ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015

Security in Vehicular Ad-hoc Network Using Digital Envelop in Distributed Environment

Prakash Tripathi[1], Dr.Kanojia Sindhuben Babulal[2]

MTech, Department of Computer Science and Engineering, United Institute of Technology, Allahabad, India[1]

Assistant Professor, Dept., of Computer Science and Engineering, United Institute of Technology, Allahabad, India[2]

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.

This paper contains Digital Envelop mechanism in a Distributed Environment for dissemination of message as well as Key Management that provide the privacy and security.

Keywords: ECDSA, ECIES, G-Private Key, I-Public Key, TESLA

I. 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]

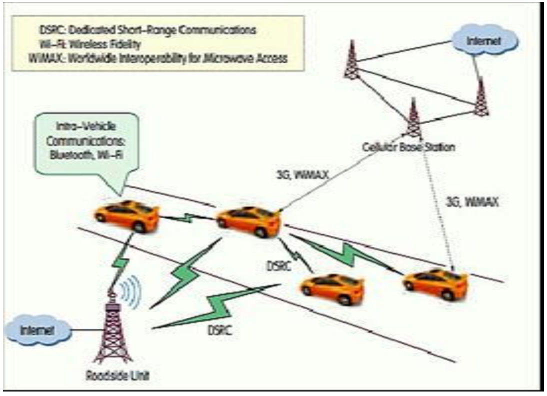
DSRC: Dedicated Short-Range Communications
Wi-Fi: Wireless Fidelity
WiMAX: Worldwide Interoperability for Microwave Access
Internet
Intra-Vehicle Communications: Bluetooth, Wi-Fi
Cellular Base Station
3G, WiMAX
3G, WiMAX
DSRC
DSRC
Internet
Roadside Unit

Fig-1 Vehicular Ad-hoc Network

II. RELATED WORK

VANETs Security and privacy related protocols are developed previously, that can be classified as follows: Public-key-cryptography (PKC)-based or secret-key cryptography (SKC)-based solutions. Protocols using a PKC approach can be further classified into two subcategories: traditional PKI-based digital signature techniques [4], [5] and group-signature techniques [6]. In our security model we propose a model that uses the PKI-based digital envelop authentication techniques in a distributed co-operative environment that uses both symmetric as well as asymmetric cryptography.

In traditional PKI-based digital signature techniques the anonymous public-key certificate of Raya and Hubaux[4] is the first noteworthy attempt to ensure security and privacy in vehicular communications, while also preserving the ability to trace messages back to their senders. Raya and Hubaux [4] proposed a protocol for secure vehicular communication. Each vehicle is preloaded with a large number of private keys, as well as their corresponding anonymous certificates (perhaps approximately 43800). The sending vehicle then randomly selects one of the anonymous certificates, using its corresponding private key to digitally sign messages to be sent. To verify the integrity of the message received, other vehicles use the sender's public key associated with this signature. Each anonymous certificate has only a short lifespan to meet the driver's privacy requirements. Unlike traditional public-key certificates, anonymous certificates are generated using the pseudo-identities of the vehicles, instead of identifying information from the driver. Each driver's entire list of anonymous certificates, which is mapped to the driver's real identity, is kept by the

DOI 10.17148/IJARCCE.2015.4313

authority, allowing messages to be traced back to the driver in the event of a dispute.

In group-signature techniques Lin et al. [6] discovered the fact that the unique characteristics of group signature, which is an important cryptographic primitive, perfectly match the security and privacy requirements in VANETs. By taking different security and privacy requirements of two types of VANET communications namely, vehicle-to-infrastructure and vehicle-to-vehicle communications, they propose a novel secure and privacy-preserving protocol for vehicular communication, based on a combination of group signature and identity (ID)-based signature techniques.

