International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 18, Issue 01) and (Publishing Month: December 2014)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Modified EMAP Protocol in VANET

Shashi Sangwan[1] and Deepti Ahlawat[2]

[1]NC College of Engineering, Israna, Haryana (India).
shashi.4308127@gmail.com

[2]NC College of Engineering, Israna, Haryana (India).
deeptijaglan@gmail.com

Abstract

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. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched. 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. This research will enhance the security in the VANET. In VANET the vehicles communicate with each other, the communication message may be warning message or other private messages. The security mechanism will be implemented by using the CRL method. In the existing work CRL checking process is speed up by replacing the CRL check by the revocation check. Still the message authentication process uses the ECDSA method to verify the signature of the message. This process can be speed up by using the RSA but the space taken by RSA is more as compared to ECDSA. This method uses the RSA in place of the ECDSA to accelerate the process. The space utilization is enhanced by performing the certificate verification and message verification in single step. This would also enhance the speed resulting reduced delay.

Keywords: *VANET, Security, CRL.*

I. Introduction

A Vehicular Ad-Hoc network is a form of Mobile ad-hoc Networks, to provide communication among nearby vehicles and between vehicles and nearby fixed equipment i.e. roadside equipment. The main goal of VANET is providing safety and comfort for passengers. Each vehicle equipped with VANET device will be a node in the Ad-hoc network and can receive & relay other messages through the wireless network Collision warning, Road signal arms and in place traffic view will give the driver essential tool to decide the best path along the way. VANET or Intelligent Vehicular Ad-Hoc Networking provides an intelligent way of using vehicular Networking [1]. Vehicles on the roads use wireless technology to communicate each other without any pre deployed infrastructure. The applications have been classified into two categories: Safety applications, which allow the passengers or drivers to share contents such as road obstacles, traffic flows and accidents that have occurred, Entertainment applications, which allow vehicles to share multimedia or local information such as MP3 music, videos, sale advertisement or virtual tours of hotel rooms. One of the main issues in VANETs is providing a reliable and efficient routing in urban scenarios with regard to the challenges (i.e., high vehicle mobility and presence of radio obstacle) [2], [3].

II. Security

A number of initiatives that seek to create safer and more efficient driving conditions have recently drawn strong support. The key enabling technology towards this goal is *Vehicular communications* (VC). *Vehicular ad hoc networks* (VANET) are envisioned to support a variety of applications for *safety, traffic efficiency and driver assistance*, and *infotainment*. For example, warnings on environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency braking), traffic and road conditions (e.g., congestion or construction sites), and tourist information downloads will be provided by such systems [4]. In VANETs, a vehicle's *On Board Unit (OBU)* communicates with other vehicles' OBUs and fixed infrastructure called *Road Side Units (RSUs)*. For VANETs to operate securely and reliably, participants needs to validate received

messages; otherwise, an attacker can easily inject bogus messages to disrupt the normal operation of VANETs. To allow authentication, we need to build key management mechanisms that allow senders to establish and update keys for security-sensitive operations. While RSUs can utilize traditional Public Key Infrastructure approaches, designing an OBU key management mechanism for secure VANET operation turns out to be a surprisingly intricate and challenging endeavor, because of multiple seemingly conflicting requirements. Recipients need to authenticate OBUs that they communicate with; and road authorities would like to trace drivers that abuse the system. However, VANETs need to protect a driver's privacy. In particular, drivers may not wish to be tracked wherever they travel [5]. Ideally, an OBU key management mechanism should provide the following desirable properties:

Authenticity, VANET participants need to authenticate legitimate OBUs and messages from those senders.

Privacy, RSUs and wireless eavesdroppers should not be able to track a driver in the long term. Authorities can already track vehicles through cameras and automatic license-plate readers. However, VANETs should not make such tracking any simpler by repeatedly broadcasting identifying information about the vehicle. The privacy requirement is seemingly contradictory to the authenticity requirement: if each OBU presents a certificate to vouch for its validity, then eavesdroppers can link any use of that certificate back to the OBU and thus the vehicle.

Short-term Linkability, For privacy, an eavesdropper should not be able to link messages from the same OBU in the long term. VANET applications require that in the short-term, a recipient be able to link two messages sent out by the same OBU.

Traceability and Revocation, An authority should be able to trace an OBU that abuses the VANET. In addition, once a misbehaving OBU has been traced, the authority should be able to revoke it in a timely manner. This prevents the misbehaving OBU from causing any further damage.

Efficiency, OBUs have resource-limited processors to make VANETs economically viable. Therefore, the cryptography used in VANETs should incur limited computational overhead.

