ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Framework for Data Security, Identification and Authentication in VANET

G.Archana ,S. Andal

Embedded System Technologies, Raja College of Engineering and Technology Madurai, Tamilnadu, India.

Department of Electronics and Communication Engineering, Raja College of Engineering and Technology Madurai, Tamilnadu, India.

ABSTRACT— The vehicular communication contains the safety and efficiency of transportation systems. Vehicular ad hoc networks (VANETs) enable vehicles to communicate with each other and road side units (RSUs). Service oriented vehicular networks are special types of VANETs that support infrastructure-based commercial services, including Internet access, real-time traffic management, video streaming, and content distribution. Privacy-preserving data acquisition and forwarding scheme by introducing a novel cryptographic algorithm for key generation and powerful encryption. Multiple numbers of users can connect for the communication. M-REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. M-REACT provides the security for data and scheduling mechanism of RSU divided into number of time slots. In M-REACT that propose an algorithm that uses the key derivation function in several iterations to strengthen the security of the encrypted message.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.

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 impart vehicles, giving rise to vehicular ad hoc networks (VANETs), which are the main focus of engineers who yearn to turn cars into intelligent machines that communicate for safety and comfort purposes. A VANET is composed of vehicles that are equipped with wireless communication devices, positioning systems, and digital maps. VANETs allow vehicles to connect to roadside units (RSUs), which may be interconnected with each other through a high-capacity mesh network. Current research trends for VANETs focused on developing applications that can be grouped into the following two classes:

1) Improving the safety level on the road and
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 (V2I) communication's 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. Security requirements based on the safety mechanism.

The unique features of inter vehicular communication (IVC) are 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 VANETs and lessening the potential risks of attacks. A detailed description of different attacks and their countermeasures can be found in and . Few works and deal with the security of *service-oriented* VANETs. 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* VANETs while ensuring efficient throughput and acceptable end-to-end latency.

II. PREVIOUS WORK

A. System and Security Models

The last decade has witnessed a rising interest in vehicular networks and their numerous applications. Although the primary purpose of VANET standards is to enable communication-based automotive safety applications, they al- low 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 VANET 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 (TA) a master key (K_m) for the user. The users get their K_m 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 K_m to them. K_m 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. We also assume a hybrid RSU architecture in which some RSUs are directly wired to each other, others connect to the RSU network through the Internet (using gate- ways), whereas a third group is both wired to other RSUs and has an Internet connection. In all cases, however, each RSU has a way of connecting to any other RSU. (possibly through other RSUs).

In addition, several TAs are connected to the RSUs through secure wired links. Similar to , we assume that TAs have powerful firewalls and other protections that prevent them from being compromised. In addition, the RSUs are supposedly equipped with trusted platform modules (TPMs), intrusion de- tection systems, and firewalls that enable them to resist software attacks. These assumptions were made by several works such as and, which showed that RSUs can be well defended against software attacks. With respect to hardware attacks, RSUs can be monitored using hidden surveillance cameras such as digital video or analog CCTV cameras that report to a central station, in which observers can immediately notice a hardware attack and take the appropriate actions. The RSUs do not store sensitive data, but each RSU has a secure connection to a database server that stores the RSUs' private information. Each RSU will have its own database to avoid the effect of failures. In addition, we assume that each RSU will be monitored by a TA, which, upon detecting a malicious behavior from the RSU, will isolate it from the network by informing other RSUs, which inform vehicles that are connecting to them. A secure protocol (such as IP tunneling) is assumed to connect RSUs to one another.

For VANET users, we assume that each user will connect to a single RSU at a single time (to reduce overhead). Vehicles and RSUs exchange messages using unicast when they are within direct range and depend on the network-layer routing protocol when they are apart. For this purpose, we designed an efficient routing protocol that transfers messages between a vehicle and an RSU (and vice versa) through other vehicles in a reliable manner. Our routing protocol, called ROAMER outperformed many routing protocols in terms of delivery ratio, delay, and bandwidth consumption. The details of ROAMER (which we used in the simulations of M-REACT) .