Lin et al. [7] developed a time-efficient and secure vehicular communications (TSVC) scheme, based on Timed Efficient Stream Loss-tolerant Authentication (TESLA) [8]. In TSVC, a number of hash chains are generated in advance for a given vehicle. The vehicle selects one chain at random and broadcasts the commitment of the chain to its neighbors, which is simply protected by a traditional PKI-based digital signature. Then, the vehicle uses the elements of the chain to generate message authentication codes (MACs) for messages originating from it. Its neighbors are able to authenticate the messages based on these MACs; however, the high dynamics of topological structure for vehicular network could jeopardize TSVC's effectiveness of message authentication.

There have been several proposals for privacy preservation of VANETs. Using pseudonyms is a natural idea. It is preferable to preserve the location privacy of a vehicle by breaking the linkability between two locations, for which the vehicle can update its pseudonym after each transmission. While the pure pseudonym schemes do not support the secure functionality of authentication, integrity, and non-repudiation.

A. Communication Protocols for VANETs

A vehicular ad-hoc network uses various kinds of communication protocols such as Cellular networks, IEEE 802.16 (WiMAX), or IEEE 802.11. cellular or WiMAX based networking is limited to single-hop base station to vehicle communications, and can hardly be applied to ad hoc vehicle to vehicle communications. Moreover, cellular and WiMAX networking heavily depend on the availability of infrastructure, which is normally expensive and might not be available in those underdeveloped areas. The cellular network is further limited with bandwidth and not suitable for large scale multihop vehicle to vehicle networking. The 802.11 based protocol has the flexibility in seamlessly supporting both single-hop RSU to vehicle communications and multi-hop vehicle to vehicle communications. System model in vehicular ad-hoc network classified as follows:

i. Certification Authorities

Authorities are responsible for key generation and malicious vehicle judgement. Authorities have powerful firewalls and other security protections. Therefore, they have the highest security level. We assume that they cannot be compromised.

ii. Road side infrastructure

Roadside Infrastructure consists of RSUs deployed at the road sides which are in charge of key management in our framework. Traffic lights or road signs can be used as RSUs after renovation. RSUs communicate with authorities through wired network. We assume a trusted platform module is equipped in each RSU. It can resist software attacks but not sophisticated hardware tampering. The cost of a trusted platform module is only a few tens of dollars which is affordable [1].

iii. Nodes

Nodes are ordinary vehicles on the road that can communicate with each other and RSUs through radio. We assume that each vehicle is equipped with a GPS receiver using DGPS [9] with an accuracy on the order of centimeters and an on board unit (OBU) which is in charge of all communication and computation tasks. Nodes have the lowest security level.

B. Group Signature Based Privacy System

In our framework, the communications can be divided into the key distribution phase and the regular broadcast phase. Vehicles get keys dynamically in the key distribution phase and then start to broadcast their geographic and road condition messages periodically in the regular broadcast phase. We resort to the group signature scheme for privacy provision. With group signature, members of a group sign messages under the name of the group. In a group, there are one group public key and many corresponding group private keys. A message that is signed by any group private keys can be verified with the unique group public key, and the signer's identifier will not be revealed. However, authorities hold a tracing key which can be used to retrieve the group private key from the signature. If one group private key is assigned to only one user, the signer can be identified after authorities get its group private key. Those vehicles getting keys from the same RSU form a group, where the communication range of RSUs is 300 meters. We consider that RSUs are only deployed at entrances/exits of the road segments. In a highway scenario, RSUs are normally far away from each other. In the region out of the RSU coverage, vehicles in the same group can communicate with each other in an ad hoc manner. In a city area, RSUs might overlap with each other. We define that a vehicle is only associated with one RSU at a moment to get the service.

C. Distributed Key Management

In this thesis work because it has smaller communication overhead than other group signature schemes. Meanwhile, in the short group signature protocol, there is a group private key generator which can be assigned to key distributors without revealing other secrets. The existence of the generator makes the third party possible to be key distributors. Another attractive feature of the short group signature is that it has a tracing key which can retrieve group private keys from signatures.