Vehicular ad hoc networks (VANET) enable vehicles to communicate among themselves (V2V communications) and with road-side infrastructure (V2I communications). Such networks present various functionalities in terms of vehicular safety, traffic congestion reduction, and location based service (LBS) applications. Recognizing the potential of VANET, there have been concerted efforts to network vehicles. However, many challenges including the security and privacy issues remain to be addressed [4].

III. Related Work

P. Papadimitratos et al. (2006) has performed the emerging technology of vehicular communications (VC) raises a number of technical problems that need to be addressed. Among those, security and privacy concerns are paramount for the wide adoption of VC. They were concerned with privacy and identity management in the context of these systems. They identify VC-specific issues and challenges, considering the salient features of these systems. In particular, they view them in the context of other broader privacy protection efforts, as well as in the light of on-going work for VC standardization, and other mobile wireless communication [4]. *Yipin Sun et al. (2010)* proposed an efficient pseudonymous authentication scheme with strong privacy preservation, named PASS, for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of Certificate Revocation List (CRL) in PASS is linear with the number of revoked vehicles and irrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports Roadside Units aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost irrelated to the number of the updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries cannot trace any vehicle even all Roadside Units have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported ones in terms of the revocation cost and the certificate updating overhead [7]. Fatemeh Teymoori et al. (2013) said that one of the main issues in Vehicular Ad-hoc Networks (VANETs) is providing a reliable and efficient routing in urban scenarios with regard to the high vehicle mobility and presence of radio obstacle. They proposed a Position-Based routing protocol using Learning Automata (PBLA). In addition, PBLA uses the traffic information for enhancing learning. As

they know, main characteristic of learning is increasing performance over time. They exploit this characteristic to decreasing use of traffic information. Initially, PBLA make effort to finding best and shortest path to mobile destination using traffic information [2]. In (2013) *Albert Wasef et al.* proposed an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The 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. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient [8].

IV. CRL Distribution

The envisioned VC (VANET Communication) systems rely on multiple Certification Authorities (CAs), with each CA managing identities and credentials for nodes (vehicles and road-side units (RSUs)) registered within its region (e.g., national territory, district, county). Each node is uniquely identified and holds one or more private-public key pairs and certificates, digitally signing messages it transmits. Nodes holding keys and credentials, however, do not necessarily comply with the implemented protocols. They may be faulty or illegitimately obtain private keys. To ensure the robustness of the VC system, it is important to evict faulty nodes and prevent the utilization of compromised keys. The distribution of Certificate Revocation Lists (CRLs) is the basic approach: each CA adds to its CRL registered nodes' certificates that have not expired yet and it deems it must revoke, and it periodically publicizes the CRL. Providing CRLs across the wireline Internet is a long-known practice that can be helpful in the VC context. For example, in a pseudonymous authentication system, a CRL sent to a provider of short-term VC credentials will expel a node by preventing it from obtaining new credentials. Nonetheless, the distribution of CRLs across the wireless part of the VC system, so that correct nodes can ignore messages signed by revoked nodes, has not been investigated [6].

V. Proposed Work

The proposed EMAP uses a fast HMAC function and novel key sharing scheme employing probabilistic random key distribution. The existing work only speeds up the CRL checking process by replacing the CRL check by the revocation check. Still the message authentication process uses the ECDSA method to verify the signature of the message. This process can be speed up by using the RSA but the space taken by RSA is more as compared to ECDSA. This method uses the RSA in place of the ECDSA to accelerate the process. The space utilization is enhanced by performing the certificate verification and message verification in single step. This would also enhance the speed resulting reduced delay. The signature of the message and certificate will be same in our algorithm. Firstly the signature of the certificate and the message is compared, if both are same only then the RSA is used to verify the signature otherwise message will be discarded. This filtering step will also speed up the process. The algorithm is added to the existing process i.e. explained below:

Algorithm

1: Verify by checking
2: if invalid then
3: Discard the message
4: else
5: Run Algorithm 2
7: end if
8: Store *ver* and
9: Erase , the hash chain values, and the original compromised secret and public keys.

This work accelerates the message signature authentication process that results in reduced transmission delay. The message acceleration is achieved by removing the steps of The signature authentication process s accelerated by Due to the secure communication, the drop packet gets reduced which results in the reduced loss ratio. The communication cost can be calculated by the delay and the total packets. As the delay reduced so the communication cost also gets reduced.

VI. Implementation

The proposed technique is implemented in NS-2.35 Simulator in Linux environment. The tcl file is

executed and it generates a tr file that is evaluated using the awk scripts to get the results. The protocol is analyzed by using the following parameters:

Parameter Analyzed

Various parameters used for analysis are described below:

1. Packet Delivery Ratio

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination .

∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

2. End-to-end Delay

The average time taken by data packets to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

These results are also shown in the table 1, 2, 3. The table shows the better performance of the proposed protocol as compared to the existing protocol.

3. Loss Ratio

The ratio of the number of dropped data packet to the packets generated. ∑ Number of packet drop / ∑

Number of packet send The lower value of loss ratio means the better performance of the protocol.

The results obtained on the above motioned parameters are given below:

Table1: Comparison of P.D.R

Sl. No.	Density	Emap	Modified Emap
1.	40	82.4567	95.9823
2.	60	84.4962	96.3903
3.	80	83.8013	96.3642
4.	100	83.5965	96.4369
5.	120	82.7833	96.5643

The results can also be compared graphically. The figure 1(a) shows the graphical comparison of PDR by using Xgraph while the figure 1(b) shows the results using bar graph.

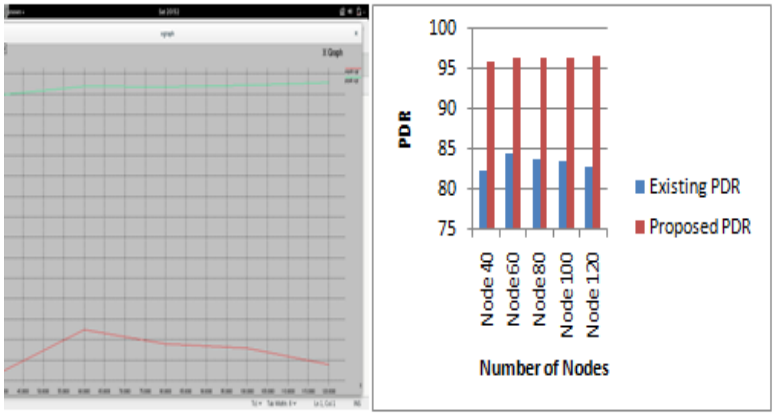

Figure1: Comparison of Packet Delivery Ratio between Existing (Emap) and Proposed (Modified Emap) (a) by Xgraph (b) Bar Graph

Table2: Comparison of Communication Cost

Sl. No.	Density	Emap	Modified emap
1.	40	1.21276	1.04186
2.	60	1.18349	1.03745
3.	80	1.1933	1.03773
4.	100	1.19622	1.03695
5.	120	1.20797	1.03558

The figure 2(a) shows the graphical comparison of Communication Cost by using Xgraph while the figure 2(b) shows the results using bar graph.

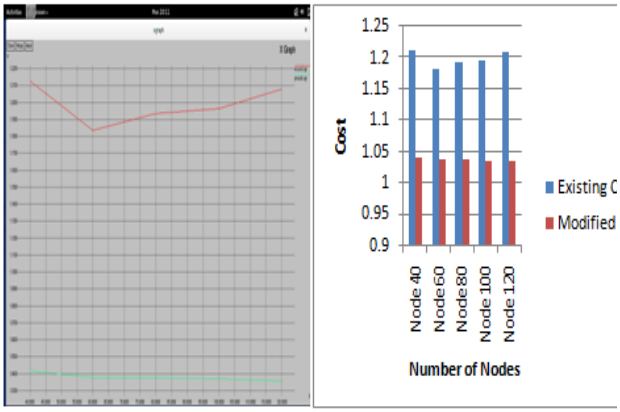

Figure 2: Comparison of Communication Cost between Existing (emap) and Proposed (Modified emap)(a) by Xgraph (b) Bar Graph

Table 3: Comparison of Loss Ratio

Sl. No.	Density	emap	Modified emap
1.	40	17.5433	4.01766
2.	60	15.5038	3.60968
3.	80	16.1987	3.63583
4.	100	16.4035	3.56308
5.	120	17.2167	3.43573

The figure 3(a) shows the graphical comparison of loss ratio by using Xgraph while the figure 3(b) shows the results using bar graph.

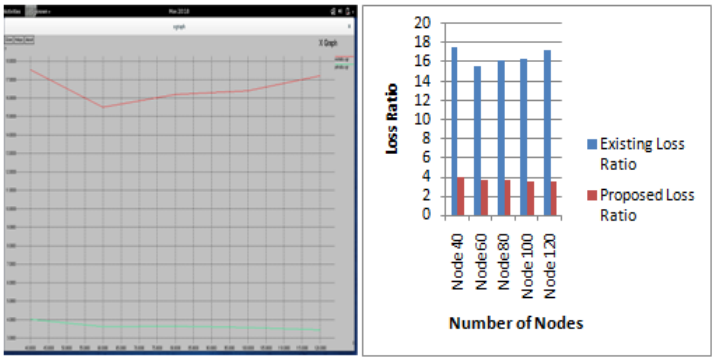

Figure 3: Comparison of Loss Ratio between Existing(emap) and Proposed(Modified emap) (a) by Xgraph (b) Bar Graph

