An Engineering Enhancement to the Safety and Efficiency of the Service-Oriented Vehicular Ad-Hoc Networks

Ahmed Abbas Jasim Al-Hchaimi

Abstract: ***A Vehicular Ad-Hoc Network or VANET is a form of Mobile Ad-Hoc Network or MANET which provides communication between vehicles and between vehicles and road-side base stations. 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. The security and privacy issues of vehicular ad-hoc networks (VANETs) must be addressed before they are implemented. For this purpose, several academic and industrial proposals have been developed. Given that several of them are intended to co-exist, it is necessary that they consider compatible security models. In this paper, a new methodology and design is issued as a service-oriented vehicular security system that allows VANET users to exploit RSUs in obtaining various types of data. propose the security of data messages exchanged between users and RSUs and the location privacy of VANET users who exchange these messages. In this paper we also propose a novel approach for users to start their connections in the VANET in a secure way. Illustrate a new handover scheme that is particularly suitable for VANETs. We explain a new cryptographic approach that provides much higher security measures compared to existing ones. We suggest two novel mechanisms for data confidentiality and users location privacy in VANETs to ensure the highly security concept is obtained.***

Keywords: VANET, Service oriented vehicular networks, Ad Hoc, road side unit, SOS

1. Introduction

At the present time cars and other private vehicles are used daily by many peoples. The biggest problem regarding the increased use of private transport is the increasing number of fatalities that occur due to accidents on the roads; the expense and related dangers have been recognized as a serious problem being confronted by modern society. vehicular ad hoc network (VANET) provides a wireless communication between moving vehicles, using a dedicated short range communication (DSRC) is essentially IEEE 802.11a amended for low overhead operation to 802.11p; the IEEE then standardizes the whole communication stack by the 1609 family of standards referring to wireless access in vehicular environments (WAVE) [1], Vehicle can communicate with other vehicles directly forming vehicle to vehicle communication(V2V) or communicate with fixed equipment next to the road, referred to as road side unit (RSU) forming vehicle to infrastructure communication (V2I). These types of communications allow vehicles to share different kinds of information, for example, safety information for the purpose of accident prevention, post-accident investigation or traffic jams. Other type of information can be disseminated such as traveler related information which is considered as non-safety information. The intention behind distributing and sharing this information is to provide a safety message to warn drivers about expected hazards in order to decrease the number of accidents and save people's lives, or to provide passengers with pleasant journeys.

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows:

Dedicated Short Range Communication (DSRC It provides a communication range from 300m to 1Km The V2V and V2R communication takes place within thi range. DSRC, uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage[2], The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channel is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE) It is also known as IEEE 802.11p. It supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. I contains the standard of IEEE 1609, This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the signal into various narrow band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels

2. Related work

2.1 Declaration and Explanation

Several researchers studied security challenges related to VANETs. In this section, we conduct a brief study of recent and relevant works. 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 VANETs. If VANET users use the same ID[3], 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, 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, the authors in assume that each vehicle acquires a new set of pseudonyms from the central authority (CA) when their stored pseudonyms are used. Another disadvantage, as depicted 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.

In AMOEBA, 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 vehicles 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 VANETs. 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 (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. 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 (AC) from the hash chain and sends it to the vehicle. The ACs are used as signatures for messages, and RSUs are used for relaying messages between vehicles and CAs. In 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 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.

A vehicle in SPECS uses a different pseudonym in each session to protect its privacy, whereas the real identity is traceable only by the CA. With regard to actual experimentation on VANET security that was done by several projects such as SeVeCom and Safe Spot, we notice that most projects focused on the security of safety beacons or traffic messages. For example, describes the types of applications whose security requirements were considered by SeVeCom. These applications vary from collisions to cruise control, including obstacles and work zone warnings. Hence, the security of data messages from SPs or web servers is not considered. In addition, ITSSv6, focuses on its security aspects on the security and privacy of messages and users only in safety and traffic applications, such applications require tight deadlines for message delivery (less than 100 ms). Furthermore, the data exchanged in these applications are usually not confidential. Hence, all proposed security systems rely on elliptical curve cryptography or ECC, because it produces less delay overhead than other schemes, particularly symmetric ones. However, the secrecy level of the exchanged data is sacrificed, ECC keys should be twice the length of equivalent symmetric key algorithms to provide the same security level. Hence, it is better to use a symmetric scheme to encrypt data messages, because these messages do not have a delay restriction. Rather, a high security level is required, because very sensitive data could be exchanged between users and Internet servers through the RSUs (such as e-mails, money transfers, and criminal records).

