ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (174-179), Month: July - September 2014, Available at: www.researchpublish.com

EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VANETs USING DATA AGGREGATION

[1]Shaiba Wahab, [2]Jemsheer Ahmed P

[1,2]Dept. of Computer Science and Engineering, MEA Engineering College,
Perinthalmanna, Kerala, India

***Abstract*: A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. For security Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs). In the Public Key Infrastructure system the authentication of a received message is performed by checking if the certificate of the sender is included in the current Certificate Revocation Lists (CRLs) and verifying the authenticity of the certificate and signature of the sender. But it takes more time for CRL checking process. So in order to overcome this problem we use an efficient revocation check process in EMAP 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 (OBUs). In addition, EMAP uses a novel probabilistic key distribution which enables non-revoked OBUs to securely share and update a secret key. To conquer computation overhead we introduce the data aggregation using probabilistic checking that can accelerate message verifications and significantly reduce computational overhead while retaining satisfactory security.**

***Keywords:* Vehicular networks, communication security, message authentication, certificate revocation, data aggregation.**

I. INTRODUCTION

Vehicular Ad hoc networks(VANETs)have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs).Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic communication modes, which, respectively, allow OBUs to communicate with each other and with the infrastructure RSUs.

To ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages, each OBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. In this paper, we introduce an expedite message authentication protocol1 (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function. EMAP 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.

Data aggregation in VANETs has been analyzed in several papers. Details about speed and information are exchanged within nodes in the cluster and as soon as the cluster grows, information records are aggregated. Such a mechanism reduces the amount of data transmitted in a group.

II. RELATED WORK

In VANETs, the primary security requirements are identified as entity authentication, message integrity non repudiation, and privacy preservation. The PKI is the most viable technique to achieve these security requirements. PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

Studer et al. propose an efficient authentication and revocation scheme called TACK. TACK adopts a hierarchy system architecture consisting of a central trusted authority and regional authorities (RAs) distributed all over the network. The authors adopted group signature where the trusted authority acts as the group manager and the vehicles act as the group members. Upon entering a new region, each vehicle must update its certificate from the RA dedicated for that region. The vehicle sends a request signed by its group key to the RA to update its certificate; the RA verifies the group signature of the vehicle and ensures that the vehicle is not in the current Revocation List (RL). After the RA authenticates the vehicle, it issues short lifetime region-based certificate. This certificate is valid only within the coverage range of the RA. Although TACK eliminates the CRL at the vehicles level, it requires the RAs to verify the revocation status of the vehicles upon requesting new certificates. To check the revocation status of a vehicle, the RA has to verify that this vehicle is not in the current RL by performing a check against all the entries in the RL. Each check requires three pairing operations. Consequently, checking the revocation status of a vehicle may be a time consuming process. The authors suggested to use an optimized search method to remedy the computationally expensive RL check.

There are some works addressing the problem of distributing the large-size CRL in VANETs. Raya et al. introduce Revocation using Compressed Certificate Revocation Lists (RC2RL), where the traditional CRLs, issued by the TA, are compressed using Bloom filters to reduce its size prior to broadcasting. Papadimitratos propose to partition the CRL into small pieces and distribute each piece independently. Haas develop a mechanism to reduce the size of the broadcast CRL by only sending a secret key per revoked vehicle. On receiving the new CRL, each OBU uses the secret key of each revoked vehicle to reproduce the identities of the certificates loaded in that revoked vehicle, and construct the complete CRL. It should be noted that although the broadcast CRL size is reduced, the constructed CRL at each OBU, which is used to check the revocation status of other entities, still suffers from the expected large size exactly as that in the traditional CRLs where all the identities of the certificates of every revoked OBU are included in the broadcast CRL.

The probabilistic approach is a promising technique for the key management in ad hoc networks Zhu et al. introduce the GKMPAN protocol which adopts a probabilistic key distribution approach based on predeployed symmetric keys. The GKMPAN is efficient and scalable for wireless mobile networks, because it takes the node mobility into consideration.

III. PROPOSED SYSTEM

In this paper, we propose an Expedite Message Authentication Protocol (EMAP) to overcome the problem of the long delay incurred in checking the revocation status of a certificate using a CRL. EMAP employs keyed Hash Message Authentication Code (HMAC) in the revocation checking process, where the key used in calculating the HMAC for each message is shared only between unrevoked OBUs.

3.1 Expedite Message Authentication Protocol

The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution.