DOI 10.17148/IJARCCE.2015.4313

III. SECURE KEY DISTRIBUTION PROTOCOL DESIGN

We assume that each vehicle and RSU is preloaded with a global, long term public/private key pair with key size of 224 bits and a corresponding certificate of the public key signed by the certification authority (CA). We can say the pair as identity keys (I-keys). The group public key and group private keys are local, short term keys. We can say them as group keys (G-keys). Both I-keys and G-keys are unique. Thus they are considered as identifiers of vehicles and RSUs. CA's public key size is 256 bits. Furthermore, a hash function h(x), such as SHA1, is known by authorities, RSUs and all vehicles. In this thesis work, elliptical curve digital signature algorithm (ECDSA) is employed as the signing protocol and we use elliptical curve integrated encryption scheme (ECIES) as the encryption protocol. These mechanism also used by Yong Hao, Yu Cheng . Since a reliable key distribution is the foundation for the whole system, all the messages in the key distribution procedure are transmitted over the transmission control protocol (TCP). The procedure of registration is as follows.

Message 1
RSUs broadcast I-public keys, G-public keys of themselves and their neighbour RSUs with certificates and identities of revoked RSUs in their neighbourhoods regularly. Authorities employ benign RSUs around compromised RSUs to implement revocation by regular broadcasting those compromised RSUs' identities.

Message 2
When a vehicle detects the hello message, it starts registration by sending its I-public key and the certificate to the RSU if the RSU is not revoked. Normally, a public key should not be encrypted. However, in our system model, each vehicle's I-public key is unique, so it is also an identifier of the vehicle. Therefore we encrypt it to protect vehicle's privacy.

Message 3
The RSU sends the hash value of the G-private key which plans to be assigned to the vehicle and the signature of the hash value, vehicle's I-public key and RSU's I-public key to the vehicle. RSU's I-public key is also unique. The vehicle can identify the RSU's legitimacy after it verifies this message because the RSU uses its I-private key in the message.

Message 4
The vehicle encrypts its Npri and the timestamp T by using authorities' public key. Then, it sends the encryption data with the timestamp and the signature of corresponding information to the RSU. The encryption of its Npri and the timestamp is a commitment. We will use it to detect illegitimate users later. Meanwhile, the signature signed by the vehicle binds vehicle's information and the assigned G-private key. Then, the RSU cannot re-map them because the RSU does not have vehicle's I-private key

Message 5
The RSU sends the G-private key to the vehicle. The vehicle finishes registration procedure after it gets a valid G-private key. If authorities need the information of a vehicle when there is a dispute, the RSU has to send the vehicle's corresponding information to authorities.

IV. ALGORITHM

1- firstly group public keys,isentities of revoked neighbours roadside units from RSUs to Vehicle i.e., $(R_{pub,}Sig_{CA,}\ R_{pub})$
2- In the response vehicle transmit message to RSU i.e., $\{N_{pub},\ Sig_{CA,}\ (N_{pub})\}R_{pub}$
3- Now the RSU sends the hash value of the G-private key which plans to be assigned to the vehicle and the signature of the hash value, vehicle's I-public key and RSU's I-public key to the vehicle. RSU's I-public key is also unique.
$\{\ h\ (G_{prik}),\ Sig_{Rpri},\ (h(G_{prik})),\ N_{pub},\ R_{pub})\ \}\ N_{pub}$
4- The vehicle encrypts its Npri and the timestamp by using authorities' public key. Then, it sends the encryption data with the timestamp and the signature of corresponding information i.e.,
$\{(N_{pri,}\ T)CA,\ T,\ Sig_{Npri}\ (h(G_{prik}),\ (N_{pri,}\ T)CA,T,\ N_{pub}\ )\}R_{pub.}$
5- The RSU sends the G-private key to the vehicle. The vehicle finishes registration procedure after it gets a valid G-private key. Then, the RSU stores the information i.e., $\{G_{prik,}\ Sig_{Rpri}\ (G_{prik}\ )\ \}\ N_{pub}$.