In this paper, we argue that the security of users should be accounted for, starting from the initial contact between a user and an RSU. Hence, we describe a web-based secure registration process that allows a user to create an account with RSUs. During the registration, users provide all required information that enables them to have the benefit of secure connectivity starting from the first packet that they send to the RSUs.

We propose a novel cryptographic function that enables users and RSUs to apply the required security level of exchanged messages by adjusting the number of iterations of the function. To defend against privacy hacking and impersonation, we make an RSU specify for each user the next encryption key and the next pseudonym to use. We derive a set of encryption keys that are used to encrypt the next packet from part of the data in the current packet.

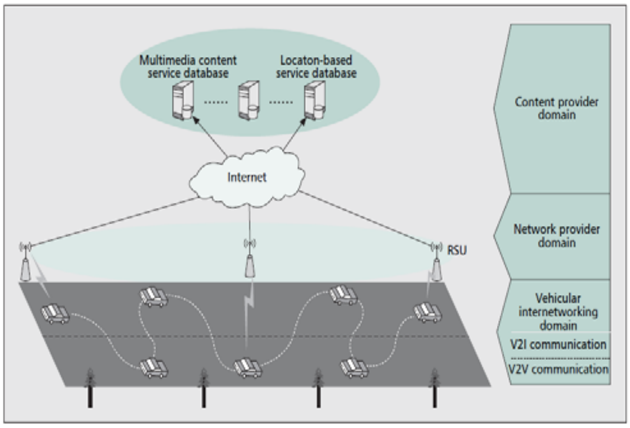
Multimedia content service database
Locaton-based service database
Internet
RSU
Content provider domain
Network provider domain
Vehicular internetworking domain
V2I communication
V2V communication

Figure 1: System architecture of service-oriented vehicular networks

3. Security Requirements For Service-Oriented Vehicular Networks

To successfully deploy service-oriented vehicular networks, a number of security requirements must be satisfied.

a) **Confidentiality:** Confidentiality is necessary to ensure that sensitive information is well protected and not revealed to unauthorized third parties. The confidentiality objective is required in a vehicular network environment to protect information traveling between different network entities including RSUs and forwarding vehicles, since an adversary may try to reveal the service content by eavesdropping. The confidentiality objective can be achieved by using end-to-end encryption, which requires the presence of mutual authentication and key agreement between the service requester and service provider

b) **Authentication:** Similar to conventional systems, authentication techniques verify the identity of the vehicular nodes in communication and distinguish legitimate vehicular users from unauthorized users. In particular, the authentication in service-oriented vehicular networks includes two levels: authentication between vehicles (V2V authentication) to provide link-to-link security, and authentication between the vehicle and RSU as well as the service provider (V2I authentication) to ensure that accounting or billing can be performed correctly [5].

c) **Privacy:** Privacy issues for service provisioning in VANETs regard primarily preserving the anonymity of a vehicle and/or the privacy of its location. Privacy protection tries to prevent adversaries (e.g., another vehicle or an external observer) from linking the vehicle to the driver's name, license plate, speed, position, and traveling routes along with their relationships to compromise the sender's privacy [6].

In summary, security issues in service-oriented (Figure -1) vehicular networks can be categorized into two major classes: security between vehicles, and security between vehicles and service providers or their operated infrastructure. In the following section we discuss possible solutions to achieve
these security objectives.

