

A Secure Hash Message Authentication Code To Avoid Certificate Revocation List Checking In Vehicular Adhoc Networks

¹Mrs.M.Danya Priyadarshini

Francis Xavier Engineering College, Vannarpettai, Tirunelveli
danyapriya88@gmail.com¹

²Mr.Christo Ananth, M.E,

Francis Xavier Engineering College, Vannarpettai , Tirunelveli
ping2christo@yahoo.com

Abstract: A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. The security and performance analysis show that our scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs.

Index terms: Vehicular ad-hoc networks, Digital signature, Hash Message Authentication Code

INTRODUCTION

One of the important research areas in networks over few years is Vehicular ad-hoc networks. Nowadays Vehicular Ad-hoc Network (VANET) provides new research challenges and problems.

VANET is to help a group of vehicles to set up and maintain a communication network among them without using any central base station or any controller. These networks are used for communication among vehicles and between vehicles and roadside equipment. During vehicle-to-vehicle collisions, accidents, drunken driving the intelligent vehicular ad hoc networks helps the vehicles to behave in an intelligent manner which has a kind of artificial intelligence. In vehicular ad-hoc networks every vehicle becomes part of the network and also manages and controls the communication on this network along with its own communication requirements. VANETs are responsible for the communication between moving vehicles in a certain environment. There are many researches are conducted

in VANETS for secure communication. Security is important during the exchanges of data messages between users and RSUs and the location privacy of VANET users who exchange these messages. For this the asymmetric encryption systems based on elliptic curve cryptography (ECC) standard is used. It also suggests two novel mechanisms for data confidentiality and users location privacy in VANETs. But it generates traffic overhead and produces small delay and traffic.

Then a robust authentication protocol was introduced that uses the signature scheme is used to help a vehicle to secretly obtain a secret member key from an RSU, and the group signature scheme is used for V2V communications. During batch verification some messages cannot be verified so average message loss rate grows. Group signature [1] is widely used to achieve anonymous authentication in VANETs for vehicles [1]–[5]. Since the group signature allows any group member to sign a message on behalf of the group without revealing its real identity. In VANETs if the vehicle receiving a message from an unknown entity that needs to check the certificate revocation list (CRL) to avoid communicating with revoked vehicles and then verify the sender's group signature to check the validity of the received message. Secure conditional privacy-preserving authentication scheme called CPAS is introduced for fastest batch verification process in V-to-I communications. To verify a signature, this scheme requires three pairing computations and it causes bottleneck at each vehicle during verifying a number of signatures sequentially transmitted from multiple vehicles causes a processing.

In this paper, a secure hash message authentication code to avoid certificate revocation list checking in vehicular ad-hoc networks. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking, HMAC and Digital signature ensures the integrity of messages. In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden

SYSTEM MODEL AND PRELIMINARIES

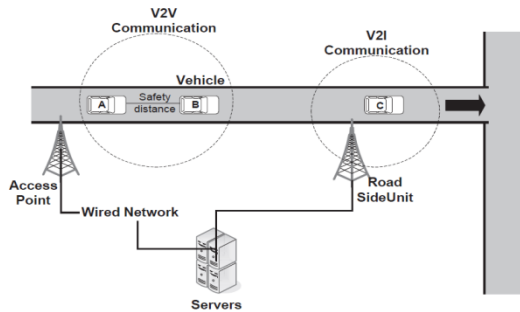


Fig. 1. System model of VANET

A. System Model:

The system model of VANETs are having three basic components namely trusted authority(server), an mobile on board units equipped with vehicles and road side unit.

- **Trusted Authority:** The trusted management center of the network is known as trusted authority. Trusted authority provides registration and certification for RSUs and OBUs when they join the network. It also divides the whole precinct into several domains. First it generates the group key and group signature materials for every domain and then sends these materials to the RSUs in the domain.
- **Road Side Unit:** Road side units are used to manage and communicate with vehicles in their communication range. They are bridges between trusted authority and end users, which connect with trusted authority by wire and OBUs by a wireless channel.
- **On Board Unit:** On board units broadcast traffic-related status information periodically. The status information contains its location, speed, and direction to improve the road environment, traffic safety, and multimedia infotainment dissemination for drivers and passengers. Each vehicle has a tamper-proof device (TPD) to store security-related materials.

B. Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. A digital signature scheme typically consists of three algorithms,

- A key generation algorithm that selects a private key uniformly at random from a set of possible private

keys. The algorithm outputs the private key and a corresponding public key.

- A signing algorithm that, given a message, hash code of message, public key components, random number k (unique for every message) and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of message to attach a code that act as a signature. It is formed by taking the hash of message and encrypting the message with creator's private key.

C. Hash Function, Hash Chain, and HMAC

A one-way hash function $h(\cdot)$ is said to be secure if the following properties are satisfied.

- 1) $h(\cdot)$ can take a message of arbitrary length as input and produce a message digest of a fixed-length output.
- 2) Given x , it is easy to compute $h(x) = y$. However, it is hard to compute $h^{-1}(y) = x$ given y .
- 3) Given x , it is computationally infeasible to find $x' \neq x$ such that $h(x') = h(x)$.

PROPOSED SCHEME

A. System Initialization

The Digital signature algorithm as the underlying signature algorithm employed by TA, RSUs, and OSUs. Here, we use it for its efficiency in the VANETs scenario. In fact, our scheme can be easily changed to use other underlying signature schemes. TA chooses

- 1) Primes p and q such that $q|p-1$, $q \geq 2140$, and $p \geq 2^{512}$;
- 2) $\alpha \in \mathbb{Z}_p$ with order q , i.e., $\alpha^q = 1 \pmod{p}$, and $\alpha \neq 1$;
- 3) a one-way hash function $h: (0, 1)^* \rightarrow (0, 1)^l$;
- 4) a random number $s \in \mathbb{Z}_q^*$ as its own private key so that

$SK_{TA} = s$.

Then, TA computes its public key $PK_{TA} = p^s$ and publishes the tuple $(p, q, \alpha, h, PK_{TA})$ as the system parameters.

B. RSU's Certificate Issuing:

TA divides its precinct into a few domains, each of which includes several RSUs. For RSU R_x in domain DA , TA verifies its identity and issues the certificate $Cert_{TA,R_x}$ as follows.

- 1) TA chooses a random number $SK_{R_x} \in \mathbb{Z}_q^*$ as the private key of R_x and computes the public key $PK_{R_x} = p^{SK_{R_x}}$ for R_x .
- 2) TA generates the signature σ_{TA,R_x} , where $\sigma_{TA,R_x} = Sig_{SK_{TA}}(PK_{R_x} || DA)$.
- 3) TA delivers SK_{R_x} and $Cert_{TA,R_x}$ to R_x , where $Cert_{TA,R_x} = (PK_{R_x} || DA, \sigma_{TA,R_x})$. The delivery of SK_{R_x} must be via a secure channel, such as Secure Sockets Layer.

C. Vehicle's Certificate Issuing

For vehicle V_i , TA issues certificate $Cert_{TA,V_i}$ after verifying its identity as follows.

1) TA chooses a random number $SK_{V_i} \in Z_q^*$ as the private key of V_i and computes public key $PK_{V_i} = p^{SK_{V_i}}$ for V_i .

2) TA generates the certificate $Cert_{TA,V_i}$ of V_i , where $Cert_{TA,V_i} = Sig_{SK_{TA}}(PK_{V_i})$.

3) TA securely delivers SK_{V_i} and $Cert_{TA,V_i}$ to V_i offline during the vehicle inspection.

D. Secure Group Key Distribution and Batch Authentication

For the domain D_A , TA generates group signature keys, containing the public materials and group public key (GPK_{D_A}). Given bilinear parameters (p, G_1, G_2, GT, e), TA generates the group public key as follows.

