International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-8 March-2013

New Lightweight Security Protocol for VANET by Using Registration Identity and Group Certificate

Aditi Garg[1], Ankita Agrawal[2], Niharika Chaudhary[3], Shivanshu Gupta[4], Devesh Pandey[5], Tumpa Roy[6]
G.L.N.A Institute of Technology, Computer Science & Engineering, Mathura, U.P-283416, India.

Abstract

Vehicular ad hoc networks (VANETs) are receiving increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users. Wellbeing information switch over enables life-critical applications, such as the alerting functionality during connection traversing and lane integration, and thus, it plays a key role in VANET. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. The communication between car to car, car to roadside unit done through wireless communication. That is why security is an important concern area for vehicular network application. In VANET some serious network attacks such as man in middle attack, masquerading is possible. In this paper we are going to propose an algorithm in order to overcome these network attacks. Finally we have analyzed and compared our algorithm with existing algorithm [1].

Keywords

Security, Road side unit (RSU), Base station unit (BSU), Network Attacks, Bandwidth, Registration Identity, Certificate.

I. Introduction

VANET- Vehicular Ad-Hoc Network is the network in which communication has been done in between road side units to cars, car to car in a short range of 100 to 300 m. Existing authentication protocols to secure vehicular ad hoc networks (VANETs) raise challenges such as certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper-proof devices. In a VANET, the communication device, vehicles will rely on the reliability of received data for deciding when to present alerts to drivers. The received data may contain the information related the traffic and any type of accident or incident. Further in the future, the received data may be used as the basis of control decisions for independent vehicles. If this information is dishonored, vehicles may present redundant or incorrect warnings to their drivers, and the results of control decisions based on this information could be even more catastrophic. Information can be corrupted by two different mechanisms: malice and malfunction. Similarly, vehicles have two defense mechanisms: an internal filter and external reputation information.

The former defense mechanism can consist of filters based on physical laws (e.g., maximum braking deceleration, maximum speed, physical space constraints) [2]. The latter defense mechanism can consist of reports from other vehicles or entities on the validity or trustworthiness of data originating from certain [1].

In this paper, we will concern ourselves with the latter defense mechanism. Information received from corrupted nodes should be disregarded or not trusted by legitimate vehicles, otherwise, a malicious vehicle could, for example, obtain a less congested route for itself by overstating the number of vehicles on its desired roadway. As a Second example, a corrupted node could trigger erroneous driver warnings to be displayed in other vehicles by falsifying its position information. IEEE 1609.2, the trial-use standard concerning security services for vehicular environments, stipulates that vehicles will be authenticated using certificates issued by a Certificate Authority (CA) in a Public Key Infrastructure (PKI) setup [3]. Illegitimate vehicles should have these certificates revoked, and the identity of the revoked certificates (although ideally not the identity of the associated driver) should be published and distributed to legitimate vehicles. Whatever mechanism that is used for distributing this revocation information should distribute the info information securely, quickly, and broadly in order to limit the amount of damage illegitimate vehicles can do.
First we discuss the general architecture and security architecture of VANET. Next our paper addresses the

analytical evaluation of different research paper in VANET. Than we compare different popular.

II. General Architecture

The communication may be of 3 types-

1. Inter-vehicle communication i.e. vehicle to vehicle communication.
2. Vehicle to roadside communication i.e. communication between roadside unit (RSU) and vehicles.
3. Inter-roadside communication i.e. communication between roadside unit and the base station. Applications based on vehicular communication range from simple exchange of vehicle status data to highly complex, large-scale traffic management including infrastructure integration.

As a start to analyze applications, this section gives an overview on envisioned application categories for vehicular networks. Although exact operation details are not yet standardized for most applications and in spite that such a collection can never be completely finished, the overview delivers basic mechanisms, components and constraints involved in the system [4].

