key after validating the public key. Two possible kinds of attacks that can occur even after providing such a higher reliability level are:

a. Attacks on Elliptic Curve Discrete Logarithmic Problem(ECDLP)
b. Attacks on the hash function

ECDSA reduces the scope of attacks from malicious users and performs better than TESLA at greater distances. It allocate lesser response time for user authentication and provide secure and faster dissemination of information. But it has verification delay due to limited processing power.

F. Digital Signtures and Challenge Response Authenticationthm(CRA):

Digital Signatures are used to authenticate the safety messages in VANETs. Digital Signatures follows an Asymmetric Authentication Scheme. Safety messages are need to be disseminated as fast as possible. The Digital Signatures are used in combination with Public Key Infrastructure (PKI).The sender encodes the message using public key cryptography and then signs it digitally before transmission. Public key cryptography provides security to the data while Digital Signature proves the authentication of the sender. An attacker can intercept the information bits during transmission, using his public key modify them and retransmitt them, but digital signature of the authenticated user cannot be reproduces by an attacker .

Inorder to prevent occurrences of any discrepancies, Digital Signatures will be assigned by a centralized government authority. There is a hardware called Tamper Proof Device(TPD) [13], which signs all the messages transmitted from that user. It is a hardware device which is highly secure and has its own battery and clock. Only authorized users are able to access TPD. The manner in which Digital Signatures authenticates the valid users and provide secure transmission of safety messages has been described in [9] and [10].The working of Digital Signatures has been shown diagrammatically in the following figure[13].

Challenge Response Authentication works as follows, when the receiver receives the message he will send a challenge to the sender. The sender will transmit his location and a timestamp to prove its authentication as a response to the challenge. Infra red rays are generally used send the response ,and as the transmitted information travels at speed of light, it is impossible to modify the information transmitted . The receiver gets the response and validity of the safety message is established. The clocks of the sender is relatively synchronized with that of the receiver. The receiver will compare the values of timestamp in both the cases. The transmission time in both the messages must be same. A deviation in the timestamp values will indicate a malicious attempt of spreading false information. Thus the Challenge Response Authentication secures the integrity of the system by reducing the transmission of fraudulent messages. Challenge Response Authentication can be successfully implemented in systems like SOLSR,VM etc.

The Challenge Response Authentication an be understood in detail from [11] and [12].

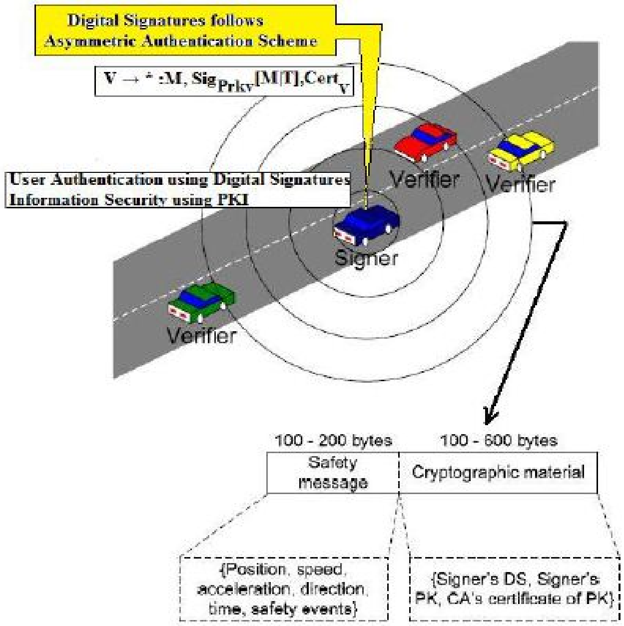

Figure: 3

Digital Signatures and Challenge-Response scores over other techniques in almost all criterions since these two techniques are very versatile. But the response is generally send using Infra red rays that may suffer from interference and must have direct Line of Sight.

A comparison of various authentication techniques discussed is shown in table 1.

Table I. Performance Of Different Authentication Techniques In Vanet

	TEAM	***CHMAA***	***ECDSA***	***Challenge Response Authentication***	***TESLA***	***TESLA++***
Features	Fast error detection,Perfect forward secrecy,Man-in-the-middle attack resistance	Authority tracking capability	Independent of the hardware used	Secures the integrity of the system	Reduce the overhead associated with user authentication	More secure than TESLA
Classifier	Trust Based	Trust Based	Digital signature Based	Digital signature Based	Symmetric cryptography Based	Symmetric cryptography Based

IV. CONCLUSION & FUTURE WORK

This paper presented a detailed survey on different authentication techniques used in VANETs. But the problem still demands more attention. We believe that our survey will be useful for researchers who are working in the area of authentication in VANETs as we have included almost all the prominent techniques currently used.