where,

Rpub/Rpri	-	RSU's public/private key pair (I-key)
Npub/Npri (I-key)	-	Node(Vehicle)'s public/private key pair
SigA(M)	-	Signature of message M signed by A's private key
(M)k	-	Message M is encrypted by k or k's public key
Gpubk /Gprik	-	Group public/private key pair (G-key) for user k
T	-	Timestamp
h(.)	-	A one-way hash function such as SHA-1

A. Messages Broadcasting

Vehicles can broadcast messages under the name of the group after they get G-private keys from the RSU. In the broadcast message format, the "Grp ID" is the group ID which is used to identify a group. We add a hash value of vehicle's I-private key and the timestamp in the message. The vehicle signs the first five items in this message using the vehicle's G-private key, resulting in the signature item. We allocate 100 bytes to the "Payload" [6].

B. Accusation

When a vehicle finds that other vehicles send false messages, it will report to authorities. For example, a vehicle may maliciously detour traffic by claiming a traffic jam at a certain place but there is not in fact. Other vehicles at that place will report such claim as a false message. “Grp ID” is the accuser’s group identifier. The “Msg.” field copies the whole message that the accusor considers false. An 8- bytes field is used to indicate “Reasons” for the accusation. “h(*Npri*,T)” is the hash value of accuser’s I-private key and the timestamp. The accuser signs the first six items in this message by using its G-private key. The entire message should be encrypted by CA’s public key so that the accusation messages cannot be read by others. After receiving an accusation, authorities verify the signature in the accusation message by using *Gpub*. Then, authorities perform key retrieve operations to get the accuser’s and the accused’s G-private keys. Whereafter, authorities contact RSUs which assign G-private keys to the accuser and the accused according to group IDs. RSUs will send corresponding information back to authorities after they receive the requests from authorities. After that, authorities will calculate accuser’s and accused’s h(*Npri*,T) by using vehicles’ I-private keys and timestamps which are obtained from the accusation message and the broadcast message respectively. If the value that authorities calculate is the same with the value they get from the report, the user will be considered as legitimate. If both of them are authorized users, authorities will start the evaluation mechanism to decide which user tells the truth.

V. CASE STUDY

We have as discussed previously about “Group Formation” that’s mean some of the vehicles in the vehicular ad-hoc network creates a group and one of them is elected as a coordinator, is called group leader but there is also a situation in which some the vehicles may change their location due to high mobility and belongs to another group, is known as “Overlapping Group”. There may more overlapping groups but a vehicle belongs to only one group at a moment and after some time it belongs to another group and so on.

The Overlapping Groups in which all vehicles $V_{s} = \{v_{i1}, v_{i2}, v_{i3} \ldots\ldots v_{in}\}$ belongs to that particular group can transmit the message to other group’s vehicles i.e., $V_{d} = \{v_{j1}, v_{j2}, v_{j3} \ldots\ldots.. v_{jm}\}$. 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. In fig-2 there are three groups G1, G2, G3. v1,v2,v3,v4,v5,v6,v7,v8,v9,v10 are vehicles belong to a particular group and there are two RSUs R1and R2 which updates the information for the groups. In fig-2 it is highway scenario all vehicles are contained in a particular group but it may happen that vehicle v8 comes in the range of both groups G2, G3. This is known as Overlapping groups [10]. In our scenario we assume that vehicle v8 comes under overlapping group. Since each vehicle and RSUs is preloaded with a global long term public/private key pair with size of 224 bits and a corresponding certificate of the public key signed by authority known as “Certification Authority (CA)“ are synonym as “Identities Keys (I-keys)”.