4. Rotuing Protocol

AODV

The Ad hoc On-Demand Distance Vector protocol. The Ad hoc On-Demand Distance Vector protocol is both an on-demand and a table-driven protocol. The packet size in AODV(Figure -2), is uniform unlike DSR. Unlike DSDV, there is no need for system-wide broadcasts due to local changes. AODV supports multicasting and unicasting within a uniform framework. Each route has a lifetime after which the route expires if it is not used. A route is maintained only when it is used and hence old and expired routes are never used. Unlike DSR, AODV maintains only one route between a source-destination pair.

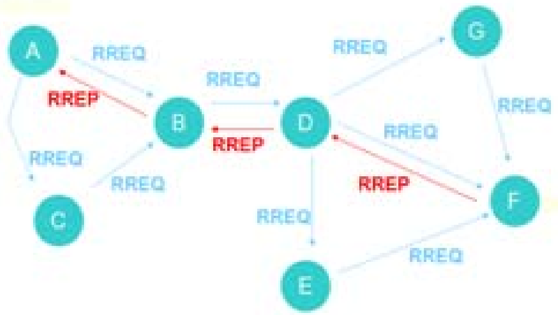

Figure 2: AODV protocol activities

5. RSA (Rivest, Shamir, Adleman)

Public Key Cryptosystem

Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge

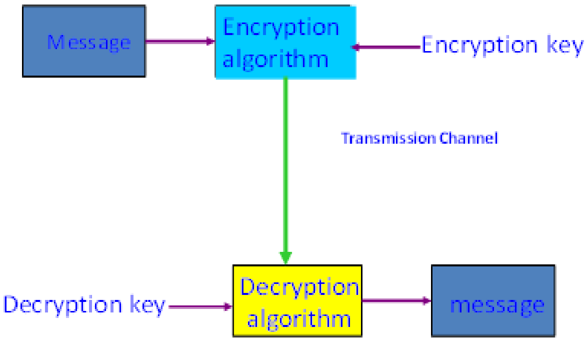

Figure 3: RSA Datagram

5.1Public Key Cryptosystem

A public encryption method that relies on a public encryption algorithm, a public decryption algorithm, and a public encryption key. Using the public key and encryption algorithm, everyone can encrypt a message. The decryption key is known only to authorized parties.

5.2 RSA Key Setup

1) The key generation process, by select any two prime numbers to get the encryption key as :
P=3
Q= 11
N = P * Q = 33
M=(P-1) * (Q-1) = 20

2) Public key:
1 < e < m
1 < e < 20
e=7 …. (Kp)

3) Private Key:

$$d=\frac{1+m(x)}{e} \ldots \text{ where } (x) = 0, 1, 2, 3 , \ldots .$$

$$d=\frac{1+20(0)}{7} = 1/7 \text{ .. is not satisfy the number should be without fractions}$$

$$d=\frac{1+20(1)}{7} = 3$$

$d=3$, and It's the Private key (K_m)

6. Handover

Is the process required to transfer the network connectivity of a mobile node from one infrastructure node to another. In this report the mobile node is usually an On Board Unit (OBU), and the infrastructure nodes are RSUs. Provided that transferring only the physical and medium access control layers is not always enough to keep the communication, in addition to the lower layers it may also be needed to transfer information regarding higher levels of the OSI model, such as context or state information regarding the mobile node.

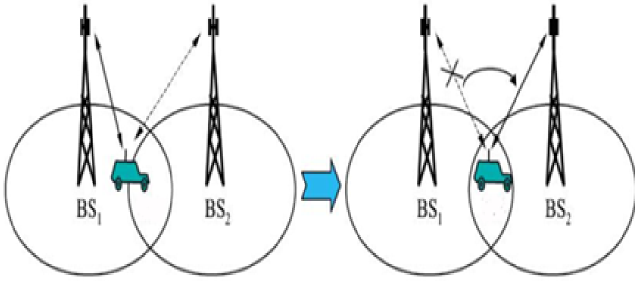

Figure 4: HANDOVER

Contrary to handover in traditional wireless networks (such as cellular networks)[7], where the communication between the mobile user and the access point is always through a single-hop connection, the communication between a vehicle and an RSU could traverse several vehicles (i.e., multihop) (Figure-5. HANDOVER sachem). Hence, the packets exchanged between the vehicle and the RSU during a handover could be sent in a multihop manner. These packets are small in size and, hence, will take much less time to travel compared to data packets.

