INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online),
Volume 4, Number 2, April- June (2014), pp: 54-59

IJCSERD

SPEEDUP MESSAGE AUTHENTICATION PROTOCOL FOR VANET

Mohan B C
Department of Computer Science and, Engineering, VTU Belgaum,
KVGCE Sullia-574324

Krishna Mohana A.J
Assoc.Professor, Department of Computer Science and Engineering, VTU Belgaum
KVGCE Sullia-574324

Dr. Antony P.J
Director of PG Studies, Department of Computer Science and Engineering, VTU Belgaum
KVGCE Sullia-574324

ABSTRACT

Vehicular Ad Hoc Network (VANET) is an emerging new technology integrating Ad Hoc network, cellular technology and wireless LAN (WLAN) to achieve vehicle to vehicle and vehicle to infrastructure communication for intelligent transportation systems (ITS). In VANET adopts the public key infrastructure (PKI) and certificate revocation a list (CRL) for their security concerns, but it's a time consuming checking process. Speedup Message Authentication Protocol for VANET which replaces the time consuming CRL checking process, the revocation check process in SMAP uses a keyed Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked On-Board Units (OBU). By performing this one can decreases the message loss ratio and decreases in the delay of transferring message is to be secure and efficient.

Key words: Vehicular networks, HMAC, Certificate Revocation.

I. INTRODUCTION

VANET is an emerging technology to achieve intelligent intervehicle communications (IVC), seamless internet connectivity resulting in improved road safety, essential emergency alerts and accessing comforts & entertainments with increased efficiency of the transportation systems [1]. It includes a wide range of technologies such as vehicle communication system, Global Positioning System (GPS), video cameras, digital mapping, and sensing technologies

together with advanced information processing tools. It provides relevant and timely information to users and traffic management systems to improve traffic efficiency, reduce traffic congestion and improve road safety.

VANET is a novel class of Mobile Ad-Hoc Network (MANET) & an important component of Intelligent Transportation System (ITS) [3], [4]. VANET is used for the exchange of messages between vehicle to vehicle (V2V) and also between vehicles and fixed roadside equipment (V2R) as shown in figure.1. Vehicles communicate using Dedicated Short Range Communications (DSRC) that includes wireless technologies like Wi-Fi, IEEE802.11, WIMAX, IEEE 802.15, Bluetooth, IRA and Zig Bee[5],[6].

A well-recognized solution to secure VANETs is to deploy Public Key Infrastructure (PKI), and to use Certificate Revocation Lists (CRLs) for managing the revoked certificates. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed before its transmission. A CRL, usually issued by a Trusted Authority (TA), is a list containing all the revoked certificates. In a PKI system, the authentication of any message is performed by first checking if the sender's certificate is included in the current CRL, i.e., checking its revocation status, then, verifying the sender's certificate, and finally verifying the sender's signature on the received message.

The problem i.e., according to the Dedicated Short Range Communication (DSRC) [8], which is part of the WAVE standard, each OBU has to broadcast a message every 300 msec about its location, velocity, and other telemetric information. In such scenario, each OBU may receive a large number of messages every 300 msec, and it has to check the current CRL for all the received certificates, which may incur long authentication delay depending on the CRL size and the number of received certificates. The ability to check a CRL for a large number of certificates in a timely manner leads an inevitable challenge to VANETs. But this process is time consuming checking process.

To address this problem proposed an approach called Speedup Message Authentication Protocol for VANET (SMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. SMAP is suitable not only for VANETs but also for any network employing a PKI system. To the best of our knowledge, this is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

