International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A Survey on User Authentication Services in Vehicular ad hoc Networks

[1]G.Vijayakumar
Professor & Principal, Muthayammal Polytechnic College, Rasipuram, Tamilnadu, India.

[2]A.Manikandan
Asst.Prof & Head, Dept. of Computer Science,
Muthayammal Memorial College of Arts & Science, Rasipuram, Tamilnadu, Inida

Abstract
Vehicular ad hoc networks(VANET) is the most widely used realization of mobile ad hoc networks (MANET). Vehicular communication was safety on roads, because million of lives were lost and much more injuries have been incurred due to car crashes. Safety messages which are of highest priority need to be delivered to the destination node on time to prevent from accidents. VANET have wide applications in Automobile Industry including Intelligent Transportation System (ITS) to avoid collision and route vehicles efficiently to improve safety. VANET includes vehicle to vehicle (V2V) communication and vehicle to road side communication. This paper describes the various user authentication protocols and compares the efficiency of user verification algorithms. This paper also highlights the use of Digital Signatures and Challenge-Response Authentication to secure user identification. We discuss the occurrence of security lapses due to counterfeit and insecure encryption vulnerability. We advocate a simple and safe encryption technique incorporating Digital signaling to develop a reliable inter vehicles communication. Then we qualitatively compare the different authentication techniques. We discuss in detail the effect of incorporating the most recent knowledge about the position of vehicle to develop secure connection between the vehicles. The paper concludes with open security concerns regarding reliable inter vehicle communication.

1. Introduction

VANET led to the development of a more advanced system computer network on wheels instead of just computer on wheels. VANET involves communication between vehicles as well as vehicles and road side base stations. VANET being an ad hoc network presents a communication environment without any visible infrastructure. The entire VANET Network is shown in Figure 1. Also, it introduces the concept of distributed database in Inter Vehicular Communication. VANET was developed mainly to provide safety and comforts to the passengers. With large number of accidents claiming precious lives, it became necessary to develop a system which could prevent accidents by developing an efficient communication system between vehicles. The resent works in VANET was started in 1980s when organisations like JSK in Japan, PATH in California and Chauffeur in EU came into existence. These organisations provided the coupling of two or more vehicles. With further research, VANET was not confined to avoidance of accidents but also preventing traffic congestion and providing comforts to the passengers. Recent research has extended uses of VANETs to provide a pool of services to the users. With VANET providing safety to human life, it becomes very important to secure the VANET system.

Figure1. Communication in VANET systems

This paper is centered on the concept of User Authentication to secure that only authenticated users exchange information. The proper User Authentication methods, the fake unauthenticated users can be prevented from accessing the information across the network. In this way, secured User Authentication increases the confidence of the user in the system. This paper describes the work done till date to provide a secured user authentication. It also discusses the role of various protocols to provide an authenticated environment.

2. User Authentication protocols and Algorithms

User Authentication can be confirmed by a number of protocols & algorithms. Practically, we use a combination of these protocols as they have higher efficiency as compared to individual protocols.

2.1 PKI (Public Key Infrastructure)

ISSN:2319-7900

It is used in VANET systems to ensure user validity that it's based on the concept of asymmetric key cryptography. It has two different types of keys. These are,

i) Public key and
ii) Private key

This pair of keys can be expressed in terms of a set as described below:

PKI: (X, Y) (1)

Where, X: Private key & Y: Public key

Each of the communicating users has both the keys. The private key is confined only to the user himself, while the Public key is shared with all the vehicles in the system. The message can be encoded using any of the keys. This encoding can be viewed mathematically as:

EM = Pr(Pu(M)) (2)

EM = Pu(Pr(M)) (3)

Where

Pr(): Private key function.

Pu(): Public key function.

M: Message to be secured.

EM: Encoded Message obtained.

The user ensures the integrity of the message by signing the encoded message using Digital Signatures. This ensures the reliability of the message. The trustworthiness of the message can be increased by Certificate Authorities(CA) who will digitally sign the data and binds the public keys with private keys effectively to ensure User Authentication. CA issues certificates to the vehicles which mark the validity of the users.

We need a centrally managed CA to avoid any discrepancy. Either a Government managed authority or the Vehicle manufacturers can act as the CA. In an Ideal situation, the vehicle manufacturer can provide the initial Temporary Certificate. This Certificate has to be validated to Permanent status only by the concerned Government Authority.