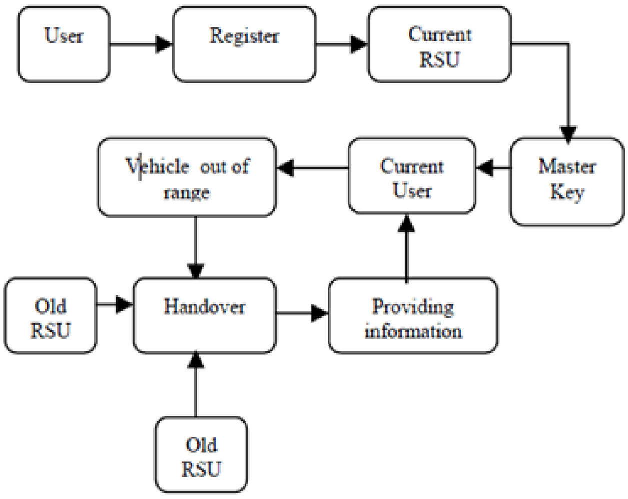

Figure 5: HANDOVER sachem

7. Proposed Architecture

The framework shown by figure 1 explains the proposed system and how communication is done with safe manner by using an authorized communication protocol associated with encrypted algorithm. And to automate this architecture we design a pattern shown by figure 2 to explain what we mean exactly in real word

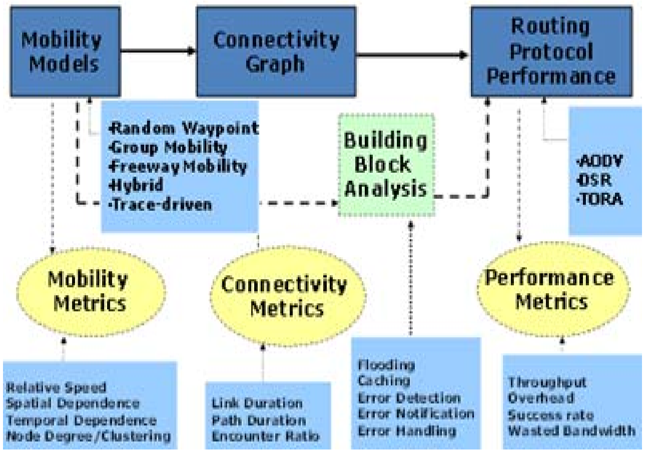

Figure 6:.Proposed system framework

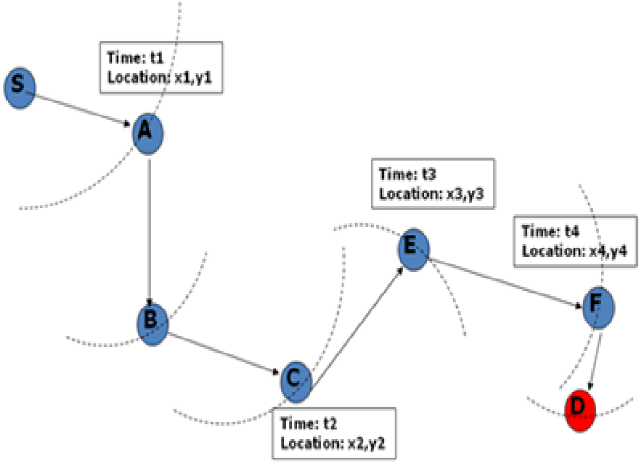

Figure 7: Automation model

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.