B. Registration and Session Management

Because vehicles might be occupied by several users, where each user might have his/her own interests,it

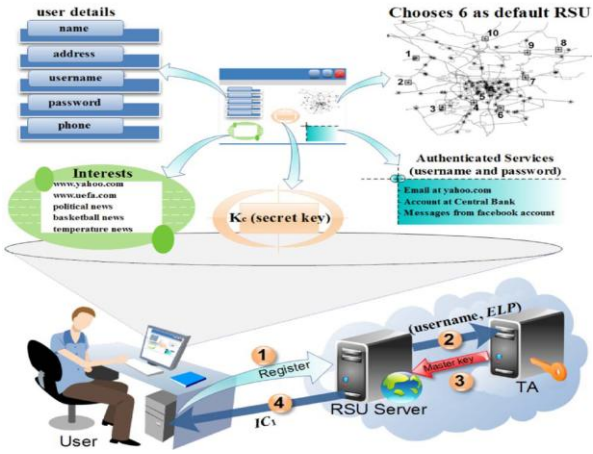

Fig.1. Sample online registration scenario.

is better consider each user as a distinct member and give him/her a 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 VANET in a secure way.

1) Registration: When users register using the RSU web- site, they specify their personal details (i.e., name, address, and phone) 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 in its database. Examples of users' interests are web pages, certain news, traffic information in certain areas, and email messages (possibly from different email accounts). When they later connect to the VANET, they send a *Hello* packet to the nearest RSU, which will notify their default RSU, which, in turn, 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 VANET. In M-REACT, we require users to provide during registration their authentication data with these SPs in addition to a secret key K_c (e.g., a sequence of 12 random characters) that is used by the RSU to encrypt their authentication data and save them.

2) Master Key: After the users have registered, their default RSU saves their account and contacts the TA to obtain a master key (K_m) for them. The users obtain K_m the first time (after registration) they connect from their vehicle to one of the RSUs. To achieve this, we propose a technique (see Section III-C1) that depends on deriving a group of encryption keys from the users' password (of their account with the RSUs) and using these key to securely transfer K_m 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 (IC_1), which is an integer kept as a secret between the user and the RSU. After registration, the RSU generates IC_1 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/she obtains and decrypts K_m. Figure shows an example of a user's registration.

III PROPOSED WORK

In M-REACT focuses on making the proposed system more scalable in terms of the number of users that can connect to an RSU. M-REACT provides the security for data and scheduling mechanism of RSU divided into number of time slots. In REACT that propose an algorithm that uses the PBKDF2 key derivation function in several iterations to strengthen the security of the encrypted message.

Recently, there have been proposals to use algorithms that require large amounts of computing resources to make custom hardware attacks (which use parallel hardware) more difficult to mount. One concrete instance of such an algorithm is the scrypt() function, which is based on the concept of sequential memory-hard functions. The scrypt() function uses PBKDF2, in addition to a pseudorandom function (PRF), to generate p blocks of length *L* octets from the provided password and salt. These blocks are independently mixed using a mixing function, and the final output is then generated by once again applying PBKDF2 using the well-mixed blocks as salt.

In M-REACT, we propose an algorithm that uses the PBKDF2 key derivation function in several iterations to strengthen the security of the encrypted message. The hardiness of cracking the final message is much increased at the expense of slight overhead in executing the algorithm.

a) Ensuring Location Privacy: In Section II, we provided a summary of the methods proposed so far to provide the location privacy of users. We described the major disadvantages that exist in these methods, such as pseudonyms refill and unknown adversary locations. To deal with these disadvantages, we adopt the concept of ad hoc anonymity in M-REACT while modifying it by making an RSU give the user a new pseudonym each time it sends a packet to him/her. Each RSU will have its own address pool, which can be viewed as a hash function that hashes the username to an integer within a certain range. Pseudonyms are made of the following two parts: 1) the RSU *ID* and 2) the random *ID* picked by the RSU from its address pool. If conflicts occur, a rehash of the obtained *ID* is performed. Because an RSU is expected to frequently send control and data packets to a vehicle during their connection, the pseudonym change frequency will be high. Each time a vehicle needs to change its pseudonym, it needs at least one neighbor that is ready to enter a mix zone with it. Then, multiple dummies can be created to ensure a powerful mix zone that can deceive the attacker, as proposed in . Note that a pseudonym change should be accompanied with changing both the physical and medium access control (MAC) addresses so that the attacker will not be able to link the two pseudonyms together. In REACT, each RSU stores a table T_r that contains five fields, i.e., username, current_*ID*, next_*ID*, current_key, and next_key . Current_*ID* is the last pseudonym that the RSU sent to the user, whereas next_*ID* is the pseudonym that the RSU will send to the user in the next packet.