1) TA selects random generator $g_2 \in G_2$ and computes $g_1 = \psi(g_2)$, where g_1 is the generator of G_1 , and ψ is an isomorphism from G_2 to G_1 such as $g_1 = \psi(g_2)$.

2) TA selects random numbers $h, u, v \in G_1$, and selects numbers $s_1, s_2 \in Z_p$, such that $u^{s_1} = v^{s_2} = h$.

3) TA selects random numbers $\gamma \in Z_p$ and $\lambda \in Z_p^*$ and sets $\omega = g_2^\gamma$.

Here, s_1 and s_2 are master secret keys of domain D_A , which are managed by TA. The public system parameters of domain D_A are ($g_1, g_2, u, v, h, \lambda$), and its group public key is $GPK_{D_A} = \omega$. TA sends the public system parameters and the group public key to all RSUs in D_A . Then, the vehicle and the RSU can realize mutual authentication by using these prestored materials. When a vehicle V_i joins a new domain D_A , it registers at the RSU that it first meets, which can prevent illegal vehicles from joining domain D_A .

1) Registration: When a vehicle V_i joins a new domain, a mutual authentication process between the vehicle and the RSU it first meets should start, notice that in our protocol, if an RSU is compromised, TA will revoke it by broadcasting the information of the domain it belongs to and its identity, i.e., every vehicle can get information of revoked RSUs. First, every RSU in the system periodically broadcasts its certificate, the domain it belongs to, and the group public key. For the RSU R_x in domain D_A , it broadcasts Message 1: ($PK_{R_x}, D_A, Cert_{TA,R_x}, GPK_{D_A}, Sig_{SK_{R_x}}((GPK_{D_A}))$), e.g., every 5 s. When a vehicle V_i gets this message, it first checks whether D_A is a new domain. If it is, this vehicle begins the registration process. By running $Verify(PK_{TA}, PK_{R_x}, D_A, \sigma_{TA,R_x})$, V_i can authenticate the validity of R_x . If $Cert_{TA,R_x}$ is valid, V_i verifies $Sig_{SK_{R_x}}(GPK_{D_A})$ by PK_{R_x} .

Second, after authenticating R_x , and if D_A is a new domain, V_i sends Message 2: ($PK_{V_i}, Cert_{TA,V_i}, xi, Sig_{SK_{V_i}}(xi)$) PK_{R_x} to R_x , where xi is the random number used for computing the group private key GSK_{D_A,V_i} . Notice that the public key PK_{V_i} with certificate $Cert_{TA,V_i}$ is unique in the system; as a result, it is also an identifier of V_i . In our scheme, the public key and the certificate of V_i are encrypted by the public key PK_{R_x} of R_x , and

only R_x can get the plaintext, which protects the privacy of V_i from revealing its identity.

Third, after getting GSK_{D_A,V_i} , R_x sends to V_i Message 3: ($H(GSK_{D_A,V_i}), Sig_{SK_{R_x}}(H(GSK_{D_A,V_i}), xi)$) PK_{V_i} . When V_i receives Message 3, it first decrypts the message by its private key SK_{V_i} and verifies the signature. Fourth, if the signature is valid, V_i sends Message 4: ($T, H(V_i||xi), Sig_{SK_{V_i}}(H(V_i||xi), T)$) PK_{R_x} to R_x , in which T is a timestamp. When R_x receives Message 4 at time T^* , it executes.

In this algorithm, $f(TID_i, y)$ is a bivariate polynomial such as $f(x, y) = s_{0,0} + s_{1,0} \cdot x + s_{0,1} \cdot y + s_{1,1} \cdot xy + \dots + S_{t,t} \cdot x^t y^t$ for $F_q[x, y]$, where x and y are variables, and $S_{i,j}$ is the constant coefficient. K_{m-j-1}^B and K_j^F are group key.

After receiving Message 5 from R_x , V_i executes Algorithm to get the group key for the HMAC computation. The current group key GK_j is computed as

$$GK_j = H(k_j^F + K_{m-j-1}^B) \quad (1)$$

where k_j^F is the forward key chain, and K_{m-j-1}^B is the backward key chain. Finally, R_x and V_i also stores the information.