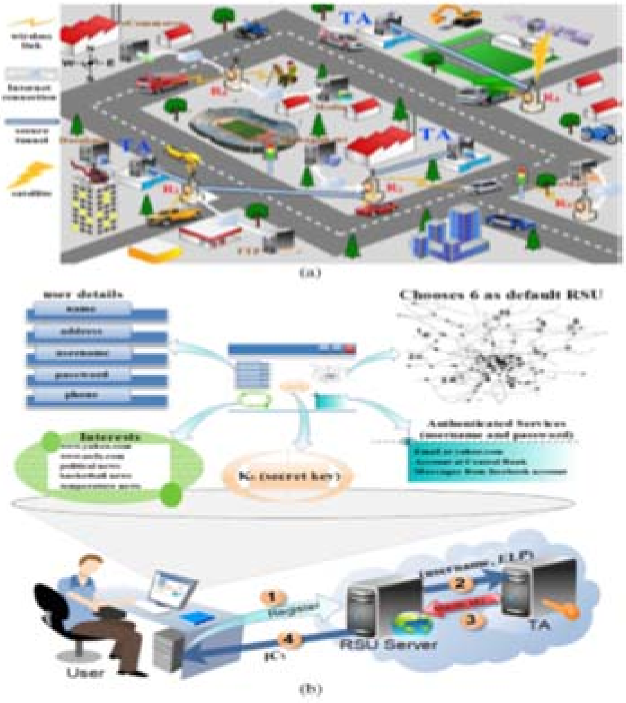

Figure 8:.a) Sample architecture of REACT. (b) Sample online registration

7.1 Registration

When users register using the RSU website, 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.

7.2 Master Key

After the users have registered, their default RSU saves their account and contacts the TA to obtain a master key (Km) for them. The users obtain Km the first time (after registration) 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 (of their account with the RSUs) 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 (IC1), which is an integer kept as a secret between the user and the RSU.

7.3 Participating in a Session

Each time a user connects to an RSU, he/she starts a new session. To preserve users' location privacy, we make an RSU assign to a user a new pseudonym in each packet, A user starts a session by sending a Hello packet that contains his/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/her interests in his/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/her username, password, and Kc. Both packets will be encrypted using Km.

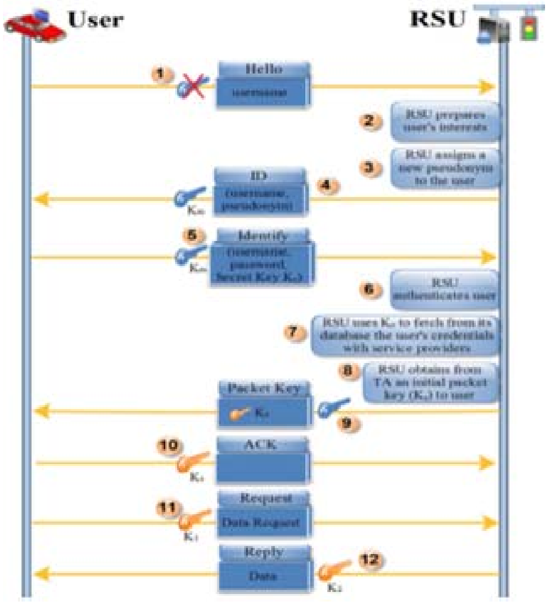
User
RSU
1
Hello
username
2
RSU prepares user's interests
3
RSU assigns a new pseudonym to the user
4
ID
(username, pseudonym)
Km
5
Identify
(username, password, Secret Key Kc)
Km
6
RSU authenticates user
7
RSU uses Kc to fetch from its database the user's credentials with service providers
8
RSU obtains from TA an initial packet key (K1) to user
Packet Key
K1
9
10
ACK
K1
11
Request
Data Request
K1
Reply
Data
12
K2

Figure 9: Sequence diagram for participating in a session.

