Advanced Encryption Standard an Hash Authentication in Service-Oriented Vanets

[1]S.Chandrapandian [2]Mrs.R.Adaline [3]Mr.M.Srinivasan
[1]M.E (Final year) [2] Suji M.E., (Ph.D). Assistant Professor
[3]B.Tech.,M.E.,(Ph.D).,Assistant Professor.,PEC
[1, 2] RatnaVel Subramaniam College of Engineering & Technology.

Abstract--- Inter vehicular communication lies at the core of a number of industry and academic research initiatives that aim at enhancing the safety and efficiency of transportation systems. Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other and with roadside units (RSUs). Service oriented vehicular networks are special types of VANETs that support diverse infrastructure-based commercial services, including Internet access, real-time traffic management, video streaming, and content distribution. Many forms of attacks against service-oriented VANETs that attempt to threaten their security have emerged. The success of data acquisition and delivery systems depends on their ability to defend against the different types of security and privacy attacks that exist in service-oriented VANETs. This paper introduces a system that takes advantage of the RSUs that are connected to the Internet and that provide various types of information to VANET users. We provide a suite of novel security and privacy mechanisms in our proposed system and evaluate its performance using the ns2 software. We show, by comparing its results to those of another system, its feasibility and efficiency.

keyword: Anonymity, hierarchal password-based key derivation (HARDY) function, key derivation, roadside units (RSUs), security, service-oriented vehicular ad hoc networks.

I. INTRODUCTION

The development and wide utilization of wireless communication technologies have transformed human lives by providing the most convenience and flexibility ever in accessing Internet services and various applications. Lately, researchers conceptualized the idea of communicating vehicles, giving rise to vehicular ad hoc networks which are the main focus of engineers who yearn to turn cars into intelligent machines that communicate for safety and comfort purposes.

A vehicular ad hoc network is composed of vehicles that are equipped with wireless communication devices, positioning systems, and digital maps. Vehicular ad hoc networks s allow vehicles to connect to roadside units (shortly RSUs), which may be interconnected with each other through a high-capacity mesh network. Current research trends for vehicular ad hoc networks focused on developing applications that can be grouped into the following two classes:

1) Improving the safety level on the road.

2) Providing commercial and entertainment services. To enable such applications, vehicles and RSUs will be equipped with onboard processing and wireless communication modules. Then, vehicle-to-vehicle and vehicle-to-infrastructure (shortly V2I) communications will directly be possible when in range or across multiple hops. RSUs are usually connected to the Internet and allow users to download maps, traffic data, and multimedia files and check emails and news.

These kinds of vehicular ad hoc networks are expected to virtually provide all types of data to drivers and passengers. The unique features of inter vehicular communication (shortly IVC) is a double-edged sword: A powerful collection of tools will be available, but a set of dangerous attacks becomes possible. Recently, there have been different proposals for securing vehicular ad hoc networks s and lessening the potential risks of attacks. A detailed description of different attacks and their countermeasures can be found. Few works deal with the security of service-oriented vehicular ad hoc networks. Most of these works provide solutions to specific problems such as user privacy or data confidentiality. Nevertheless, to our knowledge, none of the previous works proved to provide security of data and location privacy of users in service-oriented vehicular ad hoc networks while ensuring efficient throughput and acceptable end-to-end latency.

From another point of view, several projects were launched, with the security of vehicular ad hoc networks being their main concern. Some of these have already delivered their outcomes, whereas other projects, such as ITSSv6, are still in progress. Most of these projects provide a general overview of security features that should be employed in vehicular ad hoc networks. For example, the SeVeCom Project focused on safety applications such as collision warning. The security of such applications is different from the security of service-oriented applications because of their different security requirements.

For example, the data exchanged in safety messages need not be encrypted. However, messages that contain data from infotainment applications must be tightly encrypted. Many similar security requirements greatly differ between safety mechanisms and service-oriented systems.