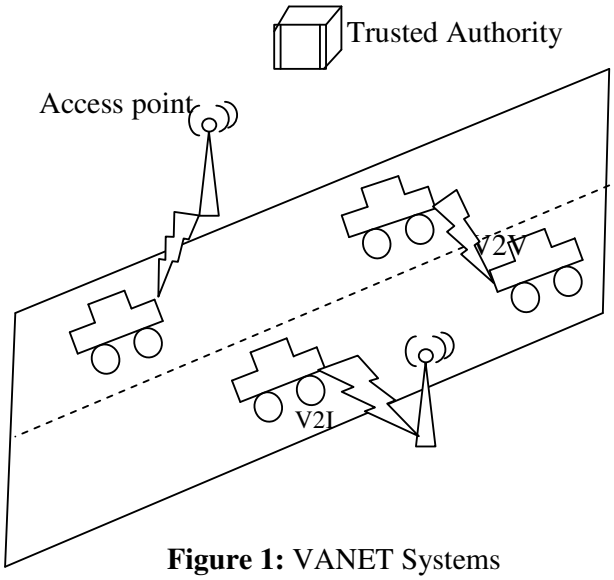

Figure 1: VANET Systems

II. RELATED WORK

CARAVAN: Providing Location Privacy for VANET, in vehicular ad hoc networks, it is possible to locate and track a vehicle based on its transmissions, during communication with other vehicles or the road-side infrastructure. This type of tracking leads to threats on the location privacy of the vehicle's user.

DCS: An efficient distributed certificate service scheme for vehicular networks in the efficient distributed-certificate-service (DCS) [5] scheme for vehicular networks. This scheme offers flexible interoperability for certificate service in heterogeneous administrative authorities and an efficient way for any onboard units (OBUs) to update its certificate from the available infrastructure roadside units (RSUs) in a timely manner.

Design and analysis of a lightweight certificate revocation mechanism for VANET. This [6] mainly focuses on lightweight mechanism for revoking security certificates appropriate for the limited bandwidth and hardware cost constraints of a VANET. A Certificate Authority (CA) issues certificates to trusted nodes, i.e., vehicles. If the CA looses trust in a node (e.g., due to evidence of malfunction or malicious behaviour), the CA must promptly revoke the certificates of the distrusted node.

MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks, Vehicular ad hoc network adopt the public key infrastructure (PKI) and certificate revocation lists (CRLs) to reliably secure the network. In any PKI system, the authentication of a received message is performed by checking that the certificate of the sender is not included in the current CRL, and verifying the authenticity of the certificate and signature of the sender.

Eviction of misbehaving and faulty nodes in vehicular networks, Vehicular networks (VNs) [9] are emerging, among civilian applications, as a convincing instantiation of the mobile networking technology. However, security is a critical factor and a significant challenge to be met. Misbehaving or faulty network nodes have to be detected and prevented from disrupting network operation, a problem particularly hard to address in the life-critical VN environment.

Certificate revocation list distribution in vehicular communication systems, the need to evict compromised, faulty, or illegitimate nodes is well understood in prominent projects designing security architectures for Vehicular Communication (VC) systems. The basic approach envisioned to achieve this is via distribution of Certificate Revocation Lists (CRLs). Nonetheless, the problem of how to distribute CRLs effectively and efficiently has not been investigated. This paper [10] approaches a flexible, simple, and scalable design that leverages on road-side VC infrastructure. This scheme can distribute large CRLs across wide VC regions within minutes, by utilizing a bandwidth of only a few Kbps at each road-side infrastructure units.

III. OVERVIEW OF THE ALGORITHM

The proposed Speedup Message Authentication Protocol (SMAP) uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

A. Distance calculation

First we should find distance between OBU (On Board unit) and (Road Side Unit) by using the distance formula

$$d = \sqrt{(\Delta x)^2 + (\Delta y)^2} = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Figure 2: Euclidean distance

For Example, OBU (car) position (20, 33) and RSU (tower) position (33, 50).

D = Sqrt ((x2 – x1) (x2 – x1) + (y2-y1) (y2-y1))
= Sqrt ((33-20) (33-20) + (50 - 33) (50 - 33))
= Sqrt (169 + 289) = 209764

B. Bandwidth calculation

RSU (Road Side Unit) has to find the size of the file and also find the available bandwidth. By using bandwidth how much data can able to transfer within stipulated time.

C. File segment and merging process

If it's in the available time period, RSU can able to send data to the vehicle1 and if it's not in available time the remaining data send to either vehicle2 or vehicle3 and file merging will happen in vehicle1.

D. File authentication Process

A Trusted Authority (TA), which is responsible for distributing secret keys and certificate number to all OBUs in the network and trigger the HMAC (Hash Message authentication code) by using certificate number and secret key. When start to downloading the file RSU (Road Side Unit) can communicate with TA (Trust Authentication) then TA will check whether secret key is valid or not.

IV. SECURITY ANALYSIS

A. Hash Chain Values

The values of the hash chains are continuously used in the revocation processes, and hence, the TA can consume all the hash chain values. As a result, there should be a mechanism to replace the current hash chain with a new one.