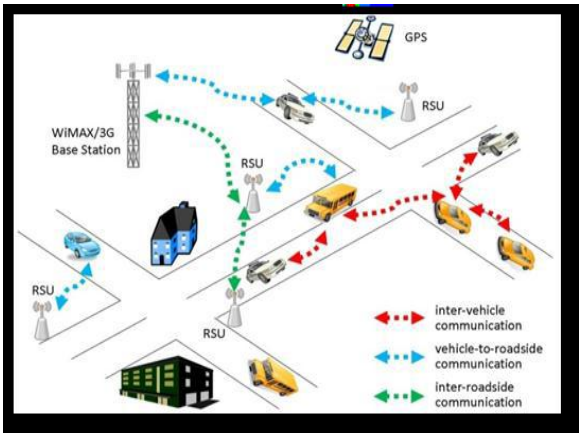

Fig.1: General Architecture
(http://naa.chosun.ac.kr/)

III. Security Architecture

All generally includes use of public key signatures. In a public key infrastructure, certificate authorities (CAs) bind between public keys and the nodes. Security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks.

1. If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behavior of other vehicles.

By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.

2. If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.

3. A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if non-repudiation is not supported, it could not be sanctioned even if discovered.

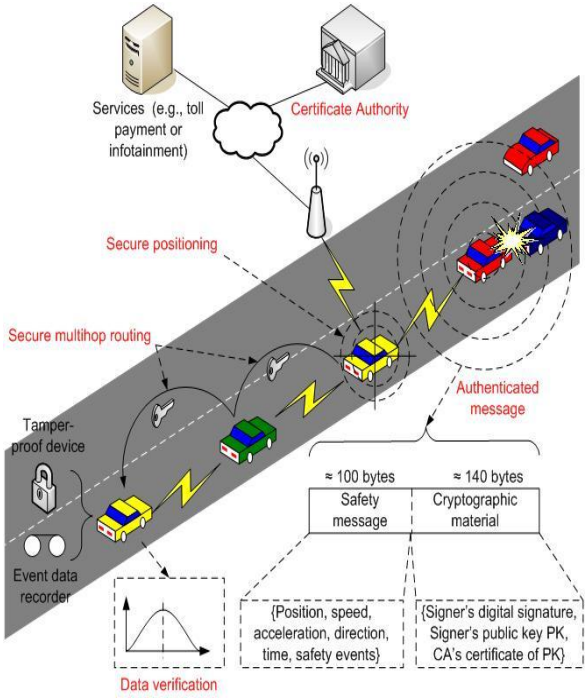

Fig. 2: General Security Architecture [4]

IV. Related Work

Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu[4] proposed an idea for improving distribution speed and distribution of CRLs by using vehicles in an epidemic fashion. In this paper [4] nodes are not confirmed about the bandwidth and hardware restrictions and the method that only employs at RSU distribution points.
M. Raya, P. Papadimitratos, I. Aad, D.jungels, and J.P.Habaux[5] gave a proposal of developing infrastructure based revocation protocol. They also gave an idea of MDS, enabling the neighbors of misbehaving or faulty nodes to detect its deviation from normal behavior. For the purpose of security they provide a LEAVE protocol to safeguard the system operation, but false rate has been provided by Bloom's Filter.

Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi[6] proposed the parameter ANGLE for RSUs, to detect Sybil nodes. They assume that the angle value remains unique for each node at any instant of time and they found that 99% is accurate with approximate. As there is no well defined processing time, storage and number of RSU, hence it results to 0.5% error rate.

D. Cooper[7], give an idea to propose a mechanism for passing CRL updates, rather than the entire CRL, which reduces the imposed network overhead. In this paper[7] high bandwidth and time is been consumed as instead of updating CRL, it exchanges whole CRL.
Lei Zhang, Qianhong Wu, Agusti Solanas[8], provide a protocol which exploits the specific feature of vehicular mobility, physical road limitations, and properly distributed RSUs. As traffic load increases performance rate decreases and if any of vehicle collapse than whole network will get fail.

M. Raya, Panos Papadimitratos, and Jean-pierre Habaux[9],discusses about the vehicular communication that exhibits unique security challenges, induced by the high speed and sporadic connectivity of the vehicles. According to this paper [9], vehicle communication exhibits short lived CRL and secure positioning is a open source which is main concern.

