International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 2 25-Aug-2014,ISSN_NO: 2321-3337

A COMPARATIVE STUDY OF SECURE ENHANCING SERVICE AUTHENTICATION PROTOCOL IN VANET

Dr.K.Ravikumar[1], R.Suganya[2]
Department of Computer Science, UGC – NET Coordinator[1]
Asst.Professor, Thanjavur, India
Asst. Prof &Research Scholar, Karpagam University[2]
Tamil University , Coimbatore, India.

ABSTRACT**−** *In the recent years, Vehicular Ad Hoc Networks (VANETs) has evolved as new paradigm for broadband Authentication Protocol. In Vehicular Ad Hoc Networks (VANETs), adopt the public key Infrastructure Service Server (SS) for their security. In any PKI system, the authentication of a client is performed by checking if the Service of the Service Server is included in the current Authenticate Server (AS), and verifying their authority of the service of the server. In this paper, we propose Secure Enhancing Service Authentication Protocol (SESAP) for VANETs, which replace the time-consuming Service Server checking process by an efficient service server process. In recent years, many secure authentication protocols has been proposed for VANETs. In this paper we present a theoretical survey on predominant secure authentication protocols and compare the security issues of the following protocol such as SAODV, SRP, and SEAD.*

Keywords: VANETs, Authentication Protocol, SAODV, SRP, SEAD Protocols.

1. INTRODUCTION

Vehicular Ad-hoc networks (VANETs) have attracted extensive attentions in recent years for their promises in revolutionizing the human driving modes and transportation systems. VANETs consist of network entities, including vehicles and road-side infrastructure units (RSUs). Vehicle-to- Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are two basic vehicular communication modes, which allow vehicles to communicate with each other or with the roadside infrastructure, respectively. Vehicular communication over the wireless medium employs the Dedicated Short Range Communications (DSRC) protocol [1].The security and privacy in VANETs faces many challenges due to the open broadcasting of wireless communications and the high-speed mobility of the vehicles. It is obvious that any malicious behaviours of user, such as injecting beacons with false information, modifying and replaying the disseminated messages, could be fatal to the other users.

Furthermore, privacy must be achieved in the sense that the vehicle related privacy information should be protected so that an attacker can be prevented from collecting vehicle messages, tracking locations, and inferring sensitive data. Hence, to satisfy above security requirements, it is prerequisite to develop a suite of elaborate protocols to achieve security, privacy, and efficient message authentication before vehicular networks can be practically deployed. A vehicular network needs strong authentication, because it is desirable to validate each message sent by the On Board Units (OBUs). A well-recognized solution is to sign each message with a signature.

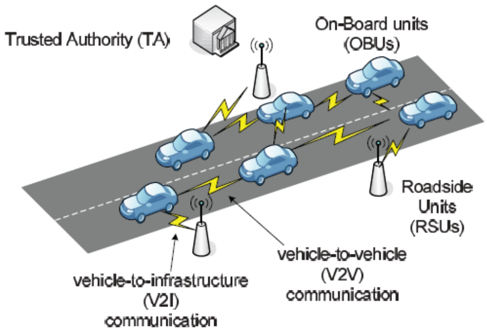
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Fig 1: The System Model

According to DSRC protocol [1], a RSU may communicate with hundreds of OBUs and each OBU will periodically transmit a safety or traffic message (beacon) to the nearest RSU via a common DSRC channel. Beaconing rate ρ typically
ranges from 3 to 10 beacons per second, with ρ = 10 currently considered as necessary for safety applications. Therefore, even in a normal traffic scenario, it is a very rigorous requirement for any RSU using classic signature schemes to verify a mass of messages in real-time. The delay caused by verifying a bulk of signatures may radically impede transmission throughput and impair the system scalability. Recently, an efficient batch verification scheme for optimizing the verification performance in V2I communications without any bogus messages has been proposed [2][3]. A prerequisite condition in this method is that all the signatures should be authentic.

2. SESAP OVERVIEW

In Vehicular Ad Hoc Networks (VANETs), adopt the public key Infrastructure Service Server (SS) for their security. In any PKI system, the authentication of a client is performed by checking if the Service of the Service Server is included in the current Authenticate Server (AS), and verifying their authority of the service of the server[4]. In this paper, we propose Secure Enhancing Service Authentication Protocol (**SESAP**) for VANETs, which replace the time-consuming Service Server checking process by an efficient service server process.