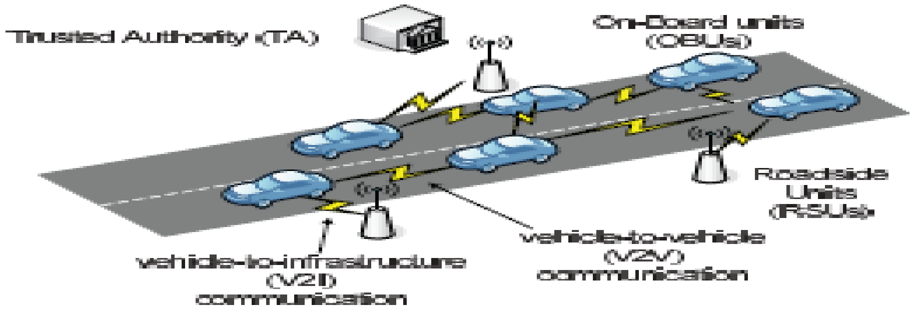
Trusted Authority (TA)
On-Board units (OBUs)
Roadside Units (RSUs)
vehicle-to-vehicle (V2V) communication
vehicle-to-infrastructure (V2I) communication

Figure 3.1 System Architecture

3.1.1 System Modules

As shown in Fig. the system model under consideration consists of the following:

1. A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network.
2. Roadside units (RSUs), which are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
3. OBUs, which are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

According to the WAVE standard [9], each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the security materials, e.g. secret keys, certificates, etc., of the OBU. Also, the HSM in each OBU is responsible for performing all the cryptographic operations such as signing messages, verifying certificates, keys updating, etc. We consider that legitimate OBUs cannot collude with the revoked OBUs as it is difficult for legitimate OBUs to extract their security materials from their HSMs. Finally, we consider that a compromised OBU is instantly detected by the TA.

3.2 Data Aggregation

In our data aggregation scheme signatures generated by different vehicles to alert about the same problem are combined. Thus, signature combination in a single packet increases packet size while the number of vehicles that can confirm the information also increases. So the effect is again an overload of the channel. Second, the fact that the information is signed does not mean that it is correct. The receiver in this scheme must verify the signatures, which means a delay in testing. It would equal or even exceed the basic model time. To solve this problem, we propose to set a maximum number of signatures that may contain the packet and a granularity. This will prevent the packet to grow infinitely in addition to define ranges where the information must be signed. Finally, in order to solve the signature verification delay, we propose a probabilistic scheme to verify only a few signatures. All these security mechanisms are detailed below.

3.2.1 Geographic Zones

Three different geographic distances are defined depending on where information is considered interesting by the receivers. In particular, three geographic zones are defined with respect to the reported event.

• Danger zone, which is the area defined by the innermost Distance, where the hazard can be detected directly by vehicles.

• Uncertainty zone, where nodes cannot confirm the information directly, but they have to make decisions quickly because In a short period of time they will be in the danger zone.

• Security zone, where nodes behave according to the store-and-carry paradigm, collecting evidences about the hazard in The form of aggregated packets.