M. Raya, and J.P Habaux[10], proposed a model that identifies the most relevant communication aspects. They also proposed security architecture along with the related protocols. .Digital Signatures showed to be the most suitable approach despite their seemingly high overhead. But these network solutions cannot be implemented in the present scenario.

Philippe Golle, Dan Greene, Jessica Staddon[2], gives an idea of Sensor driver technique that allows nodes to detect incorrect information and identify the node or nodes that are the source of this incorrect information with high probability.

V. Security Protocol Analysis

This paper[1] presents the proposed optimizations for organizing, storing, and exchanging CRL information in order to reduce the potential network and computational overhead imposed by any CRL distribution mechanism. This mechanism holds a single CA to revoke a vehicle's certificate in an efficient manner that minimizes the size of the CRL or CRL updates. It also presents a lightweight mechanism for exchanging CRL updates. Additionally, presents a formal proof of the security of proposed mechanism for reducing the size of CRL's by giving two algorithms.

Presents a certificate organization method by giving an example of a generalized Public key certificate exchange, which explains that when vehicle A hears a message from a previously unknown vehicle X, it replies with a query for the certificate and short-term public key of X.

Algorithm 1 certificate generation algorithm

Begins with the certificate loading of vehicle V then first, the CA chooses a secret revocation key s(key to block cipher) for each vehicle. Next, the CA creates a corresponding group of M (number of certificates for vehicle V) certificates. Then for each r it creates a certificate. The CA then issues these M key-pairs and associated certificates to vehicle V.

Algorithm 2 certificate exchange and update algorithm

It shows how updates are generated and distributed among vehicles. In this it is assumed that there is a single CRL. Since each CRL update will be rebroadcast many times so the CRL size should be small. It propose that only the entries necessary to bring the receiver's CRL up to the latest version be transmitted by the sender to the receiver. Also include a CA signature over the entire CRL, verified by the receiver.

Also presents the analysis of performance for practical Bloom filter implementation using revoked certificate storage. Its consequences of using Bloom filter(probabilistic data structure), that is, when searching a Bloom filter , false positives occur with some probability. And also the comparison of bloom filter with deterministic data structure is done.

VI. Proposed work

Global assumptions: Under a single base station there are maximum 100 road side units. The range of each road side units is about 300m. Each road side unit can have maximum cars considering the situation of high traffic area.

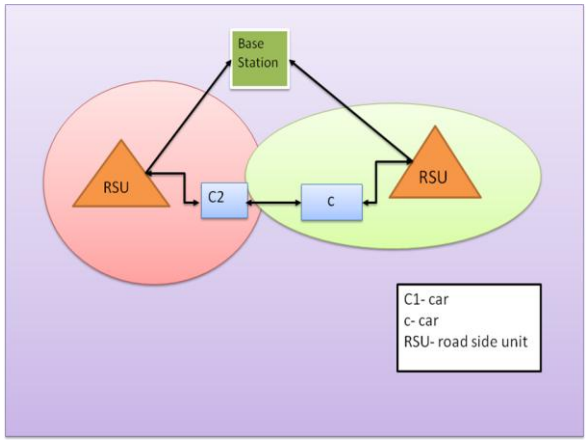

Fig 3:Global Scenerio Of VANET

Initial Phase: Base station to Road side units

1. Firstly Base Station send a message to road side unit in which a group identity (Idg_1) and a variable R is sent to the road side unit.
2. The Road Side Unit responses whether it is active or not.
3. The Base Station upon receiving the response sends the certificate. The certificate contains three variables- public key of road side unit (PU_{RSUg}), validity (valid), group identity (Idg_1). The channel is encrypted by R and upon receiving the certificate it is then decrypted by using the variable R. Thus R is responsible for the authentication purpose.