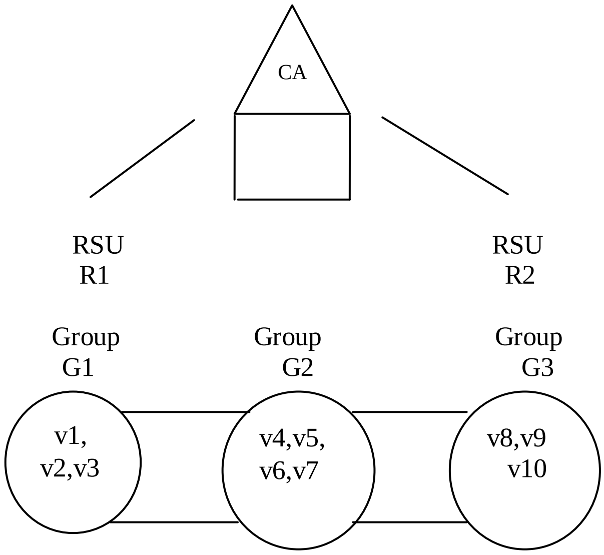

Fig-2 Group Formation in Highway

G1, G2, G3	-	Groups
v1,v2,v3,v4,v5,v6,v7,v8,v9,v10	-	Vehicles
CA	-	Certification Authority
R1, R2	-	RoadSide Unit

In above fig-2 there are three groups G1, G2, G3. v1,v2,v3,v4,v5,v6,v7,v8,v9,v10 are vehicles belong to a particular group and there are two RSUs R1and R2 which updates the information for the groups. In fig-2 it is highway scenario all vehicles are contained in a particular group but it may happen that vehicle v8 comes in the range of both groups G2, G3. This is known as Overlapping groups [10]. In our scenario we assume that vehicle v8 comes under overlapping group. Since each vehicle and RSUs is preloaded with a global long term public/private key pair with size of 224 bits and a corresponding certificate of the public key signed by authority known as “Certification Authority (CA)“ are synonym as “Identities Keys (I-keys)”.

Group public key and Group private keys that belong to a specific group are local and short term keys are known as “Group Keys (G-Keys)”. Both I-Keys and G-Keys are unique. CA’s public key size is 256 bits then a hash function h(x) such SHA1 is known by authorities, RSUs and all vehicles.

In our scenario a set of RSUs is as follows i.e.,

R = {R1, R2, R3} ----------------------------------(1)

According to our algorithm in registration process the set of RSUs {R1, R2, R3} broadcast I-Public keys, G-Public keys of themselves and their neighbour RSUs with certificates and identities of revoked RSUs in their neighbourhoods regularly. Assume in the response vehicle v4 transmit I-Public key and certificate to RSU R1. Normally a Public key is not encrypted but in our system model each vehicle’s I-Public key is unique so it also an identifier of the vehicle. Therefore we encrypt it to protect

vehicles privacy i.e.,
$\{V_{Pub,}\ Sig_{CA,}(V_{Pub})\}R_{Pub}$ --------------------------------(2)

Now the RSU R1 sends the hash value of G-Private key that is allocated to vehicle v4 and signature of hash value, vehicle's v4 I-Public key and R1's I-Public key to the particular vehicle. RSUs R1 public key is also unique i.e.,
$\{h(G_{prik}),\ Sig_{RPri},\ (h(G_{Prik})),\ V_{Pub},\ R_{Pub})\}V_{Pub}$ ------(3)

Now vehicle v4 encrypts its Private key and Timestamp T by using authorities'public key whose public key is known to every vehicle or every group then it send the encrypted data with Timestamp T and signature of corresponding information i.e.,

$\{(V_{Pri},\ T)CA,\ T,SigV_{Pri}\ (h(G_{Prik}),\ (V_{Pri},\ T)CA,\ T,\ V_{Pub})\}R_{Pub}$--(4)

Then the corresponding RSU sends the G-Private key to the relative vehicle i.e.,

$G_{Prik},\ Sig_{RPri}\ (G_{Prik})\}\ V_{Pub}$ ---------------------------(5)

Thus Our mechanism provide the Cooperative, Encryption / Decryption Digital Signature as well as Key exchange, high reliability, high authentication and integrity of data but identity based scheme provides only encryption / decryption key exchange and the reliability and authentication of Identity – based encryption scheme is moderate and provide integrity of data. But Multiparti diffie – hellman only provide key exchange and reliability and authentication of Multiparti diffie – hellman is low. Therefore the digital envelop technique provide the best results than the existing solution and it also detect and prevent many the forgery and attacks by attackers.

