Security In Vehicular Ad-Hoc Network

Prakash Tripathi, Dr. Kanojia Sindhuben Babulal.

Abstract: Vehicle connectivity can be considered as an emerging technology that provides dissemination of warning messages and traffic information to vehicles running on the road. The deployment of vehicular ad-hoc network communication is strictly dependent on strictly on their security and privacy features. Recent advances in the hardware and software technology, tremendous improvements are made. Emerging Vehicular Ad-hoc Networks have the potential to improve the safety, traffic efficiency and as well as comfort to both drivers and passengers of highways. In the last three decades, various kinds of improvements are made in Wireless Ad-hoc Network and now a day's one of the most attractive research topic is Vehicular Ad-hoc Network (VANET) and become the most relevant form of Mobile Ad-hoc Networks. In this paper we address the Security in Vehicular ad-hoc Network. We provide a detail threat analysis as well as devise the solution of these threats. We provide a set of security protocols to protect the privacy and analyze the robustness and efficiency. In this paper we propose security architecture for vehicle communication. The architecture contains symmetric and asymmetric cryptography mechanism in the vehicular distributed environment for dissemination of information securely and efficiently.

Index Terms: IEEE 802.11, IEEE 802.15, Intelligent Transportation System (ITS), VANET Protocols, Threats.

1 INTRODUCTION

Vehicular ad-hoc networks (VANETs) are wireless communication networks that do not require any kind of fixed infrastructure. It is based on IEEE 802.11p standard for Wireless Access for Vehicular Environment (WAVE). Vehicular Networks (VNs) consist of vehicles and Road Side Units (RSUs) equipped with on-board processing and wireless communication modules. Europe and US are using the Vehicular Network for safe driving and traffic management. In October 1999, the US Federal Communications Commission (FCC) allocated 75 MHz (the 5.85 –to 5.925-GHz portion) of the spectrum in America for Dedicated Short Range. Communications (DSRC) for Vehicle-to-Vehicle or Vehicle-to-Roadside communication [1, 2]. Upcoming Traffic safety initiatives rely heavily on information technology, which means that vehicles must be able to authenticate themselves and be traceable whenever necessary for law enforcement (detection of speed vehicles), crash reconstruction or toll collection.[3], [4] .

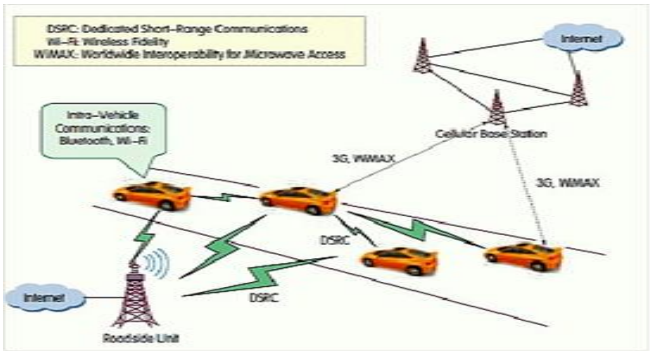

Fig 1.*Vehicular Ad-hoc Networks*

Vehicular Ad-hoc Networks (VANETs) provide variety of applications such as co-operative collision warning, lane change warning, intersection warning, work zone warning, inter-vehicle communication etc. but all them require more security and privacy since all these sort of applications are vulnerable to various attacks. Therefore Vehicular Networks must implemented on a secure environment as much as possible In this paper, we proposed the Digital Envelope approach that will support to reduce the threats and provide a sufficient level of security and privacy.

2 Related Work

Most of the researchers are still developing the security and authentication, privacy mechanism using various techniques like digital signature, public key infrastructure, pseudonym [6], Currently, every vehicle is registered with its national or regional authority, which allocates a unique identifier to it, but in parts of the US and the EU, registration authorities have made substantial progress toward electronically identifying vehicles and similar progress is being made toward machine-readable driving licenses. To allow the wireless authentication of vehicles, these authorities must provide each vehicle with a private/public key pair, along with a shared symmetric key, and a digital certificate of its identity and public key. it will use to sign broadcasted safety messages. This ensures that other vehicles will be able to authenticate a received message if it includes a digital signature and the corresponding certificate issued by a CA (Certification Authority) [3] [5]. Such authorities will most likely be cross certified, making it possible for any vehicle to check any other vehicle's certificates [3]. Many vehicles are already equipped with hardware and firmware components, such as speed limiters, tachographs, and *event data recorders* (*EDRs*), which are considered critical by manufacturers and legislators. We assume that nodes are equipped with a Trusted Component (*TC*), i.e., tamper resistant hardware and firmware. The role of the TC is twofold:

- **I.** It stores all cryptographic material and prevents its exposure to the on-board computer;
- **II.** It performs all cryptographic operations [3,7].

Group formation group agreement technique in VANET is used in many papers which combines the concept of distributed computing.