E. Batch Authentication:

According to the dedicated short range communication (DSRC), each vehicle has to broadcast a security-related message every 300 ms. To ensure the validity of the message source and integrity of these messages, the receiver should verify them. The CRL checking is widely used to exclude invalid vehicles before authentication; however, it needs 9ms to check one identity in the CRL in a group signature based scheme. Therefore, if a vehicle receives n messages, and the number of revoked vehicles is m , this vehicle needs 9 ms to check the source of these messages. Obviously, the CRL checking introduces too much computation delay, greatly degrading the system performance. To improve the efficiency of authenticating the message source, we employ the HMAC checking to replace the time consuming CRL checking. In addition, our method of HMAC checking cannot only authenticate the message source but also check the integrity of messages. Combining with the distributed management, we make valid vehicles in the same domain have the same group key seeds ($K_{m-j-1}^B || k_j^F$) during the registration phase. With the group key seeds, valid vehicles can calculate the group key. Once a vehicle receives the group key, each message sent by this vehicle will attach a HMAC value.

F. Cooperative Authentication

In our basic scheme, even if we ensure that only legal vehicles join the domain and there are no invalid signatures in the batch, the scheme can only verify 274 messages at most per second, which still cannot meet the requirement of authentication speed. Therefore, measures must be taken to solve this problem. By making the neighboring vehicles work cooperatively, their schemes can ensure that a vehicle knows the authenticity of all received messages without verifying all the message signatures. The basic requirements of cooperative authentication scheme are listed in the following.

TABLE-I: Representation of distance and direction of vehicle

Message ID	Direction	Distance(m)
1	Front	50
2	Front	115
3	Behind	45
4	Behind	85
5	Front	130

One verifier should physically be in front of V , whereas the others should be behind V , which means that the verifiers that are used to cooperate with are better to be a pair and can broadcast verification result messages to others. Verifiers should be away from each other as far as possible. The number of verifiers should be neither too small nor too large. This scheme assumes that each security-related message carries the location information of the sender vehicle. When the vehicle V_i receives messages from different senders at the same time, it first extracts location information of senders and then runs the cooperation choice process according to the given requirements to decide which messages should be used for batch verification. V_i checks the received messages every 300 ms and computes the distance between the message senders and itself according to location information.

PERFORMANCE ANALYSIS

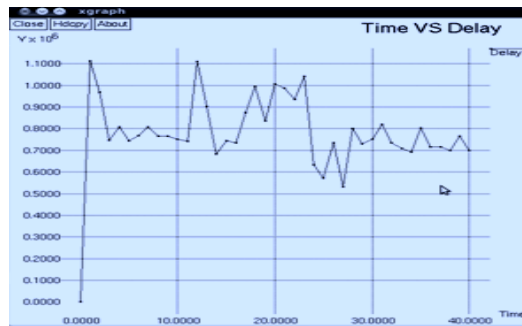


Fig 4.1 Time Vs delay

Figure 4.1 shows At the start of simulation the delay is increased due to packet loss then it gradually decreases.

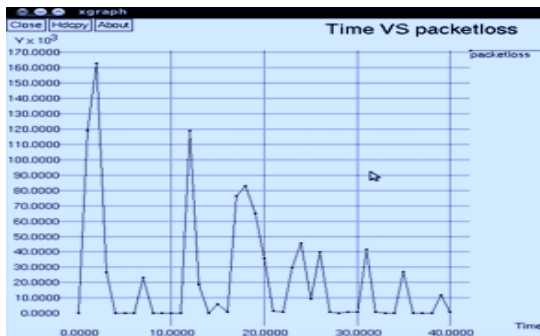


Fig 4.2 Time Vs packet loss

Figure 4.2 shows time versus packet loss graph. The packet loss is high due to high distance between vehicles and road side unit. Then it gradually decreases when the vehicle move towards road side unit.

