AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Certificate Revocation List Distribution using Minimum Spanning Tree

[1]Anitha G. and [2]Dr.Hemalatha M.

[1]*Research and Development Centre, Bharathiar University, India*
[2]*Dean, S.N.S.Rajalakshmi College of Arts and Science, India*

Address For Correspondence:
Anitha G., 1Research and Development Centre, Bharathiar University, India
E-mail: florenceanitha7@gmail.com

ARTICLE INFO

Article history:
Received 12 February 2016
Accepted 12 March 2016
Available online 20 March 2016

Keywords:
Certificate Revocation List, Vanet, Security, DMSTP, Triple D Method

ABSTRACT

Vehicular ad-hoc network provides efficient traffic information, alert messages, emergency warning, entertainment and infotainment dissemination. It places a vital role in safety fields such as defense system, traffic system, etc. Even though, some advanced digital signature and Public Key Infrastructure method were used for security, intrusion detection and prevention of malicious vehicle from jeopardizing the safety of the other vehicle is an inevitable challenge in networks. Bilinear pairing method is used in an anonymous Id creation for each vehicle. The CRL checking process has been done using Bloom Filter method which avoids false negative. It replaces the time-consuming CRL Checking process. It reduces message loss ratio by fast revocation checking and CRL updating method as well as it needs very less memory space compared to other methods. Previously, bi-directional flooding method has been proposed for CRL dissemination. This paper mainly focuses on CRL dissemination based on Distance, Direction and Density (3D) using the DMSTP (Directional Minimum Spanning Tree Protocol).Compare to bi-directional flooding method, it reduces the congestion by disseminating the CRL to the most needed node in the roadmap.

INTRODUCTION

Vehicular ad hoc networks are placing a vital role for developing a road safety applications such as incident warning, collision detection, road traffic control systems, collision avoidance, etc. It is also used in infotainment and entertainment. It consists of two main entities which are On-Board Units and Road-Side Units. On-board Unit is fastened in all the vehicles. The road-side unit is fastened in road side at uniform interval distances. There are two types of communications to provide and share information: Vehicle to Vehicle (V2V) communications and Vehicle to Infrastructure (Road Side Unit) communications. CRL dissemination is also placed a vital part in Vanet security. Because, any OBU receives any message, it checks in its current CRL. So, CRL should be disseminated quickly to the most needed OBU first instead of sending to all OBUs in the signal covered region. The most needed OBU can be found using the parameters distance, direction, density and speed. Based on these parameters, Kruskal's minimum spanning directed graph techniques have been used to find the most needed OBU.

II. Related Work:

The four main security requirements in VANET are Privacy (User, Location, etc.,) preservation, Message Authentication, Message Integrity and Nonrepudiation. Albert Wasef and Xuemin Shen (2013) introduced an expedite message authentication protocol (EMAP) which replaces the CRL checking process with an efficient revocation checking process using a fast and secure HMAC function. EMAP is suitable for any network (VANET, MANET, etc.,) employing a PKI system. The CRL checking process has been done and compared

To Cite This Article: Anitha G. and Dr.Hemalatha M., Certificate Revocation List Distribution using Minimum Spanning Tree. ***Aust. J. Basic & Appl. Sci.,*** *10(1): 670-675, 2016*

