Security in Vehicular Ad Hoc Networks through Mix-Zones Based Privacy

[1]S. Kavitha, [2]M. Parveentaj

Research Scholar, Sri Jayendara Saraswathy Maha Vidayala College of Arts and Science, Coimbatore- 05, India

M.C.A., ADCA, M. Phil, Assistant Professor,
Sri Jayendara Saraswathy Maha Vidayala College of Arts and Science, Coimbatore- 05, India

Abstract: ***Vehicular Networks (VNs) seek to provide, among other applications, safer driving conditions. Vehicles need to periodically broadcast safety messages providing precise position information to nearby vehicles. Recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular adhoc networks are multi-hop networks with no fixed infrastructure. As a result, the driver's privacy is at stake. In order to mitigate this threat, while complying with the safety requirements of VNs, the creation of mix-zones security at appropriate places of the VN to prevent the attacks Vehicle. Propose to do so with the use of cryptography algorithm AES with zone based routing protocol, analytically how the combination of mix-zones into mix-networks brings forth location privacy in vehicle node. Finally, show by simulations that the proposed zone based security is effective in various scenarios.***

Keywords: Vehicular Networks, VANET, AES, Cryptography Algorithm

1. Introduction

Vehicular Networks (VNs) consist of vehicles and Road Side Units (RSUs) equipped with radios. Using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, vehicles share safety-related information and access location-based services. Initiatives in Europe [6] and the US [8] are evaluating VNs promises of safer driving conditions and more efficient traffic management. Envisioned safety-related applications require the vehicles to periodically broadcast their current position, speed and acceleration in authenticated safety messages. This messaging increases the awareness of vehicles about their neighbours' whereabouts and warns drivers off dangerous situations.

The nature of the wireless communications makes eavesdropping particularly easy. All an adversary needs to do is to deploy its devices across the area of the network that it wishes to monitor. At the same time, safety messages provide rich information on their senders, for example, the vehicle's location. This essentially allows automatic tracking of the vehicle whereabouts. Thus, it can reveal private information regarding the activities of the driver. The wide availability of VN-compatible radios (802.11-based) makes such a threat even more credible.

The use of randomly changing identifiers (i.e., pseudonyms) has been proposed to de correlate the identity of vehicles from their locations. The purpose of such a scheme is to achieve un link ability between the vehicle and its pseudonyms in the long run. However, updating the pseudonym of a vehicle in a monitored region is in effective, because the location information of safety messages can still be used for tracking. Therefore, changing pseudonyms is effective only within regions in which monitoring is impossible.

2. Problem Statement

Problem arises when one or more users try to inject false information to the network. This information is very important, and has a key role in driver's decision making. A proper decision is the result of proper information, and improper information causes improper decisions. E. g. a vehicle reports heavy traffic on a few miles ahead. But maybe a malicious user wants to cheat others for some selfish aims, e.g., to divert traffic from a given road and thus free it for themselves or for entertainment. In such case it is said that the security of VANETs is affected.

3. Related Works

Public key certificates are envisioned for this purpose. These are electronic documents that link a public key with a subject´s identity. However, using real or permanent identity would allow tracking. As opposed from that, these credentials should not make the vehicle to be completely anonymous. Liability attribution is required by the legal authority whenever misbehaviour (e.g. traffic offence, false warning) is detected. These tradeoffs are called resolvable anonymity. Two different mechanisms have been proposed to satisfy this need in VANETs – identity-based cryptography and pseudonymous short-lived public key certificates. Although they are based on different cryptographic techniques, their underlying processes of creation and use are similar. We will focus on certificates as it is the mechanism proposed in the security standard in the area, IEEE 1609.2 (IEEE Computer Society, 2006). Particularly, pseudonymous certificates allow providing both authentication and privacy protection (Callandriello, G. Papadimitratos, Lloy, & Hubaux, 2007). Readers interested on identity-based cryptographic mechanisms can refer to (Sun, Zhang, & Fang, 2007).

Vehicular contexts have an interesting feature related to identity management. As opposed to classical computer networks, in which no central registration exists, vehicles are

uniquely identified from the beginning. Indeed, this process is performed by both manufacturers and the legal authority. Manufacturers assign each vehicle a Vehicle Identification Number (VIN). On the other hand, legal authorities require vehicles to have a license plate. Both identifiers are different by nature. Whereas VINs are intended to uniquely identify manufactured vehicles, license plates are assigned to every vehicle registered in an administrative domain. Thus, VINs cannot be changed for a given vehicle, whereas license plates can change over time. Moreover, license plates are intended to be externally visible. This issue has an immediate consequence related to privacy preservation - vehicles are not completely anonymous, as visible tracking is currently possible.