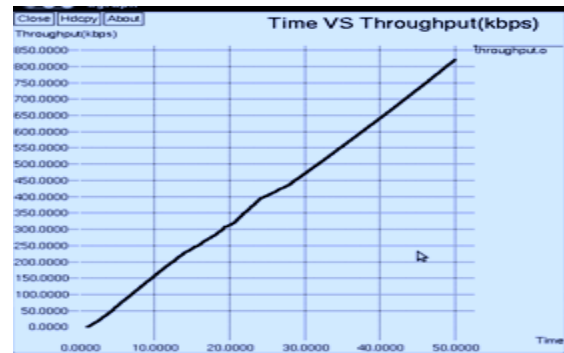


Fig 4.3 Time Vs throughput

Figure 4.3 shows the time versus throughput graph. At the start of simulation the throughput is low because of packet loss. After that it gradually increases and reaches 820kbps.

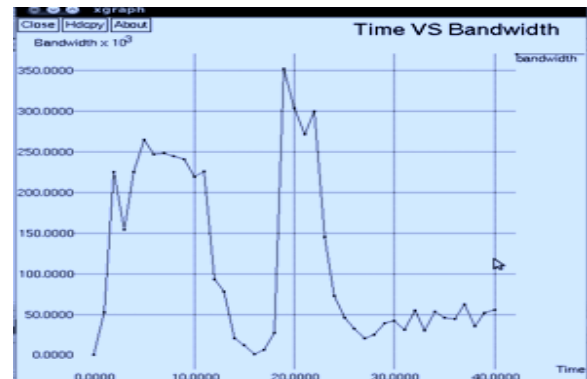


Fig 4.4 time Vs bandwidth

Figure 4.4 shows the time versus bandwidth graph. At the start of simulation the bandwidth is low due to initial stage of packet transmission. During packet transmission it will increases and after the packet transmission it will be decreased.

CONCLUSION

In this paper, a secure hash message authentication code to avoid certificate revocation list checking in vehicular ad-hoc networks is proposed for vehicular ad hoc networks (VANETs). This paper uses HMAC to replace the time-consuming CRL checking and to ensure the integrity of messages before batch verification that reducing the number of invalid messages in the batch. This scheme also use cooperative authentication to further improve the efficiency of our scheme. By employing the given methods, our scheme can meet the requirement of verifying 600 messages per second. The security and performance analysis show that our scheme can achieve

efficient group signature based authentication while keeping conditional privacy for VANETs.

REFERENCES

- [1] S. Jiang, X. Zhu, and L. Wang, "A conditional privacy scheme based on anonymized batch authentication in vehicular ad hoc networks," in Proc. IEEE WCNC, Shanghai, China, Apr. 2013, pp. 2375–2380.
- [2] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 62, no. 2, pp. 536–551, Feb. 2013.
- [3] A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 78–89, Jan. 2013.
- [4] K. A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1874–1883, May 2012.
- [5] Y. Hao, Y. Chen, C. Zhou, and S. Wei, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.
- [6] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "AKABA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.
- [7] A. Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in Proc. IEEE ICC, Cape Town, South Africa, May 2010, pp. 1–5.
- [8] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606–1617, May 2010.
- [9] Albert Wasef, Member, IEEE, Yixin Jiang, and Xuemin Shen, Fellow, IEEE "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks" IEEE Trans. Veh. Technol., vol. 59, NO. 2, Feb. 2010.
- [10] Y. Hao, Y. Cheng, and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in Proc. IEEE GLOBECOM, New Orleans, LA, USA, Dec. 2008, pp. 1–5.
- [11] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368, Nov. 2008.
- [12] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in Proc. Mobile Netw. Veh. Environ., Anchorage, AK, USA, May 2007, pp. 103–108.
- [13] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
- [14] S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in Proc. 8th ACM Int. Symp. MobiHoc, Montreal, QC, Canada, Sep. 2007, pp. 150–159.
- [15] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.