In this paper, we study the security of data messages exchanged between users and RSUs and the location privacy of vehicular ad hoc networks users who exchange these messages. There are systems that are proposed in the literature and have this same aim. However, they use asymmetric encryption systems, mainly the elliptic curve cryptography (shortly ECC) standard. We, on the other hand, use a symmetric scheme Advanced Encryption Standard and propose an approach to increase its security to a high extent by using a hierarchical-based encryption function. The main contributions of this paper can be summarized as follows.

1. We propose a novel approach for users to start their connections in the vehicular ad hoc networks in a secure way.

2. We illustrate a new handover scheme that is particularly suitable for vehicular ad hoc networks.
3. We explain a new cryptographic approach that provides much higher security measures compared to existing ones and analyze the performance of our approach using mathematical and simulation means.
4. We suggest two novel mechanisms for data confidentiality and users' location privacy in vehicular ad hoc networks. This paper is organized as follows.

We first conduct a study of previous works in Section II. Next, we discuss a framework that allows users to create accounts with RSUs and connect to them in secure sessions in Section III, where we additionally describe the security features of our framework, which employs multiple packet keys for encryption, and also describe a new approach for providing location privacy to users by using packet-based pseudonyms and mix zones.

We analyze our cryptographic scheme and the system deployment cost in Section IV. Finally, we prove through simulations in Section V that our system provides firm security while ensuring a high success ratio and low latency. We call our system secure and efficient data acquisition in vehicular ad hoc networks s (REACT).

II. Related Work

Several researchers studied security challenges related to vehicular ad hoc networks s. In this section, we conduct a brief study of recent and relevant works, Security vulnerabilities and challenges in vehicular networks. A detailed threat analysis, a basic attacker model, and appropriate security architecture are provided.

In addition, there have been several proposals for privacy preservation in vehicular ad hoc networks s. If vehicular ad hoc networks users use the same ID whenever they send a packet, an attacker could listen to their packets and build a profile of their locations, which jeopardizes their privacy. Hence, pseudonyms were proposed to deceive attackers. It preserves the location privacy of a user by breaking the link ability between two locations.

A vehicle can periodically update its pseudonym. Considering that a powerful adversary may still link the new and old pseudonyms by monitoring the temporal and spatial relations between new and old locations, the techniques of mix zones and silent period, and ad hoc anonymity were proposed. A mix zone is an area in which several vehicles change their pseudonyms together so that an attacker will not distinguish the new pseudonym of each vehicle. The silent period approach enables mobile users to jointly change their pseudonym with other approaching users by simultaneously entering a silent period, in which all nearby users suppress their location updates and wield new pseudonyms. Ad hoc anonymity extends mix zones by using dummies, which are virtual users that are created before the pseudonym change starts and disappear after it ends.

The dummies link several pseudonym change sets together and mix up all the users who have participated in pseudonym changes at different times. One major disadvantage in the mix zone approach is the process of pseudonyms refill. For example, assume that each vehicle acquires a new set of pseudonyms from the central authority (shortly CA) when their stored pseudonyms are used. Another disadvantage, is that vehicles do not know where the adversary installed its radio receivers, i.e., where the observed zones of the adversary are. Current approaches that use mix zones assume that the observed zones are small and scattered such that users who change their pseudonym every several transmissions will avoid sending multiple packets with the same pseudonym from within an observed zone. This assumption, however, is not viable in case of a global eavesdropper who can hear all messages in the network. Another disadvantage is that a user might not always find other near users that are willing to enter a mix zone. Vehicles form groups, and the messages of all group members are forwarded by the group leader. Hence, the privacy of group members is protected by sacrificing the privacy of the group leader.