8. Analysis

To generate keys, we proposed a new key derivation and encryption function. One of the inputs to this function is an initial iteration count (IC1), which is an integer kept as a secret between the user and the RSU. The Little time deference (Figure-10.deffrince between the timing) that occur in the proposed system just because it take the time to generate the key and authorized the user who need to participate in the session

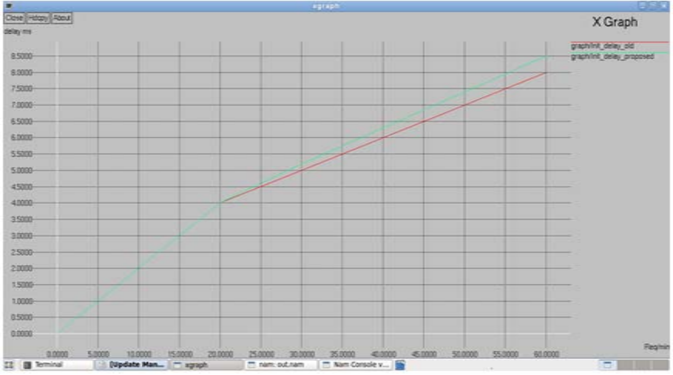

Figure 10: Difference between the timing in the old work and proposed work

9. Conclusion and Future work

Vehicular networks have been envisioned to play an important role in the future wireless communication service market. Service-oriented vehicular networks, which rely on both V2I and V2V communications, can be regarded as a combination of infrastructure-based broadband wireless networks and ad hoc networks. So how we can ensure security and privacy in service-oriented VANETs 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. 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. Using this scheme, the RSU distributes its load among the available TSs.

In this project we have discussed the key security requirements, and pointed out that existing solutions may face the challenges of long V2I authentication delay and public key revocation issues. The proposed V2I fast authentication scheme based on vehicle mobility prediction and an RSU-aided short-time certificate scheme can successfully address the authentication latency and public key certificate revocation issue. Our further research will focus on how to seamlessly integrate security at the V2I and V2V levels to obtain a general security platform for the service-oriented VANETs. We will also investigate the security performance by simulating in more realistic scenarios.

Due to the importance of security for safety transportation, in this paper report, we analyze various studies focusing on security in VANET. We found some of the treats and challenges related to VANET security. Also, we obtain the requirements that are required for creating and designing a security model. These security issues make a potential stumbling block to deploy VANETs. From the analysis in survey, we came to know that there doesn't exist a comprehensive security protocol or framework that covers all security aspects of VANET. Therefore, it is necessary to develop a suitable framework or Scope which mitigates all these security problems; more research is required in this area. Moreover, the impact of trust on security in VANET is other objective in future work.

References

[1] S. Lee et al., "Content Distribution in VANETs Using Network Coding: The Effect of Disk I/O and ProcessingO/H," Proc. SECON '08, 2008.

[2] "Brute-force attack," Wikipedia. [Online]. Available:http://en.wikipedia. org/wiki/Brute-force_attack

[3] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. ICPS, Santorini, Greece, Jul. 2005, pp. 88–97.

[4] M. Raya and J. P. Hubaux, "The security of vehicular ad hoc networks,"in Proc. SASN, Alexandria, VA, Nov. 2005, pp. 11–21.

[5] E. Coronado and S. Cherkaoui, "An AAA Study for Service Provisioning in Vehicular Networks," Proc. IEEE Conf. Local Comp. Net., 2007.

[6] M. Raya and J.-P.Hubaux, "The Security of Vehicular Ad Hoc Networks," Proc. SASN, 2005.

[7] 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.

Author Profile

Ahmed Abbas JasimAl-Hchaimi, presently is a master of technology degree (M.Tech) , in Computer Networks and Information Security, from SIT - Jawaharlal Nehru Technological University Hyderabad-India in 2014, and also he was received his (B.sc) degree in Computer Techniques engineering specialization, from Islamic University College - Najaf, Iraq, in 2011, his research and according to his specialization in network security, made him work on the security management in service-oriented vehicular ad hoc networks and the possible ways to make it trusted and safe for the interesting end users.