Table4: Comparison of End-2-End Delay

Sl. No.	Density	Emap	Modified emap
1.	40	0.18948	0.0335858
2.	60	0.235113	0.0467378
3.	80	0.250396	0.0483141
4.	100	0.268551	0.0565086
5.	120	0.304071	0.0635369

The figure 4(a) shows the graphical comparison of E2E delay by using Xgraph while the figure 4(b) shows the results using bar graph

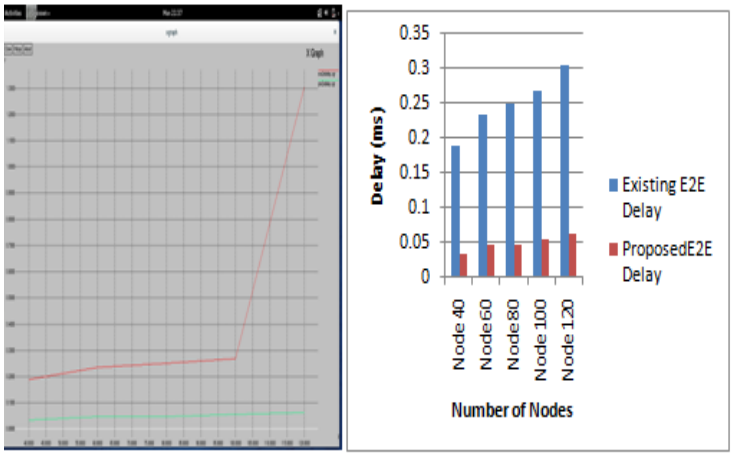

Figure 4: Comparison of E2E Delay between Existing (emap) and Proposed (Modified emap) (a) by Xgraph (b) Bar Graph

The graphical comparison confirms the better performance of the proposed protocol is better than the existing protocol.

VII. Conclusion

This work enhances the security in the VANET. In VANET the vehicles communicate with each other, the communication message may be warning message or other private messages. The security mechanism is implemented by using the CRL checking method. The existing work only speeds up the CRL checking process by replacing the CRL

check by the revocation check. Still the message authentication process uses the ECDSA method to verify the signature of the message. This process can be speed up by using the RSA but the space taken by RSA is more as compared to ECDSA. This method uses the RSA in place of the ECDSA to accelerate the process. The space utilization is enhanced by performing the certificate verification and message verification in single step. This would also enhance the speed resulting reduced delay. The signature of the message and certificate will be same in our algorithm. Firstly the signature of the certificate and the message is compared, if both are same only then the RSA is used to verify the signature otherwise message will be discarded. This filtering step will also speed up the process. The work is implemented using the NS2 and the PDR, loss ratio and the delay is analyzed the decrease in delay and loss ratio shows the better performance of the proposed work . In future following work can be done: The work can be extended to enhance the QOS., The work can be analyzed on various scenario to analyze the performance.

References

[1] Kohli, S., Kaur, B., & Bindra, S. (2010). A Comparative Study of Routing Protocols in VANET. Proceedings of ISCET.

[2] Teymoori, F., Nabizadeh, H., & Teymoori, F. (June, 2013). A New Approach In Position-Based Routing Protocol using Learning Automata for VANETs in City Scenario. ArXiv preprint arXiv:1308.0099, International Journal of Ambient Systems and Applications (IJASA), Volume1, Issue 2.

[3] Nikumbh, M. D., & Bhoi, M. A. (2013). A Survey of Positioned Based Routing Protocol in VANET, International Journal of Modern Engineering Research (IJMER), Volume 3, Issue2, pp.1015-1018.

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

[5] A. Studer, E. Shi, F. Bai, and A. Perrig, (2009) Tacking Together Efficient Authentication, Revocation, and Privacy in VANETs, Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9.

[6] P.P. Papadimitratos, G. Mezzour, and J. Hubaux, (2008), Certificate Revocation List Distribution in Vehicular Communication Systems, Proc. Fifth ACM Int'l Workshop Vehicular Inter-Networking, pp. 86-87.

[7] Sun Yipin, Lu Rongxing, Lin Xiaodong, (Sherman) Shen Xuemin, Su Jinshu,(2010), An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications, IEEE Transactions On Vehicular Technology, Vol. X, No. X, Xx.

[8] Wasef Albert and (Sherman) Shen Xuemin,(January 2013), EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transactions On Mobile Computing, Volume: 12, Issue: 1.