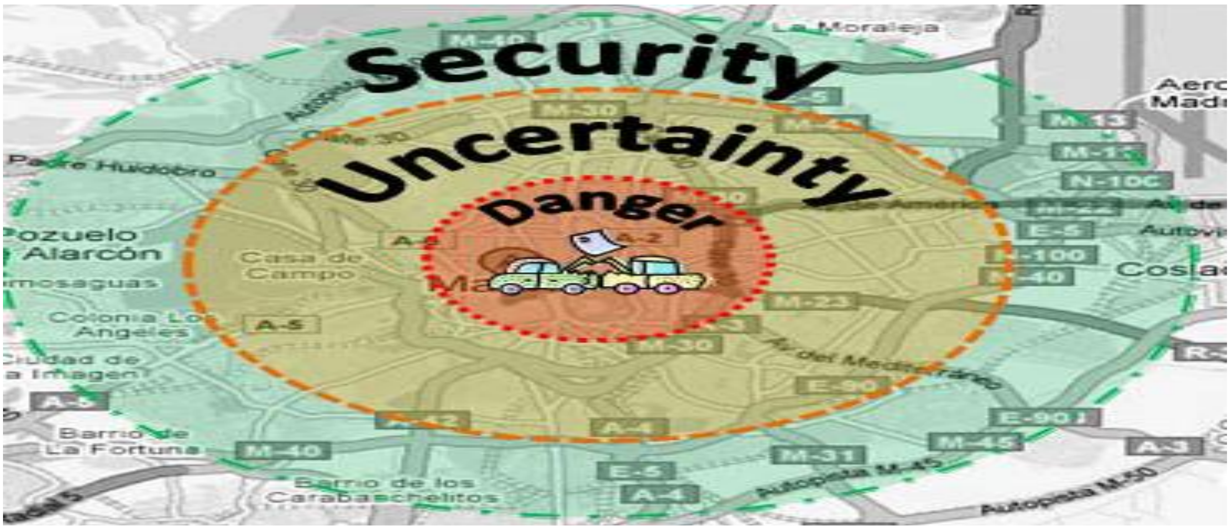

Figure 3.2. Geographic Zones

3.2.2 Packet Size and Granularity

As discussed in the previous section, packet size must be fixed to a maximum value *T* that does not over-saturate the communication medium and allows delivering the packet quickly. In this case the packet size should be large enough To have sufficient evidence of the same danger without exceeding the maximum supported by the wireless channel.

For this assessment, we need to define a certain criterion to attach cryptographic clues in the aggregate packets. On the one hand we propose to attach in the first and second packet position the borders of a common area where vehicles share common values about an incident. So, if a vehicle is able to present valid signed information about all borders of an aggregate area it can be alleged to be valid. This is the case of V1 and V6 in Figure 3 where the vehicles define the hazard area of an incident.

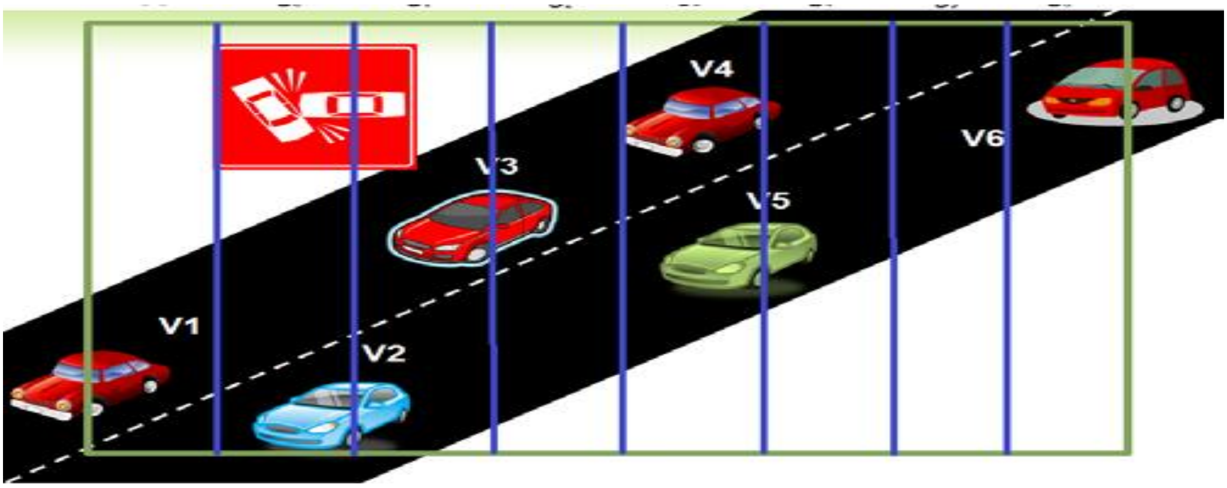

Figure 3.3. Hazard Area

3.2.3 Probabilistic Verification

Note that probabilistic verification only applies to vehicles which are unable to verify the information that reaches them that is, when they receive a warning message about an incident that is not covered by the coverage of their antenna.

In this case, if a vehicle wants to ensure the authenticity of the received message, it must verify all the message's signatures. As we already mentioned, it is inefficient to check all the signatures contained in a packet, but it will be necessary to verify the information before giving it as valid and send it to the driver. In order to fix the problem only a few signatures are proposed to be verified. In this section, we introduce an authentication scheme that allows making sure that the message is valid, without checking all the signatures of the received message.

```
function Main(...)
    bool P[c];
    Thread H[c];
    for (i=0;i<c;i++) do
        if (ProbH[i]=1) then
            P[j]=H[i](VerifySignature(S,M));
            j++;
        end if
    end for
    if (IsTrueAll(P)) then
        return ReliableMessage;
    else
        if (NotIsTrueAll(P)) then
            return NotReliableMessage;
    else
      return VerifyNodeReputation;
    end if
  end if
end Main

bool function VerifySignature(Signature S,text M)
  if (IsValid(S)) then
    return true;
  else
    return false;
  endif
end function
```