2.1 Authentication Server Ticket (AST)

An authentication server is an application that facilitates authentication of an client that attempts to access a network[5]. Authentication is the process of determining whether someone or something is actually who or what it declares itself to be. When a potential subscriber accesses an authentication server, a username and password may be the only identifying data required the user name will be the caller ID. In a more sophisticated system called Kerberos[6][7], the subscriber must request and receive an encrypted security token that can be used to access a particular service. RADIUS (Remote Authentication Dial-In User Service) is a commonly used authentication method. TACACS+ (Terminal Access Controller Access Control System Plus) is similar to RADIUS but is used with UNIX networks. RADIUS employs UDP (User Datagram Protocol) and TACACS+ employs TCP

(Transmission Control Protocol. Some specialized authentication servers employ smart cards or biometric verification in addition to one or more of the above mentioned technologies.

In SESAP, AS requires a username and password to provide a secure communication. The AS receive the user details from the TA .Because the client require a service from the SS only. The ticket will be generated by the entity priorities the SS.TA as the key distribution centre is responsible for generating and assigning related parameters for the vehicles. The SS collects the traffic related information. Such as location, traffic accidents and other important information from RSU, this comes under the range of OBU. The RSU may communicate with 100's of OBU at the same time within its range.

2.2 Crypt Derive Key

In SESAP Crypt Derive Key (CDK) is generated. This is based on fixing some parameter in the VANET. The CDK is generated by the AS by utilizing the MAC[7][8], Unique ID, Client Name, IP Address, and Time Stamp of the individual client who are all in the SESAP queue. The parameters are converted into long string. This process is called Text Streaming (TS).In large VANET the length of text stream will be very long. This Text Stream will be encrypted using SESAP algorithm. The length of the encrypted text stream will vary for each session. For each session the CDK vary because SESAP derive the CDK by Random Number Generation method. This random number generation method works on the Text Stream (TS); consequently, upon receiving the random number. These numbers also vary for each session. So this process ensures security on CDK. This random number is implemented on the TS to generate the CDK[9]. Based on the random number. SESAP generate the TEXT Stream of random length called Random Text Stream (RTS). SESAP picks the fixed stream and this stream is known as Derived Crypt (DC).This DC will be reversed and produced as CDK and it is supplied to the SS and client as Message D. The CDK will be frequently changed for a every single minute and it will generate a new CDK.

3. SESAP PROTOCOL THREATS

3.1 Message verification

In the bogus information attack and its derivatives, one or several legitimate members of the network send out false information to misguide other vehicles about traffic conditions. To cope with such misbehaviour, data received from a given source should be verified by correlating them with those received from other sources. This can be typically done by reputation-based systems. In SESAP, the Message D will hold the CDK or session key. This will be verified with the SS and the client if both are match together the SS will grant access the client/Entity. Similarly the Message C will have the service server request from client but before the request send to the SS it will be authenticated by the verifying the ticket.

3.2 Secure positioning

The most common approach to positioning vehicles is by GPS. But this has several drawbacks, because the precision of GPS is to the order of several meters and degrades in urban environments because of constructions such as buildings and tunnels that weaken GPS signals. The recently introduced DGPS solves the precision problem by reducing the error to a few centimetres [10]. GPS can also be subject to a series of attacks such as signal jamming and spoofing [11]. Some attempts have been made to correct this problem [12], although no definitive solution is available yet.In SESAP, the vehicle host information via TA. These OBU are permitted by the relevant authorities to operate particular public safety applications.

4. SAODV (Secured AD HOC on Demand Vector Routing)

SAODV is s secure variant of AODV reactive routing protocol has been proposed by Zapata and Asokan in 2002, which can be used to shield the route discovery process by providing security characteristics like integrity and authenticity of routing messages.

4.1 How SAODV works

In SAODV, each node checks the security of its neighbours before forwarding route requests. It won't forward route request packets to increase neighbours. This measures, clearly, ensures that malicious nodes will not participate in the data transfer from the source to the destination.