The Certificate consists of public key, the certificate lifetime and Signature of the CA. Regular Certificate Revocation will create a Certificate Revocation List. This list has to be appended to the Certificate after each revocation. The certificates were signed by a CA can also be revoked in two cases of Information compromise. These are Cryptographic keys get compromised and a fraudulent user is using signed certificates to transmit fake information. The Public Key Infrastructure (PKI) also uses anonymous public keys to secure user identification and location privacy. Anonymous Public Keys are used to avoid backtracking by an unauthenticated user.

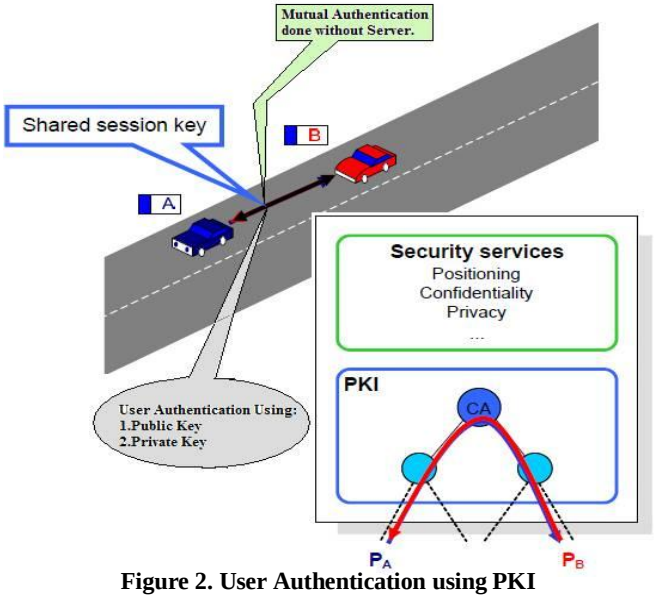

Figure 2. User Authentication using PKI

2.2 TESLA

It is an acronym for Timed Efficient Stream Loss-Tolerant Authentication. It is used as an authentication method for multicast and broadcast network communications. In VANET, PKI is not the only option to confirm User Authentication. There is a completely different technique called TESLA which provides an efficient alternative to signatures. Instead of using Asymmetric Cryptography, TESLA uses symmetric cryptography with delayed key disclosure (which provides the necessary element of asymmetry) to prove that the sender was the authenticated source of the message. In other words, we can describe TESLA as a lightweight broadcast authentication mechanism. TESLA performs broadcast authentication mechanism in the same manner and applies the same approach that is applied in the unicast authentication mechanism. This proves to be a more efficient way of broadcasting messages. TESLA is compliant to computational Delay of Service(DoS) attacks because symmetric cryptography is significantly faster than signatures and thus delay is avoided. In spite of these versatilities, TESLA is susceptible to attacks arising due to memory-based Denial of Service[7].

In TESLA, the information send by the source is stored at the receivers end until the corresponding key is disclosed. Malicious attackers can deluge receivers with a huge collection of invalid messages which never have a corresponding key. This leads to a situation referred as pollution attack. In pollution attack, the attacker continuously fills receiver's memory with the junk data that affects the systems performance. With the large amount of junk data, Performance of the system

ISSN:2319-7900

deteriorates. The system can even crash if the amount of junk exceeds the maximum workload the system can successfully sustain. TESLA uses symmetric key cryptography for broadcast authentication. TESLA depends completely on time to provide the necessary asymmetry in the authentication scheme, allowing only the sender to generate a broadcast authentication at a given point of time. Though symmetric cryptography significantly reduces computation, but still it fails to prevent the occurrence of repudiation. TESLA is used in VANET system to reduce the overhead associated with user authentication. But TESLA is vulnerable to storage based Denial of Service attacks. This becomes the basis for the development of TESLA++.