b) Packet-Based Keys: Many proposed systems for VANET security disagree on the best key-management method to be used when assigning encryption keys to vehicles. Using a single key to encrypt all messages in a session allows an eavesdropper to relate the key with its source, which violates the user's privacy. Hence, short-lived keys are used to strengthen the confidentiality of data and preserve the user's privacy. The TA and periodically renewed after all the keys have been used. In, it is proposed that the encryption keys should frequently change (e.g., every couple of minutes), depending on the driving speed. Another approach assumes that the encryption key is changed whenever connecting to a new SP. A recent scheme assumed that the keys should be changed depending on the frequency with which the vehicle joins the network. The approach of periodic key renewal is considered unsafe, because an attacker can eaves drop the packet that contains the new keys and apply a brute-force attack to get the keys. In REACT, we define the concept of packet-based keys, where each set of keys will be used to encrypt a single packet. In addition, a packet key is not sent from the RSU to the user in a specific packet; rather, it is derived from the encrypted content of the current packet.

When a user U starts a new session with an RSU R, the RSU obtains from the TA a packet key K_s and sends it to U, encrypted with his K_m. U uses K_s to encrypt the next packet that he sends to R. Then, each packet will be encrypted with a new set of keys. The body of each packet will contain a start_of_key variable of type integer that contains the index of a random byte in the packet body. A string S will be chosen starting from this byte. For example, if the size of S is 40 and if the value of start_of_key is 47, then U will count 47 B from the start of data and will save the next 40 characters as the new value of S with which the next set of packet keys will be derived. The user must check the entropy of S before sending the packet. If the resulting S has an entropy below a certain threshold (e.g., 60), U changes the value of start_of_key, checks the entropy of the new S, and so on. If U tries many values of start_of_key without finding a suitable S, he generates a suitable random value of S and adds it at the end of the packet.

IV. SIMULATIONS

This section presents the simulations that we performed to evaluate M-REACT. We used the ns2 software (version 2.34 with the 802.11p amendment and the Nakagami propagation model), and we used SUMO to generate the vehicle movement file that was input to ns2. The map that was used to generate the movement file has a size of 1.5×1.5 km^2 . The wireless bandwidth and the radio transmission range were assumed 6 Mbps and 300 m, respectively. In the Nakagami model, we used an m-value of 3 for distances less than 50 m, 1.5 for distances between 50 and 150 m, and 1 for distances above150 m. The default

number of vehicles was set to 100, and their minimum and maximum speeds were set to 15 and 30 m/s. Each scenario was repeated ten times, and the final results are the average of the ten runs. Five RSUs were evenly deployed across the map to balance their loads as much as possible. Fig. 7 shows the map and locations of RSUs.
Two of the four corner RSUs were wired to the RSU at the center, whereas the other two corner RSUs and the one at the center were simulated to have an Internet connection. Each RSU was simulated to be wired to an SP, linked through an access point to a second one, and connected through the Internet to a third one. Consistent with the literature, the delay for an RSU to access the wired SP was set to 20 ms, and the delay for accessing the wireless SP was set to 50 ms. The delay for an RSU to send a message to another was uniformly distributed over the range [0.05, 0.1] s. Each vehicle generates every 5 s a new request that randomly targets one of the 15 SPs. Hence, the default value of the request rate (R_r) was set to 12 requests per minute. The size of data packets was set to 350 B. This value was chosen to ensure that the size of the encrypted packet will be less than the maximum transmission unit (MTU) of 802.11 MAC (1500 B) after adding the necessary headers, as we noticed from the experiments that we made on AES using theCrypto++package.

IV. Simulation Results

In M-REACT, an RSU prepares the user's data on his behalf. The probability of successful data retrieval through the fixed network is higher than that the through the wireless network. In addition, RSUs cache certain types of data (such as news, advertisements, and web pages). Whenever a user requests a data item that exists in the RSU cache, the RSU sends the item to him without contacting the SP (on the condition that the item has not expired). This fact increases the value of the MSR in REACT. The total delay between the instance at which a vehicle issues a request packet and the instance at which it receives the answer. The total delay reflects the efficiencies gained by assigning keys from within the packets themselves and having RSUs contact SPs on behalf of the users.