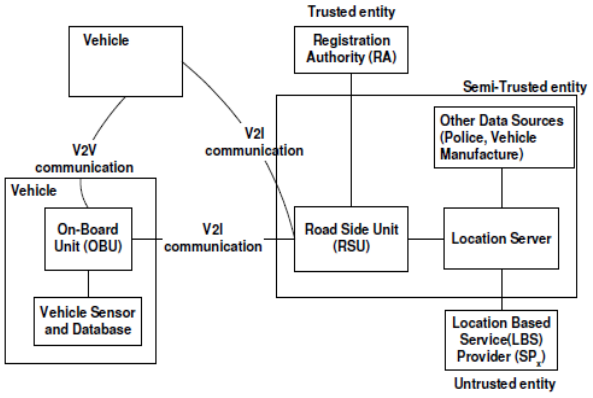

Figure 1: Alternatives to retrieve vehicular credentials

Pseudonymous certificates must be issued by a trusted authority. A Vehicular Public Key Infrastructure (VPKI) is often assumed for this purpose (Raya, Papadimitratos, & Hubaux, 2006). Figure 2 shows its composition and its relationships with other entities that were introduced on the VANET model.

VPKI is composed by a set of Trusted Third Parties (TTPs) in charge of managing pseudonymous certificates. It is assumed to be structured hierarchically. There is a single root Certificate Authority (CA) in each administrative domain (e.g. a country) and a delegated CA in each region within that domain. As vehicles from different regions (or even domains) can encounter themselves in a VANET, it is generally assumed that these CAs will be mutually recognized.

4. Proposed System

In this paper achieving location privacy in VNs with randomly changing identifiers in the presence of a global passive adversary. We are fully aware of the need for strong security in VNs, along with privacy protection. In particular, in this context, pseudonyms are anonymized public keys. Our proposal fits in this framework of pseudonymous authentication. Our contribution is threefold. First, we propose a protocol to create cryptographic mix-zones at road inter sections. This solution thwarts computationally bounded eavesdroppers while preserving the functionality of safety messages. Second, we analyze the location privacy achieved by combining mix-zones into mix-networks in VNs. These so-called vehicular mix-networks leverage on the mobility of vehicles and the dynamics of road intersections to mix vehicle identifiers. Finally, we show by means of simulations the effectiveness of the proposed mix system.

4.1 Network Model

Vehicular Networks (VNs) consist of vehicles, Road-Side Units (RSUs) and a collection of backbone servers accessible via the RSUs. We assume that a single VN Operator (VNO) is responsible for deploying RSUs in the network. Due to their relevance to life-critical applications, VNs have to satisfy several strict requirements, namely sender and data authenticity, availability, liability, and real-time delivery. VNs are a very challenging application of ad-hoc networks as all the above prerequisites must be achieved under the stringent conditions created by a highly dynamic mobile environment. To prevent accidents and inform each other of dangerous situations, vehicles periodically broadcast safety messages indicating their position, speed, acceleration, and possibly many other types of information (Fig. 1). We assume that each vehicle is equipped with a GPS device that provides accurate location information within an acceptable error margin.

Similarly to the work in, we assume that a suitable public key infrastructure is available in VNs and that the messages are properly signed to ensure the liability of their sender in case of an accident. A certificate is attached to each message to enable other vehicles to verify the sender's authenticity. Vehicles are equipped with Tamper-Proof Devices (TPDs) that guarantee the correct execution of cryptographic operations and the non-disclosure of private keying material**.**

4.2 Cryptographic Mix-Zones

A mix-zone is an anonymizing region that obfuscates the relation between entering and exiting vehicles. The adversary observes the timing and the location of the entering and exiting vehicles in order to derive a probability distribution over the possible mappings. In VNs, because we assume that mix-zones are located at road intersections, the timing of events depends on the delay characteristics of the intersection structure. Likewise, the location of entering and exiting vehicles depends on their trajectory in an intersection. Since the location of mix-zones is fixed, the adversary can identify them and thus could easily attempt to eavesdrop transmissions originating in the mix-zone area. To solve this problem, we introduce the CMIX Protocol to create Cryptographic MIX-zones: all legitimate vehicles within the mix-zone obtain a symmetric key from the road-side unit (RSU) of the mix-zone, and utilize this key to encrypt all their messages while within the zone. The symmetric key is obtained through a key establishment phase. To ensure the functionality of safety messages, this mix-zone key can be obtained by nodes approaching the mix-zone with the help of a key forwarding mechanism, and, finally, the RSU can swap to a new key through a key update mechanism. AES Symmetric Key Encryption provides data confidentiality.