with various searching algorithms such as linear search, binary search, hashing. As a result, the authentication delay is reduced CRL checking process in VANET by using the hash function method. Ghassan Samara *et al*. (Samara, G., 2010) proposed an efficient certificate management in VANET which avoids the CRL checking process. Because each vehicle must have a certificate of transmission. Even an adversary vehicle can transmit the message with its certificate. If any vehicle is a legitimate, it has a valid certificate (VC) or else it has an adversary certificate (AC). Each certificate has its own format. While receiving a message, the receiver checks the type of certificate. If it is valid certificate, the message will be accepted or else it will be discarded. Julien Freudiger *et al*. (2007) introduce CMIX protocol, which maintains the *location privacy* in VANET by changing identifiers in the presence of a global passive adversary. This protocol creates cryptographic mix-zones at road intersections. It prevents computationally-bounded eavesdroppers while preserving the functionality of safety messages. Its process is divided into three phases such as Key establishment phase, key forwarding phase and key update phase. In the key establishment phase, all legitimate vehicles within the mix-zone obtain a symmetric key from the roadside unit (RSU) of the mix-zone, and use this key to encrypt all their messages while within the zone. To ensure the functionality of safety messages, the mix-zone key can be received by nodes approaching the mix-zone with the help of a key forwarding mechanism, and the RSU can swap to a new key through a key update mechanism. The location privacy has been achieved by combining mix-zones into mix-networks in VNs.Jason J. Haas *et al*. (2011) propose an Efficient Certificate Revocation List Organization and distribution which reduced the CRL size. It was an efficient mechanism to check the presence of certificate Id in the CRL. CRL updates have been done by using lightweight mechanism. CRL checking process (checking whether the certificate's identifiers are present in the CRL or not) is done quickly by storing the certificate in a Bloom Filter which is a probabilistic data structure (i.e., searching has a non-zero, but small false positive rate) and has a constant (O(1)) cost in terms of computation for searching and storage. Ghassan Samara (Sampigethaya, K., 2005) proposed Certificate Revocation Management in VANET which reduces the channel load resulted from frequent warning broadcasting happened in the adversary discovery process. Accusation Report produces a heavy channel load. Because, it receives the adversary report from all the vehicles. It replaces the Certificate Revocation List (CRL) by Local Revocation List (LRL). It reduces searching delay and high load on the channel. As a result, adversary search process is much easier and faster. In, Hubaux identify the specific issues of security and privacy challenges in VANET, and indicate that a PKI should be well deployed to protect the transmitted messages and also authenticate all the network entities.

In (Raya, M., J.P. Hubaux, 2007), Raya and Hubaux use a classical PKI to provide secure and privacy preserving communications to VANET. In this approach, each vehicle needs to preload a large set of anonymous certificates. The loaded certificates in each vehicle should be huge to maintain security and privacy preservation for a long time, e.g., one year. Each vehicle should update its certificates from a central authority during the annual inspection of the vehicle. In this approach, revoking a single vehicle implies revoking the large number of certificates loaded in it. Anitha *et al*. proposed the authentication protocol using region based certificate revocation method. Vanet area is classified into regions and Certificate revocation list is maintained separately for each region. In this case, any vehicle receives any message, it checks in the region CRL instead of searching in a single CRL. She also proposed CRL dissemination using Road map and modified bidirectional flooding method.

III. System Architecture:

The system model has the following entities. It is shown in Fig 1.

1. Trusted Authority (TA): It distributes anonymous certificates for all the on-board units which are attached in Vehicles and the secret key for all VIRSUs & CURSU in VANET.
2. Road Side Unit (RSU): It is fixed and distributed all over the network. It is communicated with Trusted Authority and the vehicles. It can store Certificate Revocation List (CRL).
3. On Board Units (OBU): It is embedded in vehicles. It can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

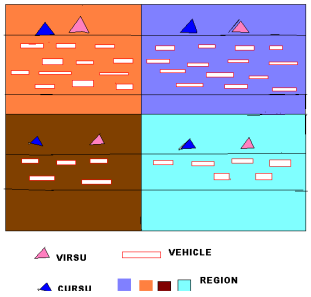

Fig. 1: VANET Architecture.

Australian Journal of Basic and Applied Sciences, 10(1) January 2016, Pages: 670-675

Trusted Authority creates a set of anonymous certificates for all OBUs in the network and also it distributes a private and public key of OBUs to the corresponding region VIRSU and CURSU in the network. The total network areas are classified into regions. Each region has two types of RSUs.

- Vehicle Info-collection RSU (VIRSU): It maintains location, direction, speed, CRL flag value of the vehicles and the density of the road. Here CRL flag value denotes whether it updates its data at present or not.
- CRL updating RSU (CURSU): CRLs can be transferred in between all the regions through CURSU. This CRL contains the invalid certificate Id of the OBUs which are in its region.