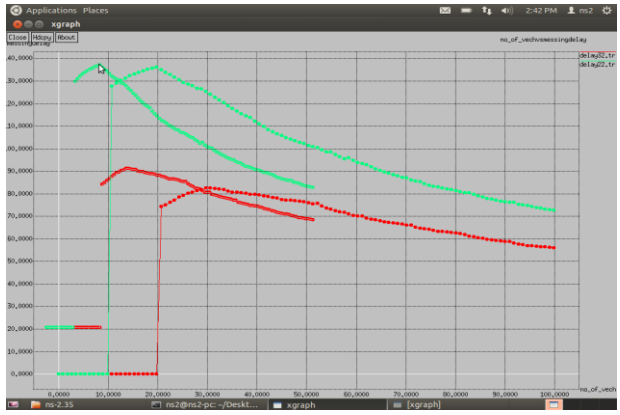

Fig.2. No.of vech.vs Messaging delay

Measuring the Delay and Traffic of the Handover and Master Key Operations: In the last set of scenarios, we test the performance of the following two main operations in REACT:
1) Obtaining the master key and 2) doing a handover. For each operation, we recorded its start and end times to measure it's

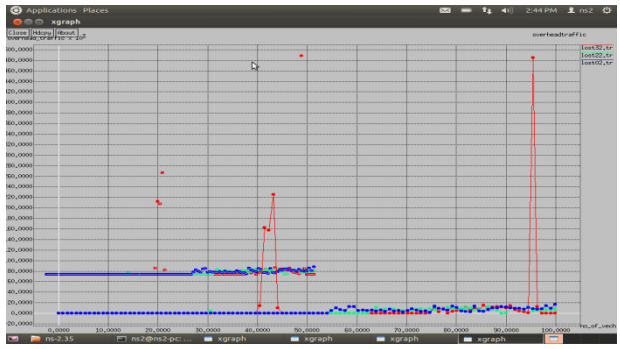

Fig.3. No-of vech.vs overhead traffic

delay. In addition, we recorded the number and type of packets exchanged during the operation to record its total traffic. The
master key operation starts when the vehicle sends the *Initiate* packet and ends when the user decrypts the *Master Key* packet. The handover operation starts when the users decrypts the master key packets.
When REACT produces high overhead traffic, its performance can be improved by decreasing the number of packet keys n used to encrypt a message. In addition, the main operations of REACT (obtaining the master key and handover) produce small delay and traffic

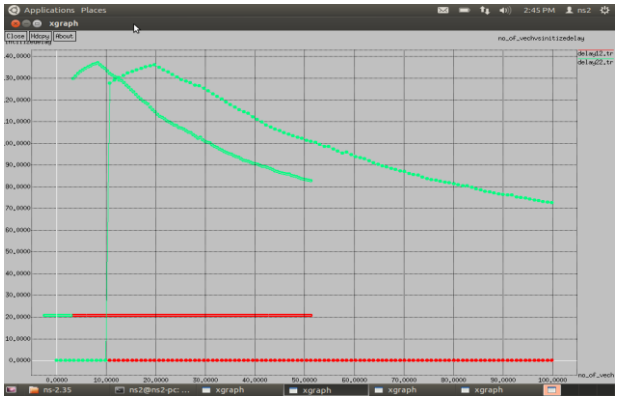

Fig.4.No.of vech.vs Initialized delay

.

V. CONCLUSION

The evaluation of our proposed scheme confirmed its effectiveness compared to a recent security mechanism for VANETs. 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, 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. In proposed privacy-preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption.

REFERENCES

[1] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, "EP2DF: An efficient privacy-preserving data-forwarding scheme for service-oriented vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 580–591, Feb. 2011.

[2] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[3] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc network," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

[4] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communi- cation scheme with authenticated key establishment and privacy preserv- ing for vehicular ad hoc networks," *Comput. Commun.*, vol. 31, no. 12, pp. 2803–2814, Jul. 2008.

[5] K. Mershad, H. Artail, and M. Gerla, "ROAMER: Roadside Units as message routers in VANETs," *Ad Hoc Netw.*, vol. 10, no. 3, pp. 479–496, May 2012.

[6] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. P. Hubaux, "Secure vehicular
communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[7] J. Petit and Z. Mammeri, "Analysis of authentication overhead in vehicu- lar networks," in *Proc. WMNC*, Budapest, Hungary, Oct. 2010, pp. 1–6

. [8] B. Kaliski, "PKCS# 5: Password-Based Cryptography Specification Ver- sion 2," RSA Lab., Cambridge, MA, 2898, Sep. 2000.