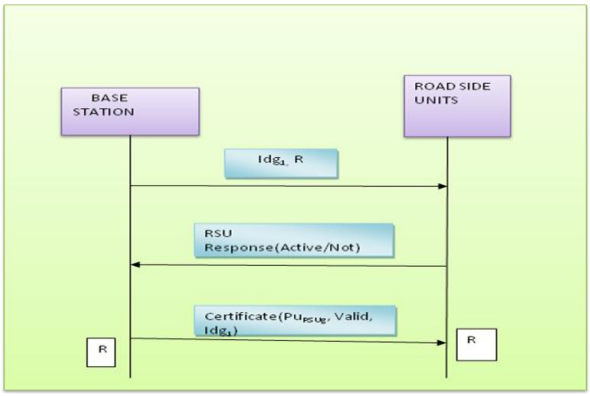

Fig 4: Message Diagram for Initial Phase

Second Phase

Road Side Unit to car

Assumption: A car already has a registration identity. Regid includes license number, car registration number.

1. Firstly car sends a message to road side unit in which registration identity (Regid), public key of car (PU_{car}).
2. RSU will respond to car in a message which includes certificate of RSU ($CERT_{RSU}$) and registration identity (Regid).
3. Car will store the $CERT_{RSU}$ and sends a message which includes $CERT_{RSU}$ and Regid . Registration id is used for checking the authentication of car and RSU.
4. RSU then divides the message into two parts. In which first part includes $CERT_{RSU}$ and second part contains Regid. Thus mutual authentication is done and communication is preceded.

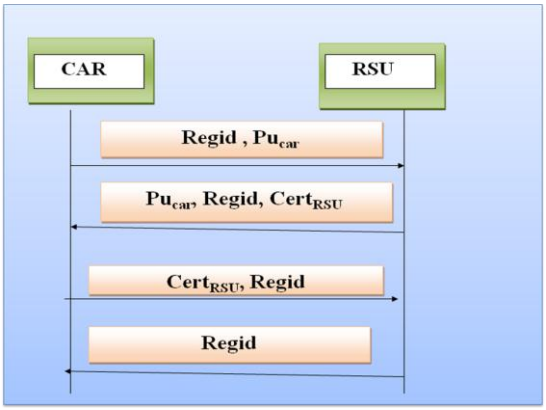

Fig 5: Message Diagram for Second Phase

Third Phase: Car to Car Communication
The car will send the certificates to each other. If the certificate is same and authenticated the communication will proceed on.

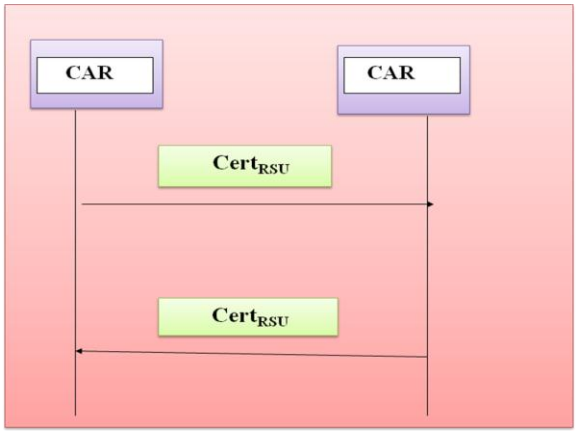

Fig 6: Message Diagram for Third Phase

VII. Comparison

1. Denial Of Service Attack : A "denial-of-service" attack is an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. Defending against Denial of Service attacks typically involves the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate.

In our proposed work DoS is checked as mutual authentication is done at each phase. Mutual authentication or two-way authentication refers to two parties authenticating each other suitably.

2. Masquerading: It allows one machine to act on behalf of other machines. That is one machine can pretend to be another and can misuse the information obtained via conversation.

The problem of masquerading is also eliminated in our proposed algorithm by mutual authentication. Since at each level the sender and receiver will authenticate each other there will be no masquerading attacks.

3.Bandwidth: In previous paper[1] since CA broadcasts the certificate to the entire channel which consumes sufficiently high bandwidth whereas in our proposed algorithm certificate is only granted whenever it is requested by the vehicle through message passing that results in lower consumption of bandwidth.