3.1. System Initialization:

A set of anonymous certificates is created by TA for all the OBUs in the network. Each certificate has its certificate identity (cert_Id). Certificate Identity consists of two fields such as private key and public key. It also provides secret key to all the CURSU. Each CURSU contains the list of Certificate Identity for all the OBUs in their region. Only the public key of this list is passed to all the OBU's in the region. Secret key generation has been done using bilinear pairing method. It is not focused in this paper. Because it was presented in the previous work.

IV. CRL Dissemination:

Service channel is divided into two parts based on the time period. First, each vehicle is sending its location, direction and speedto the neighbor vehicles in the region. Secondly, CRL dissemination is taken place using the parameters distance, direction, density and speed.

Phase 1:

VIRSU collects all OBUs information such as location, direction and speed.

Phase 2:

CRLs can be routed in the region based on the information received in VIRSU.

The VIRSU passes the CRL to the OBUs, which are in rightmost and leftmost diagonal positions on the road. If the road is multilane, it passes the CRL to the twoOBUs which are in opposite direction way lane.If it is n lane bidirectional road, CRL should be passed to the first and the n^{th} lane road OBUs which has been entered in the region at last.

OBU Selection:

Lane n
w
h
Lane 2
Lane 1

(x1,y1) (x2,y2)
w -> width of the lane
h -> Height of the lane
(x_1,y_1) and (x_2,y_2) are the two end points of the first lane.

The height of the lane can be measured using the formula

$h= \sqrt{((x_2-x_1)^2+(y_2-y_1)^{2)}}$

First OBU:

$OBU_f(x,y) = x$ | if x1< x <x1+u
Y | if y1 < y <y1+w
Else
if y1+w < y < y1+2w
if y1+(n/2 – 1)w <y < y1+ (n/2)w

Second OBU:

$OBU_f(x,y) = x$ | if x1< x <x1+u
Y | if y1 < y <y1+w
Else
if y1+w < y < y1+2w
if y1+(n/2 – 1)w <y < y1+ (n/2)w

Here, (x1,y1) and (x1,y2) are the edge points of a road.

Australian Journal of Basic and Applied Sciences, 10(1) January 2016, Pages: 670-675

This OBU takes the nearest OBUs address on the same road in both direction and passes the CRL. It is passed using the modified flooding method (MFM). In this method, the CRL is passed to nearest OBU instead of sending the CRL to all the OBUs in the region.

Algorithm to find the nearest OBU in the following MSTP algorithm:

Step 1: Select the two edge points (x1,y1)& (x2,y2) on the road in the region.
Step 2: If any point satisfies the previous steps, the distance between the two nodes can be calculated by using the formula.
Distance =sqrt $((x_2-x_1)^2-(y_2-y_1)^2)$
Step 3: The shortest distance OBU address can be captured and send the CRL to the same.

Algorithm for directional MST (Minimum Spanning Tree) Propagation [DMSTP] Method:

Require: <Vehicles in one region (a road segment) forming Graph G>
Ensure: < Graph (T)>
1: let *G* be the graph containing candidate vehicles that can be joined together with the selected vehicle in a road segment;
2: let *T* be an empty graph;
3. Let M be the number of vertices in a graph T.
4. Let N be the number of vertices (OBUs) which are moving in the same direction as OBUf in Graph G.
5.Add OBUf into T .
6. Assign 1 to M.
7. while M < N
8. calculate the out-degree(OD) of the vertex OBUf.
9. Let (V,E) are OD edges.
10. Find (v,e) have the smallest metric distance(d) in (V,E) in graph G using algorithm 2..
11. remove (*v*, *e*, *w*) from *G*
12: add *v* and *e* to *T*
13. Assign the added V as OBUf
14. Increment the value of M by 1
15. End while
16. let Hbe an empty graph;
17. Let m be the number of vertices in a graph H.
18. Let n be the number of vertices (OBUs) which are moving in the same direction as OBUs in Graph G.
19. Add OBUs into H .
20. Assign 1 to m.
21. while m < n
22. calculate the out-degree(OD) of the vertex OBUs.
23. Let (V,E) are OD edges.
24. Find (v,e) have the smallest metric distance(d) in (V,E) in graph G using the algorithm 2.
25. remove (*v*, *e*, *w*) from *G*
26: add *v* and *e* to H
27. Assign the added V as OBUs
28. Increment the value of m by 1
29. End while
30. return T and H.