In the algorithm shown before, *H[i]* denotes a thread for the variable *i* that takes an integer value between 1 and *n*, where *n* denotes the number of aggregated signatures. When a vehicle receives a message, the main process launches as many threads as signatures the message contains. Before the main process launches the threads, it checks whether the message contains enough signatures to determine whether the message has been confirmed by a significant number of vehicles. Each thread *H[i]* determines whether to verify the signature with a verification probability *p*. If *H[i]* defines a verification process, and the signature is proved to be valid, *H[i]* returns a *true* value informing that it is a valid signature. Otherwise, it returns a *false* value. The results of all those threads are stored in a structure *P*. If all fields in the structure *P* are proved to be valid, it is interpreted as evidence that all the verified signatures are correct so the message is accepted as valid. On the other hand, if *P* contains some thread results that is invalid, this could be interpreted as false message. If most threads indicate that the message is false, it is taken as invalid message, otherwise it is valid. If there is a tie or a questionable amount of false signatures, the reputation information stored by the vehicle about the different nodes which have signed the message is checked. In this case, only those nodes that have good reputations due to their active and correct participation in the network are trusted and accepted.

IV. CONCLUSION AND FUTURE WORK

The paper proposes EMAP 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 EMAP 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, EMAP has a modular feature rendering it integrable with any PKI system. Furthermore, it is resistant to common attacks while outperforming the authentication techniques employing the conventional CRL. Therefore, EMAP 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.

This paper shows the need to address a security problem in VANETs that consists in determining whether road traffic Information available to a driver is trustful or not. In particular, we propose a scheme to generate aggregated packets that cannot be replaced by an adversary. Different ideas are here combined in a new data aggregation method.

First, vehicles who agree with the generated information can sign the packet. Secondly, in order to avoid that the packets Grow indefinitely, signatures are generated according to a granularity defined depending on the type of via and making it impossible for an attacker any packet modification. At the same time, two signatures delimiting the region are generated. If more than one vehicle coincides in granularity, upgrade and replacement of signatures from the same granularity are proposed to keep the information up-to-date. On the other hand, when an aggregated packet reaches a vehicle, this may verify the information by checking the attached signature. In order to avoid the delay produced by signature checking, a probabilistic scheme according to which a few signatures are chosen to be checked is here proposed. The number of chosen signatures must be a balance so that it allows ensuring the validity and correctness of information, and at the same time it does not cause any avoidable delay in obtaining the information.

REFERENCES

[1] P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, “Privacy and Identity Management for Vehicular Communication Systems: A Position Paper,” Proc. Workshop Standards for Privacy in User-Centric Identity Management, July 2006.

[2] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing Location Privacy for VANET,” Proc. Embedded Security in Cars (ESCAR) Conf., Nov.2005.

[3] Wasef, Y. Jiang, and X. Shen, “DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks,” IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[4] M. Raya and J.-P. Hubaux, “Securing Vehicular Ad Hoc Networks,” J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[6] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, “Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in Vanets,” IEEE Trans. Vehicular Technology, vol. 61, no. 1, pp. 86-96, Jan. 2012.

[7] US Bureau of Transit Statistics, http://en.wikipedia.org/wiki/Passenger_vehicles_in_the_United_States, 2012.

[8] J. Serna, J. Luna, M. Medina “Geolocation-based Trust for Vanet’s Privacy”, Journal of Information Assurance and Security, vol. 4, no. 5, pp.432-439, 2009.

[9] K. Ibrahim, M.C. Weigle, “Accurate data aggregation for VANETs”, in Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks, VANET '07, 2007.

[10] S. Eichler, C. Merkle, and M. Strassberger, “Data aggregation system for distributing inter-vehicle warning messages,” in 31st IEEE Conf. on Local Computer Networks, pp. 543-544. IEEE Computer Society, November 2006.

[11] F. Picconi, N. Ravi, M. Gruteser and L. Iftode, “Probabilistic Validation of Aggregated Data in Vehicular Ad-Hoc Networks,” in Proceedings 3rd Int'l. Workshop Vehicular Ad Hoc Networks, ACM Press, pp. 76-85, 2006.