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:

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

$$d=\frac{1+20(0)}{7} = 1/7$$ .. 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.

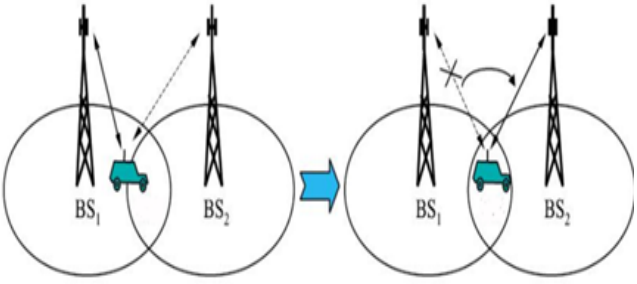

Figure 4: HANDOVER

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.

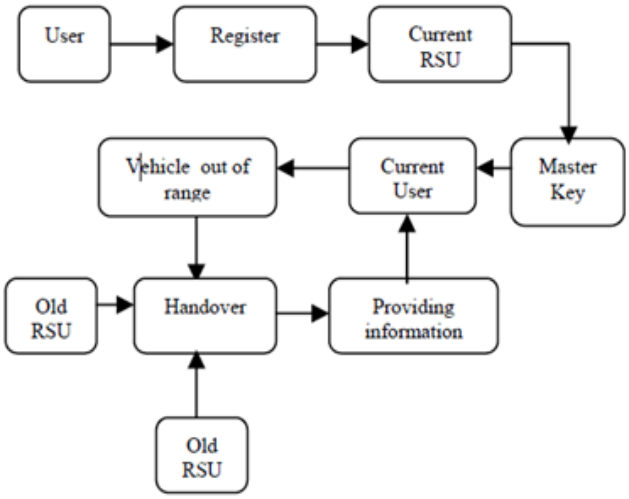

Figure 5: HANDOVER sachem

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

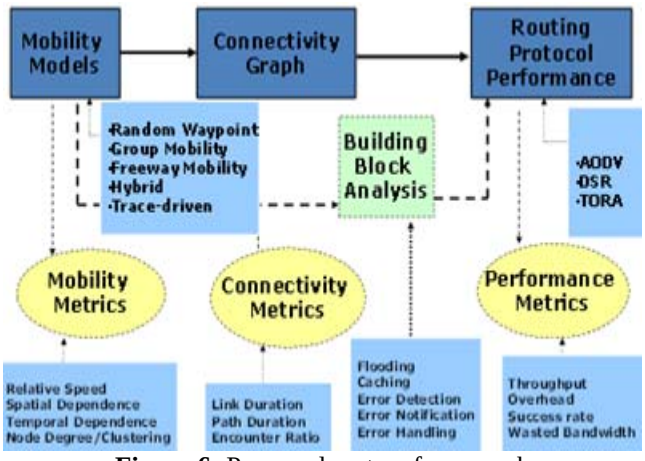

Figure 6:.Proposed system framework

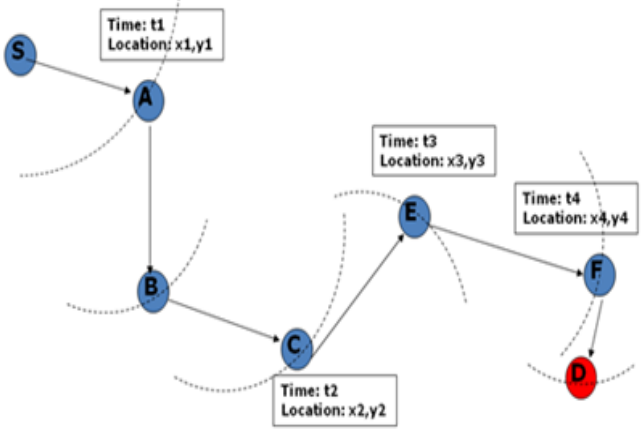

Figure 7: Automation model

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.

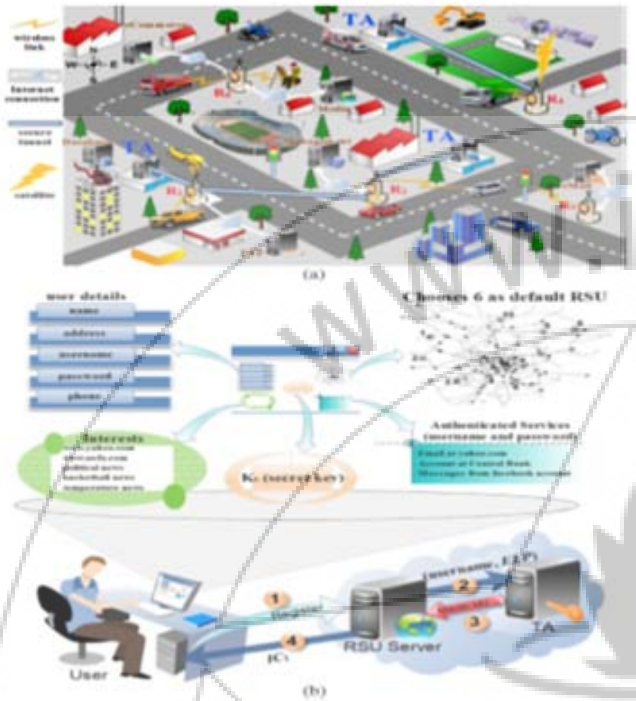

Figure 8:.a) Sample architecture of REACT. (b) Sample online registration

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.

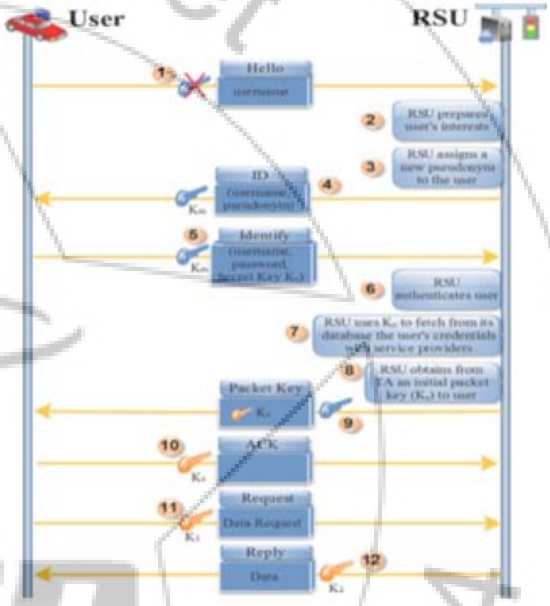

Figure 9: Sequence diagram for participating in a session.

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

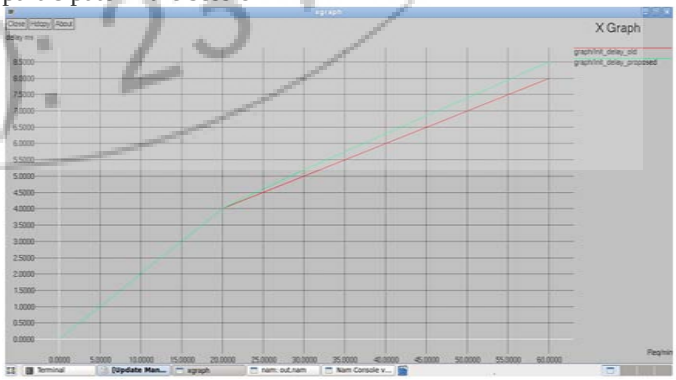

Figure 10: Difference between the timing in the old work and proposed work

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.