Hash Code of Message encrypted with sender's Private Key providing a digital signature. (Since only the sender could have produced the encrypted hash code). Even if the attacker came to know of the symmetric key, in order to alter the

message and get away with it, he would have to know the sender's private key.

4.2.1 Key Establishment

Symmetric Key systems were the first type of cryptosystems used to secure information. In these systems, nodes can only communicate after sharing and agreeing on a secret key that is used to process communication messages. As stated previously, VANETs are a relatively new research area and the security for such networks is only starting to be a major research topic. Hence, there are not many papers that propose the use of such systems for VANET security as the attention is more directed towards Public Key and Identity Based systems. Nevertheless, this section discusses existing proposals of using Symmetric Key systems for VANET security.

$$Vi \rightarrow RSU : Request, T_s, Sign_i(Request, T_s), Cert_{i,k}$$

$$RSU \rightarrow v_i : EK_{i,k}(V_i, SK, T_s, Sign_{RSU}(V_i, SK, T_s)), Cert_{RSU}$$

$$Vi \rightarrow RSU : ACk, T_s, Sign_i(ACK, T_s), Cert_{i,k}$$

The Key Establishment protocol. Ts is a time stamp, Sign () is the signature of the message, Cert is the certificate of the message sender. As soon as a vehicle vi enters in the of transmission range of an RSU, R Beacon, it initiates the key establishment protocol described. As the vehicle knows its own location and the location of the RSU (announced in the beacon), it can estimate whether it is within the mix-zone, defined by a transmission range RCMIX < R Beacon. If so, the vehicle vi broadcasts one or, if needed, several key request messages (first message in Table 1). The RSU replies with the symmetric key SK encrypted with the public key of vehicle vi and a signature. vi receives and decrypts the message. If the message is validated, vi acknowledges it and SK can be used to encrypt all subsequent safety messages until vi leaves the mix-zone. In case RSUs are co-located (i.e., their mix-zones overlap), vehicles are aware of all CMIX keys so that they can decrypt all messages. Alternatively, co-located RSUs could coordinate to use the same CMIX key.

4.2.2 Key Forwarding

Vehicles in the extended mix-zone, that is, at a distance d from the RSU where RCMIX < d < R Beacon may be unable to obtain directly the key from the RSU; for example, they are beyond their transceiver's range for bidirectional communication. Thus, they cannot decrypt safety messages coming out of the CMIX. As vehicles know they are within an RSU transmission range, when they receive encrypted safety messages, they issue one or, if needed, several key requests to obtain the SK key with the help of vehicles already in the mix-zone which are aware of it.

The signature from the RSU, along with the time stamp, allows validating the transmitted symmetric key. Note that vehicles in the extended region do not encrypt their safety messages with the CMIX key before entering the mix-zone (RCMIX). The entire above message is in addition signed by v1.

4.2.3 Key Update

Propose a Key Update mechanism to renew or revoke CMIX symmetric keys. The RSU is responsible for such key updates and determines when to initiate the process. Key updates occur only when the mix-zone is empty and vehicles obtain new keys via the key transport and key forward protocols. The CA obtains the new symmetric key from the RSU over a secure channel, to satisfy the liability requirements (i.e., possibly, decrypt safety messages in the future). The robustness provided by the system is increased, if key up dates are asynchronous across different base stations. But there is a trade of between security and cost, as frequent updates can incur additional overhead.

5. Simulation Results

Presents the average location privacy obtained in an intersection for various vehicle densities. We show that the achieved location privacy varies with respect to the traffic congestion and the vehicle density. We observe that the less congested the traffic is, and the easier it is for the adversary to track vehicles based on their delay characteristics. The upper bound is the average of over the number of user per intersection in the simulation.

Table 1: Table showing the Simulation parameters

Parameter	*Value*
Field Size	3000X3000m
MAC	802.11
Fading	Rayleigh
Simulation Time	60s or user define
Number of (s,d) paris	10
Number of nodes	25…100

Presents the success probability of an adversary in tracking vehicles. The adversary success probability is the ratio of the number of successfully mapped vehicles to the total number of vehicles in a mix-zone, averaged over all mix-zones. As expected, the success ratio decreases as the entropy increases. Even with a high ½ and congested traffic, the adversary success ratio is relatively high. We show next that the combination of mix-zones into mix-networks significantly reduces this success ratio.