V. REFERENCES

[1] V. Casola, J. Serna, J. Luna, M. Rak and M. Medina," An Interoperability System for Authentication and Authorization in VANETs", International Journal of Autonomous and Adaptive Communications Systems, Vol. 3,No. 2. (2010), pp. 115-135

[2] Ming-Chin Chuang and Jeng-Farn Lee,"TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks",IEEE SYSTEMS JOURNAL ,2013.

[3] Song Guo,Deze Zeng,Yang Xiang,"Chameleon Hashing for Secure and Privacy-Preserving Vehicular Communications",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,2013.

[4] H. Krawczyk and T. Rabin, Chameleon signatures, in Network and Distributed System Security" in Proceedings of the Network and Distributed Systems Security Symposium (NDSS 2000)

[5] Ahren Studer, Fan Bai, Bhargav Bellur and Adrian Perrig, "Full Paper:Flexible, Extensible, and Efficient VANET Authentication", Published in the 6th Embedded Security in Cars Conference,2010.

[6] Emanuel Fonseca and Andreas Festag," A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS.", In Technical Report NLE-PR-2006-19, NEC Network Laboratories,March 2006.

[7] Yih-Chun Hu and Kenneth P. Laberteaux, Strong VANET security on a budget, In Proceedings of the 4th Annual Conference on Embedded Security in Cars (ESCAR 2006), November 2006.

[8] D. Johnson, A. Menezes, and S. Vanstone, The elliptic curve digital signaturealgorithm (ECDSA), International Journal of Information Security,vol. 1, no. 1, pp. 3663, 2001.

[9] Maxim Raya and Jean-Pierre Hubaux,"The Security of Vehicular Ad Hoc Networks", In Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 2005.

[10] M.Burmester,E.Magkosand,"Strengthening Privacy Protection in VANETs", IEEE International Conference on Wireless and Mobile Computing, Networking and Communication,2008.

[11] Jaafer Al-Saraireh and Sufian Yousef, "A New Authentication Protocol for UMTS Mobile Networks.", Published in EURASIP Journal on Wireless Communications and Networking", v.2006 n.2, p.19-19, April 2006.

[12] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung." Secure Location Verification for Vehicular Ad-Hoc Networks. ",In Global Telecommunications Conference, IEEE GLOBECOM 2008.

[13] Arzoo Dahiya,Vaibhav Sharma,A survey on securing user authentication in vehicular ad hoc networks,International Journal of Information.Security, Vol. 1 (2001).

[14] 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, Nov. 2008.

[15] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen,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. 27th IEEE INFOCOM,USA, 2008.

[16] Y. Jiang, M. Shi, X. Shen, and C. Lin, BAT: a robust signature scheme for vehicular networks using binary authentication tree, IEEE Transactions on Wireless Communications, vol. 8, no. 4, pp. 19741983,2009.

[17] Jie Zhang,"A Survey on Trust Management for VANETs",International Conference on Advanced Information Networking and Applications 2011.

[18] Xiaodong Lin,Xu Li,"Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 7, SEPTEMBER 2013.

[19] Jason J. Haas ,Yih-Chun Hu,Kenneth P. Laberteaux,"Real-World VANET Security Protocol Performance",IEEE "GLOBECOM" 2009 proceedings.

[20] M Raya and Jean-Pierre Hubaux. The Security of Vehicular Ad Hoc Networks. In Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), November 2005.

[21] A.Wasef, X. Shen,"ASIC: Aggregate Signatures and Certificates Verification Scheme for Vehicular Networks",IEEE "GLOBECOM" 2009 proceedings.

[22] Q. Xu, T. Mak, J. Ko, and R. Sengupta, Vehicle-to-vehicle safety messaging in DSRC, in Proceedings of VANET, 2004.

[23] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, Trafficview: Traffic data dissemination using car-to-car communication, ACM SIGMOBILE Mobile Computing and Communications Review, vol. 8, p. 2004.

[24] Rongxing Lu,Xiaodong Lin,Xiaohui Liang,Xuemin (Sherman) Shen,"A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs"IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 13, NO. 1, MARCH 2012.

[25] A.-N. Shen, S. Guo, D. Zeng, and M. Guizani,"A Lightweight Privacy-Preserving Protocol using Chameleon Hashing for Secure Vehicular Communications, in Proceeding of IEEE Wireless Communications and Networking Conference (WCNC). IEEE, April 2012.

[26] T. C. to Car Communication Consortium (C2CC), http://www.cartocar.org/.

[27] T. N. on Wheels (NOW) Project, http://www.network-on-wheels.de/.

[28] OpenSSL. http://www.openssl.org, September 2008.

[29] Multicast security ietf working group (msec).http://www.ietf.org/html.charters/msec-arter.html, 2002.

[30] 5.9 GHz DSRC. [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

CONFERENCE PAPER
Two day National Conference on Innovation and Advancement in Computing
Organized by: Department of IT, GITAM UNIVERSITY Hyderabad (A.P.) India
Schedule: 28-29 March 2014