Moreover, if a malicious vehicle is selected as a group leader, all group members' privacy may be leaked. The group signature is a privacy scheme in which one group public key is associated with multiple group private keys. Although an eavesdropper can know that a message is sent by the group, it cannot identify the sender of the message.
In a pseudonym is combined with a group signature to avoid storing pseudonyms and certificates in vehicles. With regard to message (or data) security, we notice that few studies were devoted to developing security mechanisms for value-added applications in vehicular ad hoc networks. We proposed a secure and efficient scheme with privacy preservation in which a vehicle needs to acquire a blind signature before it can access the desired services from the near RSU. A service provider (Shortly SP) is responsible for verifying the validity of signatures. The ABAKA protocol uses ECC at the RSUs to authenticate requests from multiple vehicles together. ABAKA requires a tamper-proof device to be installed in vehicles and requires SPs to generate session keys that will be used in their connection with vehicles. An RSU is made to sign and deliver messages to end users on behalf of CAs.

The CA derives a secondary secret key from its private key and securely sends it to the RSU. The receiver verifies a message by checking both the correctness of the key signature and the location of the sender.

Another approach depends on hash chains to sign messages. Each vehicle periodically generates a new hash chain and sends it to the CA, which generates an authentication code (shortly AC) from the hash chain and sends it to the vehicle. The ACs is used as signatures for messages, and RSUs are used for relaying messages between vehicles and CAs. An approach that is based on Lite-CA-based public key cryptography and on-path onion encryption scheme is proposed. The approach relies on encrypting a message by each relaying hop and thus prevents any adversaries from tracing message flows.

The secure and privacy enhancing communications schemes (shortly SPECS) protocol is based on bilinear pairing and bloom filters to replace hash values in notification messages to reduce the message overhead and enhance the effectiveness of the verification phase.

III. Proposed Framework

The security of such applications is different from the security of service-oriented applications because of their different security requirements. The data exchanged in safety messages need not be encrypted. Data from

infotainment applications must be tightly encrypted. It uses a symmetric scheme (Advanced Encryption Standard (AES)) and proposes an approach to increase its security a high extent by using a hierarchical-based encryption function. The receiver verifies a message by checking both the correctness of the key signature and the location of the sender. Another approach, in depends on hash chains to sign messages. Each vehicle periodically generates a new hash chain and sends it to the CA, which generates an authentication code (AC) from the hash chain and sends it to the vehicle.

A. Procedure

1. The CA derives a secondary secret key from its private key and securely sends it to the RSU.
2. The receiver verifies a message by checking both the correctness of the key signature and the location of the sender
3. The data exchanged in safety messages (such as location information or warnings) need not be encrypted. Each vehicle periodically generates a new hash chain and sends it to the CA, which generates an authentication code (AC) from the hash chain and sends it to the vehicle on the RSU is used for relaying the message between CA and vehicle.

B. System and Security Models

The last decade has witnessed a rising interest in vehicular networks and their numerous applications. Although the primary purpose of vehicular ad hoc network standards is to enable communication-based automotive safety applications, they allow for a range of comfort applications. Many services could be provided by exploiting RSUs as delegates to obtain data on the user's behalf.

These services span many fields, from office on-wheels to entertainment, downloading files, reading e-mail while on the move, and chatting within social networks. In this paper, we design a service-oriented vehicular security system that allows vehicular ad hoc network users to exploit RSUs in obtaining various types of data. In REACT, users register once with the RSUs online (through the Internet) before they start connecting to the RSUs from their vehicle. After registration, the RSUs obtain from a trusted authority (shortly TA) a master key (Km) for the user. The users get their Km the first time they connect to an RSU from their vehicle. We describe a novel algorithm that uses the users' password from their account to securely transfer their Km to them. Km will be used to encrypt the initial packet key, which is assigned to the user at the beginning of each session.

Then, each packet will be encrypted by a set of derived keys. With regard to the assumptions, we presume that each vehicle is equipped with a positioning system and a digital map and has an Electronic License Plate (shortly ELP) installed.

In all cases, however, each RSU has a way of connecting to any other RSU (possibly through other RSUs).