B. Resistance of forging attacks

To forge the revocation check of any on board unit an attacker has to find the current problem. And find the TA secret key and signature. To the revocation check and TA message and signature are unforgeable.

C. Forward Secrecy

The values of the hash chain included in the revocation messages are released to non-revoked OBUs starting from the last value of the hash chain, and given the fact that a hash function is irreversible, a revoked OBU cannot use a hash chain value received in a previous

revocation process to get the current hash chain value, a revoked OBU cannot update its secret key set.

D. Resistance to Replay Attacks

Each message of an OBU includes the current time stamp in the revocation check value check an attacker cannot record REV check at time T and replay it at a later time process as the receiving OBU compares the current time.

E. Resistance to Colluding Attacks

A legitimate OBU colludes with a revoked OBU by releasing the current secret key such that the revoked vehicle can use this key to pass the revocation check process by calculating the correct HMAC values for the transmitted messages. All the security materials of an OBU are stored in its tamper-resistant.

V. PERFORMANCE ANALYSIS

A. Computation Complexity of Revocation Status Checking

Computation complexity of the revocation status checking process which is defined as the number of comparison operations required to check the revocation status of an OBU. Let N_{rev} denote the total number of revoked certificates in a CRL. To check the revocation status of an OBU_u using the linear search algorithm, an entity has to compare the certificate identity of OBU_u with every certificate of the N_{rev} certificates in the CRL, i.e., the entity performs one-to-one checking process. Consequently, the computation complexity of employing the linear search algorithm to perform a revocation status checking for an OBU is $O(N_{rev})$. In the binary search algorithm, the certificate identity of OBU_u is compared to the certificate identity in the middle of the sorted CRL. If the certificate identity of OBU_u is greater than that of the entry in the middle, then half of the CRL with identities lower than that of OBU_u are discarded from the upcoming comparisons. If the certificate identity of OBU_u is lower than that of the entry in the middle, then half of the CRL with identities higher than that of OBU_u are discarded. The checking process is repeated until a match is found or the CRL is finished. It can be seen that at each step in the binary search method half of the entries considered in the search is discarded. Thus, the computation complexity of the binary search algorithm to perform a revocation status checking for an OBU is $O(\log N_{rev})$. In SMAP, the revocation checking process requires only one comparison between the calculated and received values of REV_{check}. As a result, the computation complexity of SMAP is O(1), which is constant and independent of the number of revoked certificates. In other words, SMAP has the lowest computation complexity compared with the CRL checking processes employing linear and binary search algorithms.

VI IMPLEMENTATION

In order to implement the speedup authentication of VANET systems, the HMAC function is used, HMAC is the revocation checking process where the key used in calculating HMAC, each message shared only between non revoked onboard units. In order to achieve the HMAC system first initializes the system by setting up parameters, after initializing the system message verification is done through HMAC keys ,once verification is done revocation of certificate takes place and finally updated to onboard units and ultimately speedup authentication process completed.

CONCLUSION

System proposed a SMAP for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed SMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. In addition, SMAP has a modular feature rendering it integral with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, SMAP can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking. Our future work will focus on the certificate and message signature authentication acceleration.

REFERENCES

[1] wikipedia.org/wiki/Vehicular Ad Hoc Networks.

[2] M. Kihl and M. L. Sichitiu, **Inter-vehicle communication systems: A survey**, *IEEE Communications Surveys &Tutorials,* Vol. 10, Issue 2*,* pp.88–105, 2008.

[3] "US bureau of transit statistics." [Online]. Available: http://en.wikipedia.org/wiki/Passenger vehicles in the United States.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proc. ACM conference on Computer and communications security*, pp. 41–47, 2002.

[5] S. Zhu, S. Setia, S. Xu, and S. Jajodia, "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks," *Journal of Computer Security*, vol. 14, pp. 301–325, 2006.

[6] A. Wasef and X. Shen, "PPGCV: Privacy preserving group communications protocol for vehicular ad hoc .

[7] A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks," *IEEE Trans. On Vehicular Technology*, vol. 58, no. 9, pp. 5214 – 5224, 2009.

[8] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," *Proc. 21st Annual International Cryptology Conference on Advances in Cryptology*, pp. 213–229, 2001.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[10] M. Scott, "Computing the Tate pairing," *Topics in Cryptology, Springer*, pp. 293–304, 2005.

[11] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 19, no. 2, pp. 173–193, Mar. 2000.