3 Group Formation

Vehicles are arranged in the form of a group and one of them a vehicle is chosen as a co-coordinator act as a group leader and group membership managed dynamically. Within each group, one or more vehicles, automatically determined by their positions, transmit the data aggregated in that group to neighboring groups. Location based group is used to solve the problem of overlapping groups. The map (more precisely, the roads) is dissected into small area cells that actually define the groups. A vehicle will automatically know to which group it belongs by comparing its GPS position to a preloaded dissection of the area map into cells. The group leader, the vehicle closest to the center of the cell, is determined

dynamically. Cells, and hence groups, overlap in such a way that any vehicle moving from one cell to the next remains in transmission range of both group leaders. This means that the cell size depends on the transmission range of vehicles. Using the typical DSRC (Dedicated Short Range Communications) [2] range of 300 m, we have set the cell length in our simulations to 400 m, which proved to be a suitable value [5].

3.1 Benefits of Location-Based Groups

- **a)** Efficiency- A vehicle will automatically know to which group it belongs. Hence, group formation will not require any additional communication overhead or delay.
- **b)** Routing- As most routing in safety applications are geographic, determining which groups should relay messages are straightforward [5].

3.2 Combined Signatures

Each vehicle broadcasts a signed safety message. This creates considerable security overhead, especially in terms of message size and signature generation delay. There may be an additional delay resulting from data verification algorithms running on the receiving vehicles. We have sought to combine the signatures generated by a group of vehicles reporting the same event. Thus, all the overhead will be grouped in one message instead of being spread over several, resulting in a more efficient channel usage. In addition, once a vehicle receives such a combined message, it can skip the data verification process because the combined signatures imply that all the involved signers agree on the content of the message. There are several types of signature combinations, each with its own benefits and drawbacks, especially in terms of overhead. The formats of the three types of combined signatures are shown in Figure 1. It should be noted that this aggregation technique makes use of only asymmetric cryptography, hence the need for including the public key certificates of all signers in the corresponding message [5].

(a) Concatenated Signatures

A vehicle that receives a message with correct information (from the receiver's perspective) appends its signature to the existing signatures and rebroadcasts the new message. As signatures are appended to the message independently of each other, they will also be verified independently. Hence, there is no need for signers to verify the other signatures. Thus, concatenating signatures generates the same security overhead in terms of signature size and generation as the basic scheme. But it has some network overhead. It also overcomes the basic scheme in terms of data verification delay because a destination vehicle receives data explicitly approved by several signers [5].

(b)Onion Signatures

In this signature Instead of simply appending its signature, a vehicle signs the signature of the previous transmitter. Before retransmitting the new message, it should also include the last signature, i.e., the one it received, so that the vehicle at the next hop can verify the new signature. With this approach, no matter how many times a message is over signed, the ultimate result will always be the safety message with two signatures (the new and the previous ones). Since this technique is similar to the message re encryption process in onion routing [8], it is called *onion signature*. To reduce the processing costs of signature verification at the receiver, each signer has to verify the last signature before over signing. If the signature is invalid, it has to discard the existing signature and restart the onion signature generation. Obviously, verifying signatures at each hop increases the overall computation overhead, in addition to delaying the delivery of the combined signature to the destination. Moreover, a false message with a valid signature cannot be detected directly. But this attack can be thwarted by the possibility of punishment as the non-repudiation property of digital signatures allows the CA to determine the attacker [5].

(c) *Hybrid Signatures*

Although concatenated signatures, in terms of computation overhead, are more efficient than onion signatures, the opposite is true with respect to communication overhead. a hybrid solution that combines features of both approaches is possible. A *hybrid signature* would consist of several concatenated onion signatures, each of a given depth. The signature depth represents the number of layers it includes [5].

Concatenated Signatures

M	S1(m)	…	Sn(m)	c1	…	cn

Onion Signatures

m	Sn-1	Sn (...(S1(m)))	c1	…	cn

Hybrid Signatures

M	Si-1	Si..(S1(m)))	Sn-1	Sn..(Sj(m)))	c1	.	c1

Fig 2. *Types of combined signatures n is total number of signers.*

4 Overlapping Groups

Overlapping groups are based on Symmetric key cryptography in which each group having its own symmetric key. Vehicles in the intersection of two groups know the keys of both groups and hence are able to assure the bridge for data flow between the two groups. The main advantage of data flow between overlapping groups is the reduced communication and computation overhead due to symmetric cryptography. The drawbacks are the need for secure position verification, the overhead of group aspects, and the loss of the non-repudiation property. This loss of non-repudiation drawback is resolved by dynamic group key creation [5].

5 Digital Envelope Creation

The key idea of digital envelope creation is both symmetric and asymmetric world of cryptography. Firstly the group leader and group members are identified in overlapping groups. Once this task is achieved, the group leader and their members that want to transmit the message to another group must create a key request message to CA (Certificate Authority) to obtain the asymmetric key (public key) pair of group. The CA will use the information transmitted by group G1. This dynamic key request message format will be as follow [5]:

Key Request	P1	.	Pn	S1 (m)	.	Sn (m)	c1	.	cn	{K}PuK (BS)

Fig 3. *The format and content of dynamic key request message*

Pi – Position
Si – Signature of vehicle i.
ci – Certificate of vehicle i.