Table 2: Comparison of node disjoint path

Number of Nodes	0	100	200	300	400	500	600	700
Geocast(AAG)	2	2	2	2	2	2	2	2
Aggregation	2	4	6	8.3	10	12	11	10.8
Baseline	4	12	21	32	44.6	50	55	60
Proposed	1.2	1.5	1.53	1.65	1.67	1.87	1.9	1.99

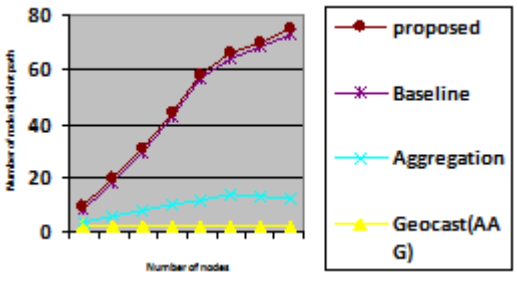

Figure 2: Number of node v/s node disjoint path

In figure 2 check with different type exiting system method with proposed one here we show to reduce the disjoint path in proposed system.

Table 3: Comparison of information routing

Distribution of information	0	20	40	60	80	100
Existing City 100 nodes	5	21	22	22.65	23	28
Proposed City 100 nodes	5.4	22.4	24	28	30	35.4
Existing Highway 50 nodes	21	40	40	41	43	46
Proposed 50 nodes	23	45	46.4	48	56	70

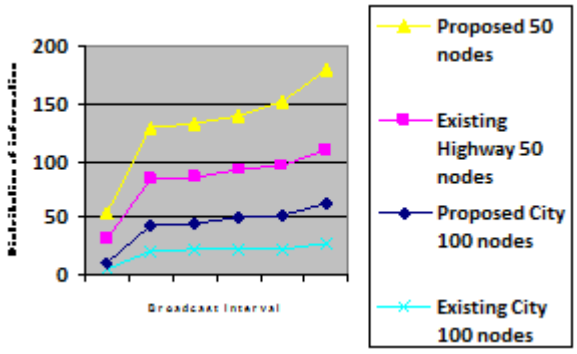

Figure 3: Information with different topology

Figure 3, information distribution compare with existing method with new method.

6. Conclusion

The problem of providing location privacy in vehicular networks. Introduce the zone based security protocol to create AES algorithm and cryptographic mix-zones at road intersections wherein vehicles can change their pseudonyms. Vehicular mix-networks rely on the mobility of vehicles to provide location privacy the efficiency of safety messages. Further, we proposed an anonymous access protocol to address threats to privacy that arise due to access to LBS (location based service) applications, and found that it was robust under the global adversary model, as well as under the safety application constraints. Future work includes evaluation of proposed location privacy solutions under more realistic mobility for vehicles, combined with map data, and with communication traffic models.

References

[1] R. Beresford. Location privacy in ubiquitous computing. Technical Report 612, University of Cambridge, January 2005.
[2] R. Beresford and F. Stajano. Mix-zones: User privacy in location-aware services. In Proceedings of PerSec, 2004.
[3] L. Butty an, T. Holczer, and I. Vajda. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In Proceedings of ESAS, 2007.
[4] G. Calandriello, P. Papadimitratos, A. Lloy, and J.P. Hubaux. Efficient and robust pseudonymous authentication in vanets. In The Fourth ACM International Workshop on Vehicular Ad Hoc Networks (VANET), 2007.
[5] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84-90, February 1981.
[6] M. Gerlach and F. GÄuttler. Privacy in VANETs using changing pseudonyms - ideal and real. In Proceedings of VTC, April 2007.
[7] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identiffers: a quantitative analysis. Mobile Networksand Applications, 10(3):315-325, June 2005.
[8] Hoh and M. Gruteser. Protecting location privacy through path confusion. In Proceedings of SECURECOMM, pages 194-205, 2005.
[9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Towards modelling wireless location privacy. In Proceedings of PET, 2005.
[10] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Silent cascade: Enhancing location privacy without communication QoS degradation. In Proceedings of SPC, pages 165-180, 2006.

Author Profile

S. Kavitha M.Sc (C.S), Pursuing M. Phil (CS) in Sri Jayendra Saraswathy Maha Vidyalaya CAS, Area of Interest, Networking, Software Project management.,

M. Parveentaj M.C.A., ADCA, M.Phil., working as an Associate Professor, in Department of Computer Science- Sri Jayendra Saraswathy Maha Vidyalaya CAS for a passed 8years. Area of Interested; Networking, Data Mining, Software Engineering. Presented 2 papers in an International Conference, 1 paper in National Level.