2.3. TESLA++

It is a more efficient and advanced form of Timed Efficient Stream Loss-Tolerant Authentication(TESLA). It is functionally more efficient and secure than TESLA. It has many advantages. TESLA++ prevents occurrence of memory based Denial of Service(DoS) attacks which are prevalent in TESLA. It reduces the memory requirements at receiver's end without affecting the efficiency of its broadcast authentication mechanism. It is not only prevents the memory based DoS attacks but also the computation-based DoS attacks with equal priority. It makes use of those cryptographic techniques which are easier to manage and control than the techniques used in TESLA. It offers a more secure User Authentication mechanism than TESLA. It is an efficient means of Information Broadcasting in case of very high computational load. TESLA++ offers reduced memory requirements at receivers end as the receiver need not to store all the Message Authentication Codes but only the self generated ones. In TESLA++, message authentication codes are broadcasted earlier than the message and the corresponding keys. The complete procedure of authenticating the validity of user in TESLA++ has been concisely provided in [1]. It provides an extensive explanation of the steps followed in TESLA++ to authenticate a user. They also provide an effective mechanism for memory management during flooding by any malicious user. Their paper proposes to discard irrelevant MACs to free the memory in case of flooding. The following steps are to be followed to discard irrelevant MACs:

(i) Discard all MACs whose key indices are older than the last authentic message received from that sender.
(ii) Discard the message whose verification is oldest in the future.

This scheme discards messages on the basis that either the older MACs were stored because a malicious user injected those messages or the message and the corresponding disclosed key were lost or the attacker made the receiver store the messages for a long duration. The disadvantages of TESLA++ are the performance of TESLA++ gets deteriorated in lossy networks as it considers MAC and the corresponding message as separate entities and broadcasts them separately. It would not be incorrect to say that in lossy networks, TESLA is a better authenticating mechanism as compared to TESLA++. TESLA scores over TESLA++ as the latter does not provides multi-hop authentication. It does not offer non-repudiation. In TESLA++ older messages are discarded to prevent Flooding condition. But this scheme surfaces one problem i.e. if any old message is discarded, then, the MAC corresponding to that message becomes useless. For any further transmission between those two users, it has to transmit the whole message again along with the MAC to authenticate the user. This leads to overhead problem.

2.4 ECDSA

It is a mathematical representation for the elliptic curve analogue of the DSA. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a mathematically derived form of Digital Signature Algorithm (DSA). The strength per key bit is significantly greater in an algorithm using elliptic curves because elliptic curve discrete logarithm problem has no sub exponential-time algorithm. Being a mathematical entity, the security of elliptic curve can be described in mathematical terms only. The computational intractability and mathematical hardness of the ECDLP contributes towards its security. It is advantageous to use ECDSA to provide secure and faster dissemination of information after authenticating the users in environments where amount of storage offered is less and lesser response time is allocated for user authentication. Asymmetric ECDSA key pair is used in VANET systems to provide User Authentication. ECDSA can also be used to generate and verify signatures. Don Johnson and others gave a complete account of ECDSA in [2]. ECDSA uses an asymmetric key pair of a public key and a private key. The public key is a random multiple of the base point, while the private key is the integer used to generate the multiple. An entity's key pair is associated with a particular set of EC domain parameters. User validation follows two steps.

1) Public key of sender is validated. The public key validation prevents chances of attacks arising from use of invalid public keys and detects transmission errors.
2) Authentication of user by validating his private key. The private key of the sender is validated to ensure that no other malicious attacker is using the identity of a valid user to transmit faulty information. After validating the public key, the sender is asked to sign the message using his private key. This provides high levels of reliability. Even after providing such high levels of security, attacks can be made mainly using the two methods. These two methods are attacks on Elliptic Curve Discrete Logarithmic Problem (ECDLP) and attacks on the hash function. Though ECDSA reduces the scope of attacks from malicious users, but still we need to dedicate a lot of research efforts to further improve the security of the ECDSA system.

3. Digital Signatures

User Authentication verifies that only valid users exchange information. It avoids the malicious users from

ISSN:2319-7900

transmitting junk information and intercepting confidential information. It provides message legitimacy to protect the VANET system from outside attacks. Digital Signatures are used to authenticate the safety messages. Since, safety messages do not contains any confidential information therefore we need only to authenticate them. This is the reason why no encryption of safety messages is required. To avoid the dissemination of false information, we need to ensure the authentication of the message. Digital Signatures follows an Asymmetric Authentication Scheme. Though asymmetric authentication involves more overhead bits per data unit transmitted, but still Digital Signatures are preferred in VANET systems. Safety messages are need to be disseminated as fast as possible. Symmetric Authentication involves handshake mechanism which delays the transmission of safety messages. Therefore, we use Digital Signatures to effectively disseminate the safety messages. The Digital Signatures are used in combination with Public Key Infrastructure(PKI).