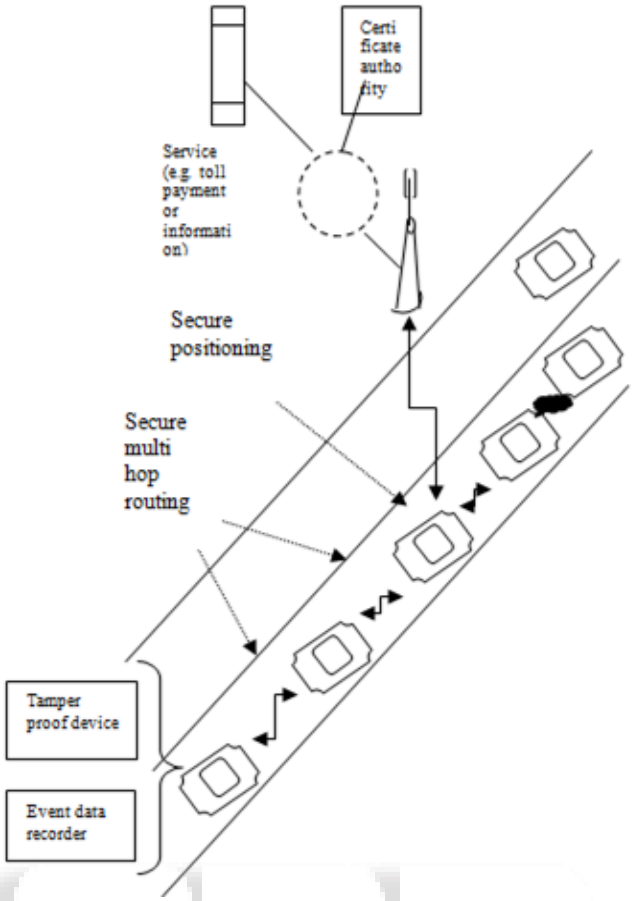

Fig.1: Overview of the Security Architecture

HARDY function for encrypting and decrypting messages:
Algorithm:

Hierarchal Password – based key derivation function (HARDY)
At the source:
Input: construct-size string S, plain text message M, initial count IC1, encryption function E [], number of algorithm rounds n, size of encryption key: L bits.
Output: cipher Message M_c

(1) Begin
(2) Generate random salt S_1, of size S_3 bits.
(3) Calculate k1=$PBKDF_2$ (S_1,S_2,IC_1,L)
(4) For (i=2;i>1;i++)
(5) Generate IC1 (random integer above 1000)
(6) Generate Si (random salt of size S5 bits)
(7) Calculate Ki = BKDF2 (Ki-1,Si,ICi,L)
(8) Encrypt Mp using Kn to get Mn=Ekn[Mp]
(9) For(i=n;i>1;i--)
(10) Calculate mi-1=Eki-1[Si][ICi][Mi]
(11) Calculate final cipher message Mc=S1
(12) Return Mc
(13) End

C. Registration and Session Management Vehicles might be occupied by several users, where each user might have his or her own interests, it is better to consider each user as a distinct member and give him or her unique account with the RSUs. Hence, we require users to register with the RSUs at the beginning through the web before they start connecting from their vehicles. The registration is done by the user only once to create an account with the RSUs and to

benefit from security measures that exist in Internet protocols.

These measures will enable users and RSUs to exchange credentials and keys that will help them start their connection in the vehicular ad hoc network in a secure way.
i) Recordkeeping: When users register using the RSU website, they specify their personal details plus a username and password to use for authentication when they connect to the RSU network from their vehicle. Users also choose a default RSU, which will save their account n its database. Examples of users' interests are web pages, certain news, traffic information in certain areas, and email messages. When they later connect to the vehicular ad hoc network, they send a Hello packet to the nearest RSU, which will notify their default RSU, which, return, retrieves their interests from its database and collects the required data for them. This later operation might entail fetching certain news and grouping them, contacting web servers and saving their HTML files, contacting email servers on the user's behalf, and downloading messages. User can choose any RSU as their default one, but it is best to select the nearest to their starting point in the vehicular ad hoc network.