4. Computational cost: This paper[1] presents that CRL update is rebroadcasted many times and that to periodically. This uses cryptographic hash functions for encryption of certificates that would results in excessive computational cost and storage overhead whereas in our paper only nine messages have been exchanged, resulting in low computational cost.

VIII. Conclusion

In this paper we had discussed about VANET and its architecture. We studied the previous work that has been done related to VANET. We have proposed an algorithm which is secured, cost effective and give better performance. We analyze the research work done and made a comparison between our work and their work. We laid out comparison on the basis of security, performance and cost. In future we would like to simulate our research work using Matlab.

References

[1] Jason J. Haas, Yih-Chun Hu, Kenneth P. Laberteaux ―Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET in VANET'09, September 25, 2009, Beijing, China. 2009 ACM .
[2] P. Golle, D. Greene, and J. Staddon, ―Detecting and correcting malicious data in vanets, in VANET '04: Proceedings of the 1st ACM international workshop on Vehicular Ad hoc networks, (New York, NY, USA), pp. 29–37, ACM, 2004.
[3] IEEE, IEEE 1609.2-Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, available from ITS Standards Program.
[4] Kenneth P. Laberteaux, J.J. Haas, and Y.C.Hu, ―Security Certificate revocation list distribution for VANET. In VANET '08 Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking .
[5] M. Raya, P. Papadimitratos, I. Aad, D.jungels, and J.P. Habaux), ―Eviction of misbehaving and faulty nodes in vehicular networks, in IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, vol. 25, num. 8, p. 1557-1568.
[6] Jyoti Grover, Manoj Singh Gaur, Vijay Laxmi, A Novel Defense Mechanism against Sybil Attacks

in VANET, in Proceeding SIN '10 Proceedings of the 3rd international conference on Security of information and networks .

[7] D. Cooper, ―A More Efficient Use of Delta-CRLs, in IEEE Symposium on Security and Privacy.

[8] Lei Zhang, Qianhong Wu, Agusti Solanas ― A Scalable Robust Authentication Protocol for Secure Vehicular Communications.

[9] M. Raya, Papadimitratos and J.P Habaux Special issues on Inter-Vehicular Communication.

[10] [M. Raya, and J.P Habaux ,Securing Vehicular ad hoc networks.

Aditi Garg She is the perusing her graduation in B.Tech, Computer Science & Engineering from GLNA Institute of Technology, Mathura, UP. Recently, she has published a review paper on "Security on Ad-Hoc Network (VANET): A REVIEW", International Journal of Emerging Technology and Advanced Engineering. After completion of her graduation she would like to do her post graduation as MS,CSE from a repudiated university.

Ankita Agrawal She is the student of B.Tech, Computer Science & Engineering from GLNA Institute of Technology, Mathura, UP. She has published review paper on "Security on A REVIEW", International Journal of Emerging Technology and Advanced Engineering. Her area of interest is Networks, and want to pursue M.Tech , Networks.

Niharika Chaudhary Presently, she is the perusing her graduation in B.Tech, Computer Science & Engineering from GLNA Institute of Technology, Mathura, UP. Recently, she has published a review paper on "Security on Ad-Hoc Network (VANET): A REVIEW", International Journal of Emerging Technology and Advanced Engineering. After completion of her graduation she would like to do her post graduation in M.Tech, CSE, and if possible she would like to work with R & D center.

Shivanshu Gupta He is presently a student of B.Tech, Computer Science & Engineering from GLNA Institute of Technology, Mathura, UP. Recently, he has published a review paper on "Security On Ad-Hoc Network (VANET): A REVIEW", International Journal Of Emerging Technology and Advanced Engineering. He is interested in studying Networking and wants to pursue his Post graduation in Networking.

Devesh Pandey He is the student of B.Tech, Computer Science & Engineering from GLNA Institute of Technology, Mathura, UP. His area of interest is computer networks. He has published a review paper on "Security On Ad-Hoc Network (VANET):A REVIEW", International Journal Of emerging Technology and Advanced Engineering.