V. Performance Evaluation:

5.1. Authentication Delay:

We compare the message authentication delay employing the CRL with that employing this RMDP protocol to check the revocation status of an OBU. The authentication of any message is performed by three consecutive phases: the sender's revocation status checking, the sender's certificate verification, and the sender's signature verification. In the first authentication phase, we can apply any searching method for checking the revocation status of the sender. In this method, bloom filter technique has been used to check the revocation status. While CRL distribution period, it is not sending the CRL to all the nodes. Instead of this, it sends it to nearest OBU in the road. It is shown in Fig 2.

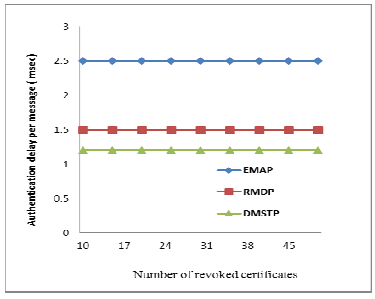

Fig. 2: Authentication Delay.

5.2. End-to-End Delay:

It is the time to transmit the data from the sender to the receiver. It depends on the number of revoked certificates included in the CRL and also it depends on the CRL checking process. The proposed system consists of region-wise CRL which consists of revoked certificates in its region as well as it uses directional minimum spanning tree method. The time taken for sending the data from sender to the receiver is less when compared to EMAP method. It is shown in Fig 3.

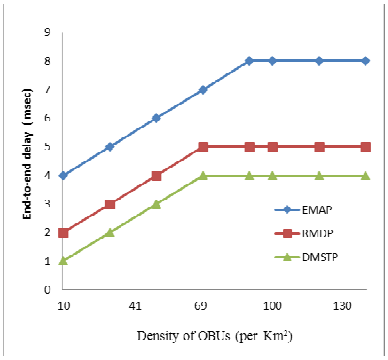

Fig. 3: End-to-end delay.

5.3. Message Loss Ratio:

The average message loss ratio is defined as the average ratio between the number of dropped messages every 300 milliseconds, due to the message authentication delay, and the total number of received messages every 300 milliseconds by an OBU. It increases with the number of OBUs within the communication range. In this protocol, only limited OBUs may be involved in communication within the region and also it incurs the minimum revocation status checking. As a result, this DMSTP decreases the message loss ratio compared to that employing either the linear or binary or EMAP. It is shown in Fig 4.

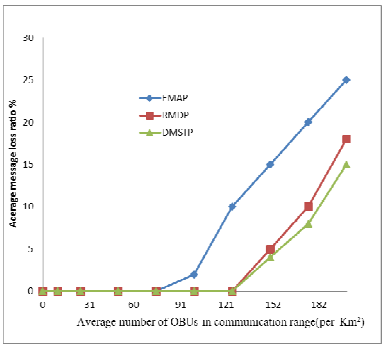

Fig. 4: Message Loss ratio.

5.4. Communication Overhead:

In this protocol and EMAP, each OBUu broadcast the message in the form (M || T_{stamp} || carte(PID_u, PK_u, $sig_{TA}(PID_u || PK_u)$) || sig_u (M || T_{stamp}) || REV_{check}). In the WAVE standard, a signed message has the certificate and signature of the sender with a time stamp on the transmitted message. The additional communication overhead incurred in RMDP, DMSTP and EMAP compared to that in the WAVE standard is mainly due to REV_{check}. It reduces the communication overhead by sending the CRL to the nearest one in the region.

VI. Conclusion:

In this paper, we have proposed protocol for VANET which provides message authentication and efficient certificate revocation list management by replacing the time-consuming CRL checking process with a fast revocation checking process with Bloom filter. And also, CRL distribution is performed based on Directional Minimum Spanning Tree Protocol using the main three parameters Distance, Direction and Density. Instead of sending the CRL to all the OBUs in the region, it sends to the only one nearest OBUwhich is in same direction lane on the road. It reduces message loss ratio, space complexity and congestion in RSU and OBU by introducing region-based revocation checking process and also it maintains privacy by using anonymous keys for OBUs. In future, most efficient CRL distribution technique may be proposed including the speed parameter.