Some user interests may require authentication, which means that the RSU needs to obtain from the users their credentials with the corresponding SPs so that it can connect to these SPs on the users' behalf. In REACT, we require users to provide during registration their authentication data with these SPs in addition to a secret key Kc that is used by the RSU to encrypt their authentication data and save them. The RSU does not save Kc, which remains a secret to the users. When the users connect to the vehicular ad hoc network from their vehicle, they send Kc to the RSU, which will then use Kc to decrypt the user's credentials with the SPs and obtain the data. However, the RSU in this last step does not save Kc, which is used by the RSU's software only. This way, the user credentials with other systems remain hidden in the RSU database. Nevertheless, it uses them to obtain the users data as fast as possible after the users have connected to the vehicular ad hoc networks. In addition, the users provide, during registration, the ELP of the vehicle from which they will connect to the vehicular ad hoc networks.

D. Main Key:

After the users have registered, their default RSU saves their count and contacts the TA to obtain a master key (Km) for them. The users obtain Km the first time they connect from their vehicle to one of the RSUs. To achieve this, we propose a technique that depends on deriving a group of encryption keys from the users' password and using these key to securely transfer Km to them. To generate these keys, we propose a new key derivation and encryption function. One of the inputs to this function is an initial iteration count (shortly IC1), which an integer is kept as a secret between the user and the RSU.

After registration, the RSU generates IC1 and sends it to the user (online during the Internet session in which the user registers), who saves it and uses it as an input to the hierarchal password-based key derivation (HARDY) function when he or she obtains and decrypts Km.

E. Participating in a Session:

Each time a user connects to an RSU, he or she starts a new session. Preserve users' location privacy, we make an RSU assign to a user a new pseudonym in each packet. A user tarts a session by sending a Hello packet that contains his or her username to the nearest RSU. Each packet will include a timestamp to be used for resisting replay attacks. When the RSU receives the Hello packet, it starts preparing the user's data that do not require authentication with other systems, according to his or her interests in his or her profile. Interests that require authentication with other systems will be delayed until the RSU gets Kc from the user. Although the RSU prepares users' data, it assigns them a pseudonym and sends it to them in an ID packet. The user replies with an "Identify" packet that contains his or her username, password, and Kc. Both packets will be encrypted using Km.

IV. Simulations Result

The simulation results given as follows:

1. Message success ratio (shortly MSR), which is the percentage of messages that are successfully received at their destinations.
2. Message response time (shortly MRT), which is the total time required to send a request from a vehicle to an SP and to receive the answer.
3. Initialization phase time (shortly IPT), which is the system security initialization time, i.e., the average time between the instance a vehicle starts a session to the instance it sends the first packet encrypted with a session key.
4. Average overhead traffic (shortly AOT), which is the extra traffic sent or received by a vehicle.

V. Conclusion

How we can ensure security and privacy in service-oriented vehicular ad hoc networks represents a challenging issue. In this paper, we have answered this question with our proposed privacy-preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption.

VI. Future Work

The evaluation of our proposed scheme confirmed its effectiveness compared to a recent security mechanism for vehicular ad hoc networks. The ongoing work on REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. We are designing an RSU scheduling mechanism in which an RSU builds a schedule that is divided into time slots (TSs). In each TS and all users that are expected to connect to the RSU are specified. Hence, an RSU prepares users' data and caches them during a free TS before the users connect. Using this scheme, the RSU distributes its load among the available TSs.

References:

[1] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks".

[2] "Brute-force attack," Wikipedia. [Online]. Available: http://en.wikipedia. Org/wiki/Brute-force attack.
[3] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs".
[4] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs".
[5] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and robust pseudonymous authentication in VANET".