{K}PuK(BS) – symmetric group key encrypted with the public key of base station BS that receives the request. The symmetric group key is included in key request message and this symmetric group key is generated by SVGP (Secure VANET group protocol) that is inspired by the GKMP (Group Key Management Protocol) [9]. Now the message is encrypted with a symmetric key and the symmetric key is encrypted with public key of recipients group, the sender group puts both encrypted message and encrypted symmetric key inside a digital envelope and transmit it. Receiver group will obtain the encrypted message as well as one time encrypted symmetric key. Receiver's group use its private key to decrypt symmetric key that was encrypted using Receiver's group public key and apply the same symmetric key to the encrypted message to obtain the original message.

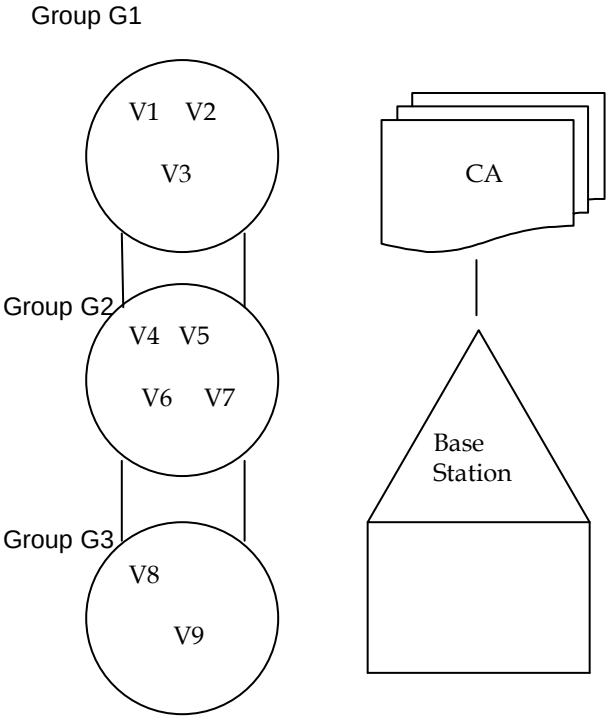

Fig 4. *Communication establishment between Groups, Base Station and Certification Authority (CA).*

In above figure-3, V1, V2, V3, V4, V5, V6, V7, V8, V9 are vehicles of respective Group. Thus key exchange as well as authentication is achieved by using the symmetric and asymmetric cryptography. The digital envelope technique is feasible since it achieves fast encryption because of encryption of message with symmetric key. The message also includes the unique ID assigned by CA to the sender group member. This mechanism will use the ECC (Elliptic Curve Cryptography) algorithm [10] because it imposes a significant load in storing and processing keys and message.

6 Conclusion

In this paper we have addressed the security, privacy and authentication in Vehicular Network and also analyze the previous security, privacy and authentication mechanism work. Our future work will be to improve the delay and reduce network overhead since high mobility and synchronization is the key factor of Vehicular Networks (VNs).

Acknowledgment

I would like to thanks my guide Dr. Sindhuben Kanojia who guided me at each step and give her precious time to the completion of this research paper and familiar me with key aspects and challenges of research area.

References

[1] Car2Car Consortium. http://www.car-to-car.org/

[2] 5.9GHz DSRC. http://grouper.ieee.org/groups/scc32/dsrc/index.html

[3] The Security and Privacy of Smart Vehicles- JEAN-PIERRE HUBAUX,SRDJAN CAPKUN, AND JUN LUO EPFL

[4] Vehicular ad hoc networks (VANETS): status, results, and challenges - Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen · Angela Irwin · Aamir Hassan

[5] Efficient Secure Aggregation in VANETs Maxim Raya, Adel Aziz and Jean-Pierre Hubaux Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences EPFL, Switzerland {maxim.raya, adel.aziz@epfl.ch, jean-pierre.hubaux}@epfl.ch

[6] Architecture for Secure and Private Vehicular Communications P. Papadimitratos EPFL Lausanne, Switzerland L. Buttyan BUTE Budapest, Hungary J-P. Hubaux EPFL Lausanne, Switzerland F. Kargl Ulm Univesrity Ulm, Germany A. Kung TRIALOG Paris, France M. Raya EPFL Lausanne, Switzerland

[7] Eviction of Misbehaving and Faulty Nodes in Vehicular Networks M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux

[8] D. Goldschlag, M. Reed, and P. Syverson. Onion routing. *Communications of the ACM*, 42(2):39–41,1999.

[9] H. Harney and C. Muckenhirn. Group Key Management Protocol (GKMP) architecture. RFC 2094, 1997.

[10] Cryptography and Network Security –William Stallings.