Table 1- Comparative study between different mechanisms

SI No	**Parameters**	**Digital Envelop**	**Identity Based Encryption**	**Multiparti Diffie - Hellman**
1	Co operative Authentication	Yes	No	No
2	Encryption / Decryption	Yes	Yes	No
3	Digital Signature	Yes	No	No
4	Key Exchange	Yes	Yes	Yes
5	Reliability	High	Moderate	Low
6	Authentication	High	Moderate	Low
7	Integrity	Yes	Yes	No
8	Tunnel Attack	High detect and prevent	Moderate detect and prevent	Low detect and prevent
9	Man in the middle attack	High detect and prevent	Moderate detect and prevent	Low detect and prevent
10	Sybil Attack	Highly secured	Moderate secured	Low secured

VI. RESULT AND DISCUSSION

Vehicles may be attacked in both the key distribution phase and the regular broadcast phase. We discuss detailed attacks and give corresponding solutions to them in this section.

A. Key Distribution Phase

i. Appropriating the ID of other vehicles

In the accusation, the compromised RSU can launch this attack by replying other vehicle's information to authorities when it requests the registration record for a certain G-private key. Then, the user of the G-private key cannot be identified. In the registration record, each vehicle has to sign its unique I-public key, hash value of G-private key and other information by using its own I-private key. Then, the vehicle's I-public key and its assigned G-private keys are bound together. RSUs cannot re-map vehicles' unique I-public keys and G-private keys arbitrarily because RSUs do not have vehicles' I-private-keys.

ii. Receiving key without acknowledgement

Both RSUs and vehicles can be malicious in this attack. In the key distribution procedure, RSUs have to get registration records, while vehicles need to obtain G-private keys. The one which is defined to send the information later could refuse to transmit after it gets secrets from the counterpart. In our design, the RSU only sends the hash value of Gprivate key and the signature of the hash value, RSU's I-public key and vehicle's I-public key to the vehicle. Then the vehicle has to submit a signature including its I-public key and the hash value of G-private key to the RSU as a part of registration record. The RSU will send the G-private key to the vehicle only after it receives this signature. We let RSUs transmit the critical information later because they are semi-trust which are more reliable. Moreover, an RSU has to get the registration record before it assigns the G-private key, so each group private key must have a corresponding registration record. It would be easy to detect RSUs' compromise if they cannot provide a legal record for a G-private key. Those vehicles which do not get the G-private key, in case the RSU is a malicious, can join the next group.

iii. Collusion Attacks

The compromised RSU and its accomplice vehicles will collude to attack. An RSU sends other vehicle's G-private key to its accomplice. Then, the malicious vehicle can broadcast messages on behalf of others. In the registration procedure, a vehicle sends a commitment to the RSU which is the encrypted vehicle's I-private key and timestamp. Then, in every message that the vehicle broadcasts, the hash value of its I-private key should be included in it. If there is a dispute, authorities get vehicle's information from RSUs. Then, they will calculate accuser's and accused's hash values by using vehicles' I-private keys and timestamps. If values that authorities calculate are different from hash values in the accusation

DOI 10.17148/IJARCCE.2015.4313

message, the attack can be detected. Both RSUs and malicious vehicles have no access to other vehicles' I-private keys. So, we prevent RSUs and their accomplice from attacking. On the other hand, a malicious vehicle may fill a wrong hash value into a broadcast message to frame up a normal RSU. When authorities find the mismatch, they will consider the RSU as a malicious. Authorities cannot decide which is the malicious, the RSU or the vehicle or both, when they find a mismatch. But they can be sure that, at least, there is one malicious. If authorities check the RSU physically and find that the RSU is working well, they can decide that the vehicle is a malicious one. As we discussed in the security model, RSUs are equipped with trusted platform modules. Only hardware attacks can compromise an RSU. Thus, it must be easy to check whether an RSU is compromised or not. Moreover, we assumed that attackers are rational. Malicious vehicles know that this attack will be detected by authorities, so they tend not to attack in this way.