PKI has been explained in the previous section. 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. A malicious user can intercept the information bits during transmission, modify them using his public key and resends them, but still he would not be able to reproduce the digital signature of the authenticated user. The receiver will be cognizant that the information was transmitted by a malicious user as the message would not have authenticated digital signature[4]. Digital Signatures are assigned by a centralized government authority to prevent occurrences of any kind of discrepancy. There is a hardware called Tamper Proof Device(TPD) which signs all the messages transmitted from that user. TPD is a highly secure hardware device with its own battery and clock. TPD can only be accessed by authorized users. Digital Signatures authenticates the valid users and provide secure transmission of safety messages.

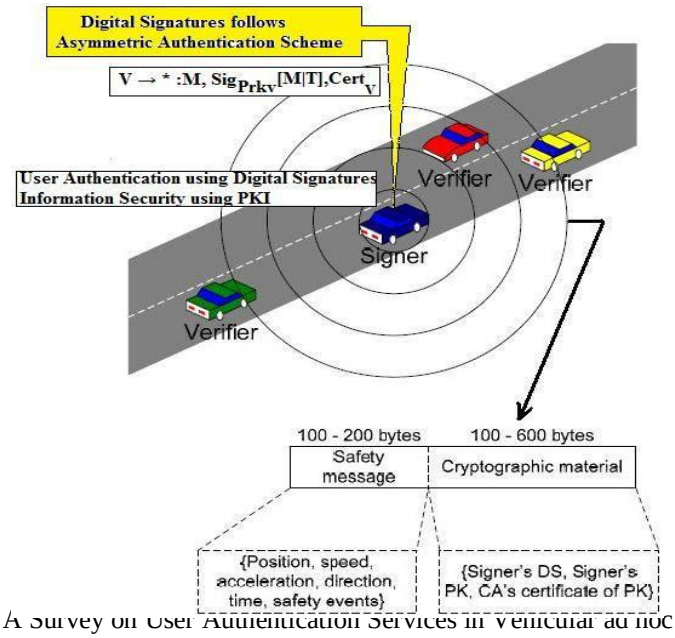

Figure 3. Diagrammatic Representation of working of Digital Signatures authenticating a user

4. Challenge Response Authentication

Sometimes a malicious attacker sporadically transmits false information tagged as safety message. This can lead to panic situations. Suppose a user wants free path to travel. The malicious attacker can disseminates the information about an accident on that path. All other users will decode the information using their public keys. Without knowing the intention of the attacker, they would avoid that route as accident would have created heavy traffic congestion. This way the attacker would get a free path to move and his intentions would be achieved. We use the technique of Challenge–Response Authentication to minimize the chances of such incidences.

In Challenge–Response Authentication, as soon as the receiver receives the message, he sends a challenge to the sender. In response to the challenge, the sender transmits his location and a timestamp to prove its authentication. The clocks of both the sender and receiver are relatively synchronized. The response is generally send using Infra red rays and it is nearly impossible to modify the information transmitted as the response travels at speed of light. The receiver gets the response and validity of the safety message is established. The receiver also compares the values of timestamp in both the cases. The transmission time in both the messages should remain the same. Any deviation in timestamp values would reflect malicious attempt of spreading false information. Challenge–Response Authentication minimizes the transmission of fraudulent messages and secures the integrity of the system. This authentication has been successfully implemented in systems like SOLSR, VM etc. After analysing all the techniques involved in authenticating a user, this paper supports the combination of Digital Signatures and Challenge-Response Authentication to be used to authenticate a user.

5. How position of vehicles assist in User Authentication.

This paper supports the use of the attribute position of the vehicle disseminating the safety message to validate the authentication of user as well as the accident. This attribute will not exactly pinpoint the vehicle but will only tell whether the vehicle was in the vicinity of the accident site. This parameter will increase reliability of the safety message. If the position of the vehicle justifies that the user could have any information of the accident, then it would increase the probability of message being valid. This

ISSN:2319-7900

scheme presents many security concerns. We have to effectively find a way to protect the location privacy [13] of the vehicle. No one should be able to track down anybody location [10] discuss issues related to location privacy. The user privacy should not be sacrificed in any case. A lot of studies are being done to provide privacy to the users.