REFERENCES

Wasef, A., X. Shen, 2013. EMAP: expedite message authentication protocol for vehicular ad hoc networks. *Mobile Computing, IEEE Transactions on*, *12*(1): 78-89.

Samara, G., W.A. Al-Salihy, R. Sures, 2010. Efficient certificate management in VANET. In *Future Computer and Communication (ICFCC), 2nd International Conference on*, 3: V3-750. IEEE.

Freudiger, J., M. Raya, M. Félegyházi, P. Papadimitratos, 2007. Mix-zones for location privacy in vehicular networks.

Raya, M., J.P. Hubaux, 2007. Securing vehicular ad hoc networks.*Journal of Computer Security*, *15*(1): 39-68.

Haas, J.J., Y.C. Hu, K.P. Laberteaux, 2011. Efficient certificate revocation list organization and distribution. *Selected Areas in Communications, IEEE Journal on*, *29*(3): 595-604.

Sampigethaya, K., L. Huang, M. Li, R. Poovendran, K. Mastsuura, K. Sezaki, 2005. Providing Location Privacy for VANET. *Proceedings of Embedded Security in Cars ESCAR. CARAVAN*.

Haas, J.J., Y.C. Hu, K.P. Laberteaux, 2009. Design and analysis of a lightweight certificate revocation mechanism for VANET. In*Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking* (pp: 89-98). ACM.

Sun, Y., R. Lu, X. Lin, X.S. Shen, J. Su, 2010. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *vehicular Technology, IEEE Transactions on*, *59*(7): 3589-3603.

Lu, R., X. Li, T.H. Luan, X. Liang, X. Shen, 2012. Pseudonym changing at social spots: An effective strategy for location privacy in vanets.*Vehicular Technology, IEEE Transactions on*, *61*(1): 86-96.

Wasef, A., X. Shen, 2009. MAAC: Message authentication acceleration protocol for vehicular ad hoc networks. In *Global Telecommunications Conference,. GLOBECOM. IEEE* (pp: 1-6). IEEE.

Hubaux, J.P., S. Capkun, J. Luo, 2004. The security and privacy of smart vehicles. *IEEE Security & Privacy Magazine*, *2*(LCA-ARTICLE-2004-007), 49-55.

Raya, M., J.P. Hubaux, 2007. Securing vehicular ad hoc networks.*Journal of Computer Security*, *15*(1): 39-68.

Raya, M., P. Papadimitratos, I. Aad, D. Jungels, J.P. Hubaux, 2007. Eviction of misbehaving and faulty nodes in vehicular networks. *Selected Areas in Communications, IEEE Journal on*, *25*(8): 1557-1568.

Papadimitratos, P.P., G. Mezzour, J.P. Hubaux, 2008. Certificate revocation list distribution in vehicular communication systems. In*Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking* (pp: 86-87). ACM.

Laberteaux, K.P., J.J. Haas, Y.C. Hu, 2008. Security certificate revocation list distribution for VANET. In *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking* (pp: 88-89). ACM.

Nowatkowski, M.E., H.L. Owen, 2010. Certificate revocation list distribution in VANETs using most pieces broadcast. In *IEEE SoutheastCon (SoutheastCon), Proceedings of the* (pp: 238-241). IEEE.

Randhawa, N.K., 2012. Design and Implementing PGP Algorithm in Vehicular Adhoc Networks (VANETs). *International Journal of Engineering Research and Applications*, *2*(3): 647-650.

Kponyo, J.J., Y. Kuang, E. Zhang, K. Domenic, 2013. VANET cluster-on-demand minimum spanning tree (MST) Prim clustering algorithm. In *Computational Problem-solving (ICCP), International Conference on* (pp: 101-104). IEEE.

Anitha, G., D.M. Hemalatha, 2014. Intrusion prevention and Message Authentication Protocol (IMAP) using Region Based Certificate Revocation List Method in Vehicular Ad hoc Networks. *International Journal of Engineering and Technology*, *6*.