B. *Regular Broadcast Phase*

i. *Collusion and Sybil Attacks*

If vehicles collude with each other, for example, verifiers are all accomplices of a sender, then all invalid messages that are sent by the sender will not be notified although the proportion of malicious vehicles may be not high. Or a malicious vehicle may launch a sybil attack by creating fictitious vehicles to act as its verifiers. In our protocol, A-Mode is only implemented when the density of vehicles reaches a bottom line. Vehicles travel on the road with high velocities, so it is not easy for accomplice vehicles to get all verifiers' positions at the same time. As we discussed in the security model, attackers are minority. Hereby, it is more difficult to launch the attack when the number of verifiers increases. Another way to defend collusion attack is choosing verifiers from the other side of the road. It would be difficult for an adversary to have colluding vehicles on both directions [12]. For sybil attack, some techniques can be employed to defend it. For instance, signal strength detection [13] in the physical layer can identify the real location of the sender. Rangefinders [14] which cost about 100 EURO is another way to locate vehicles.

ii. *Selfish Behaviours*

Selfish behaviour is inherent in the cooperative networks. In the regular broadcast procedure, some nodes may not verify any messages. They only wait for reports from others. Or some nodes verify messages, but they never report invalid messages to others. As we discussed in the security model, the VANETs are civilian networks that overwhelming majority of users are honest. Therefore, the proportion of selfish vehicles should be very small.

VII. CONCLUSION

This thesis covers the analysis, design and optimization of various attacks that may occur in the Vehicular Ad-hoc Network. The digital envelop concept reduce the possibility of attacks by attackers that may be active or passive since Vehicular Ad-hoc Network is generally applied on Intelligence Transportation System and the vehicles running on the roads are the part of vehicular ad-hoc network that have a greater mobility than mobile ad-hoc network. In this thesis work we have studied the performance of key management in a distributed environment which authenticate the message in vehicular ad-hoc network. Group formation and Overlapping Group mechanism is used to solve the problem of position and location of vehicle in vehicular ad-hoc network. 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. Since a vehicle will automatically know to which group it belongs. Hence, group formation will not require any additional communication overhead or delay.

Our approach guarantees that RSUs distribute keys fairly and provide some mechanisms to detect compromised RSUs and malicious vehicles. 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] JEAN-PIERRE HUBAUX, SRDJAN CAPKUN, AND JUN LUO EPFL, "The Security and Privacy of Smart Vehicles"
[4] Maxim Raya and Jean-Pierre Hubaux, *Laboratory for computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Switzerland E-mail: {maxim.raya, jean-pierre.hubaux}@epfl.ch* - Securing vehicular ad hoc networks
[5] "Veh. safety commun. project final report. Appendix H: WAVE/DSRC security," Nat. Highway Traffic Safety Admin., Washington, DC, USA,Apr. 2006.
[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[7] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.
[8]. A. Perrig, R. Canneti, D. Song, and J. D. Tygar, "The TESLA broadcast authentication protocol," *RSA Crypto.*, vol. 5, no. 2, pp. 2–13, Summer/Fall 2002.
[9]. P. Enge, "Retooling the global positioning system," *Scientific American*, May 2004.
[10] Prakash Tripathi, Dr.Kanojia Sindhuben Babulal, "Security in Vehicular Ad-hoc Network. "
[11] Yong Hao, Student Member, IEEE, Yu Cheng, Senior Member IEEE, Chi Zhou, Senior Member, IEEE and Wei Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs"
[12] S. Park and C.C.Zou, "Reliable traffic information propagation in vehicular ad-hoc networks," *IEEE Sarnoff Symposium*, Apr. 2008.
[13] B. Xiao, B. Yu and C. Gao, "Detection and localization of sybil nodes in VANETs," in *Proc. ACM/SIGMOBILE Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*, 2006.
[14] K. Ibrahim, M. C. Weigle and G. Yan, "Light-weight laser-aided position verification for CASCADE," in *Proc. International Conference on WAVE*, Dearborn, MI, Dec. 2008.

DOI 10.17148/IJARCCE.2015.4313