6. Open Security Issues

These issues are,

1. User Authentication should not pave the way to this identification, unless he permits.
2. Bactracking tricks to obtain user identification should be prevented at any cost.
3. The user authentication schemes should be highly reliable and very safe. No data should be counterfeited while establishing authentication.
4. Confidentiality of User should not be compromised.
5. The location privacy of user should not be revealed under any circumstances.

7. Conclusion

The improvement of security primitives for VANET is an area that has not received a lot of attention to date. We consider the potential threat associated with an increased reliance on wireless communication for the smooth flow of traffic. This paper surveys some user authenticating skill and explains them in detail. It performs a review of all the work done by earlier researchers in this direction. We discuss threats to privacy in VANET and explain privacy importance. Although this paper presents no technical results but this paper helpful for future researchers to scrap down the privacy in vehicular networks.

References

[1] Arzoo Dahiya, Vaibhav Sharma**,** A surevey on securing user authentication in vehicular ad hoc networks, Institute of Technology and Management, Gurgaon.

[2] 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.

[3] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey. Secure V2V Communication With Certificate Revocations. In proceedings of the IEEE Infocom 2007, MOVE Workshop.

[4] Chae Duk Jung, Chul Sur, Yougho Park and Kyung-Hyune Rhee. A Robust Conditional Privacy-Preserving Authentication Protocol in VANET. In the 1st International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec 2009), 2009.

[5] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing Vehicular Communications. In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006.

[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] aae l-Saraireh & Sufian Yousef . A New Authentication Protocol for UMTS Mobile Networks. Published in EURASIP Journal on Wireless Communications & Networking, v.2006 n.2, p.19-19, April 2006.

[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] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura and Kaoru Sezaki. CARAVAN: Providing Location Privacy for VANET. In 3rd workshop on Embedded Security in Cars (ESCAR 2005), 2005.

[11] Mike Burmester, Emmanouil Magkos and Vassilis Chrissikopoulos. Strengthening Privacy Protection in VANETs. In proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication.

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

[13] Akram Belajouza & Clemens miner. Privacy in Vehicular Ad-hoc Networks (VANETs). In Proceedings of Fraunhofer IGD, 2009.

[14] Meng Jun Tong, Li Yu, Chang Heng Shu, Qi Fen Dong, Feng Gao, 2011, „„Research and Simulation of Routing Protocol in Different VANET Scenarios", Journal of Advanced Materials Research (Volumes 217 - 218), Switzerland.

[15] Yun-Wei Lin, Yuh-Shyan Chen and Sing-Ling Lee, 2010 "Routing in Vehicular Ad Hoc Networks: A Survey and Future Perspectives," Journal of Information Science and Engineering.

Biography

G.VIJAYAKUMAR received bachelor's degree in 1994 and Master degree in 1996 from Bharathidasan University, Trichy, Tamilnadu. He completed M.Phil from Periyar University, Salem, Tamilnadu, India in 2007. He completed M.E CSE in 2009 from Anna University, Chennai, Tamilnadu, India. Currently, he is working as a Principal in Muthayammal Polytechnic College, Rasipuram, Tamilnadu. His research interests are in Wireless Ad Hoc Networks, Wireless Sensor Networks and Network Security. He is a life member of Indian Society for Technical Education, New Delhi. He published several books. These titles are Data Structure

ISSN:2319-7900

Using C(Pradeepa Publications, Coimbatore, Tamilnadu) and Computer Application (RSPR Publications, Salem, Tamilnadu).

A.MANIKANDAN received bachelor's degree in 1997, Master degree in 1999 from Bharathidasan University, Tamilnadu, India and M.Phil from M.S University, Tamilnadu, India in 2003. He completed M.Tech in 2011 from Prist University, Tamilnadu, India. He submitted his Ph.D thesis in Sep' 2014 at Dravidian University, Andra Pradesh, Inida. Currently, he is working as an Assistant Professor and Head, Department of Computer Science in Muthayammal Memorial College of Arts & Science, Rasipuram, Tamilnadu.. His research interests are in Wireless Ad Hoc Networks, Wireless Sensor Networks and Network Security. He is a life member of Indian Society for Technical Education, New Delhi. He published several books. These titles are Programming in C, Embedded Systems & Web Technology (Krishnagiri, Tamilnadu and Bharathi & Bharathi Publishers) and Computer Programming (Chennai, Tamilnadu, Global Publishers).