5. SEAD (Secure and Efficient Ad Hoc Distance Vector routing Protocol)

SEAD is a secure proactive routing protocol has been proposed by Hu,Perrig and Johnson based on the Destination-Sequenced Distance Vector Protocol(DSDV).SEAD protects routing updates from attackers by preventing them to change hop count or sequence number in update packets. It authenticates the sequence number and metric of a routing table update message using hash chains elements.

5.1 How SEAD Works

Nodes maintain distance to designation and keep information about the next hop in the optimal path to destination. SEAD routing tables maintain a hash value for each neighbour to prevent attackers to forge better metrics or sequence numbers. The characteristics of SEAD are that it uses a one way hash function. Each node computes a list of hash values[14].

6. SRP (Secure Routing Protocol)

As proposed by papadimitrators and Hass, is an extension of a reactive routing protocol, similar to DSR [15]. The basic idea of SRP is to set up a security association (SA) between the source and the destination node. The SA is usually set up by negotiating a shared key based on the other party public key. The routing path is always sent along with the packets, unencrypted since none of the intermediate nodes have knowledge of the shared key.

7. Comparison of Secure Authentication Protocols

Protocol Name	Routing Strategy	Security Form				
		Rushing Attacks	DOS	Black Hole	Worm Hole	Spoofing
SAODV	On	NO	NO	YES	NO	YES

	Demand					
SEAD	Table Driven	YES	YES	NO	No	YES
SRP	On Demand	NO	YES	YES	NO	YES
EMAP	DSRC	NO	YES	NO	NO	NO
SESAP	DSRC	NO	NO	NO	NO	NO

Yes->Attack Possible
No->Attack Not Possible

8. CONCLUSION

In this Survey, we try to inspect the security issues in the VANETs. First, we introduce the basic characteristics of the VANETs. SESAP for VANET, a secure, efficient and practical scheme. SESAP uses a novel key generation mechanisms CDK which efficiently eliminate intruders. In addition it has a modular feature which renders random generation method for ticket generation which provides basic authenticity for client. We have analyzed the three secure routing protocols such as SAODV, SEAD and SRP. Furthermore, we showed defence against from different types of attacks in the table and this comparison shows which protocol is better in different types of attacks. The main conclusion of this paper is that the choice of which protocol to use depends on the properties of the network.

9. REFERENCES

[1] Dedicated Short Range Communications (DSRC), [On-line] http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] W. Franz, C. Wagner, C. Maihofer, and H. Hartenstein, “Fleetnet: platform for inter-vehicle communications," in *Proc. 1st Intl. Workshopon Intelligent Transportation*, Hamburg, Germany, 2004.

[3] “NoW: Network on Wheels Project," [On-line] http://www.network-onwheels. de, 2007.

[4] “US Vehicle Safety Communication Consortium," [On-line] http://wwwnrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm

[5] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, “Security issues in a future vehicular network," in *Proc. European Wireless, Next Generation Wireless Networks*, vol. 1, pp. 270-274, 2002.

[6] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, and J.-M. Tang, “Framework for security and privacy in automotive telematics," in *Proc.2nd International Workshop on placeMobile Commerce*, pp. 25-32,2002.

[7] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,"*IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46-55, 2003.

[8] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K.Sezaki, “CARAVAN: providing location privacy for VANET," in *Proc.Workshop on Embedded Security in Cars (ESCAR)*, 2005.

[9] K.P. Laberteaux, J.J. Haas, and Y. Hu, “Security Certificate Revocation List Distribution for VANET,” Proc. Fifth ACM int’l Workshop VehiculAr Inter-NETworking, pp. 88-89, 2008.

[10] H. Chan, A. Perrig, and D. Song, “Random Key Predistribution Schemes for Sensor Networks,” Proc. IEEE Symp. Security and Privacy, pp. 197-213, 2003.

[12] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

[13] S. Zhu, S. Setia, S. Xu, and S. Jajodia, “GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks,”J. Computer Security, vol. 14, pp. 301-325, 2006.

[14] A. Wasef and X. Shen, “PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks,” Proc.IEEE Int’l Conf. Comm. (ICC ’08), pp. 1458-1463, 2008.

[15] Y. C. Hu and H. J. Wang, “A framework for location privacy in wireless networks," in *Proc. ACM SIGCOMM Asia Workshop*, China, 2005.