Secure and Efficient Data Acquisition in Service Oriented VANET

shah shruti k.

M.E.Scholar
Information technology, PIET, vadodara, India
sshruti50@gmail.com

***Abstract*— service oriented VANET include various services like internet access, video streaming, etc. communication over service oriented VANET publically accessible so there is need to maintain confidentiality and integrity of data over service oriented VANET without affecting the system performance. RELIIM provide the framework for the secure and efficient data acquisition in VANET. RELIM encrypt each and every packet sent over the network using the different packet key and HARDY algorithm for packet key generation. The generation of packet key may affect the system in certain scenarios like heavy traffic. The session key is used in proposed approach with HARDY for encrypting data sent over the network. Thus the key generation time will decrease and increase the system performance.**

***Index Terms*— vehicular ad hoc network(VANET),RSU(road side unit),PBKDF2(password base key derivation function),TA(trusted authority),serice oriented VANET(SOV)**

I. INTRODUCTION

Service oriented VANET is type of VANET [9].VANET is a wireless ad-hoc network where nodes be a vehicles or RSU can communicate or exchange data with each other. Goal of VANET is enhance safety for drivers and reduce traffic conjunctions. VANET is highly dynamic in nature because changing their location with different speed and direction. There are two types of communication V2V (vehicle-to-vehicle) and V2R (vehicle-to-Road side). In VANET there are many security issues [3][13]; one of the most important issues is to improve network throughput and minimize end-to-end delay[9][1] without compromising security and to evaluate this performance Ns3 software is use[14].

II. EXISTING WORK RELATED TO SECURE VANET

Registration

In V2R communication, user pass his personal information on RSU website such as user name, password, address, ELP (electronic license plate), secret key Kc. RSU use Kc to encrypt data and store in its data base, after registration RSU contact TA and it verify that user is registered or not, if he is already registered, it obtain ELP and user name and generate master key Km and IC1 and send to RSU. RSU use HARDY function and derive encryption key using user's password and transmit Km and Ic1 safely to the user, other side user decrypt packet by deriving the same key from his password and store Km and Ic1

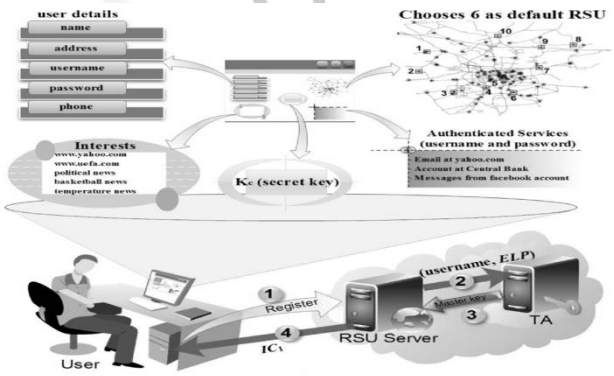

Fig.1 Registration [1]

HARDY Function

HARDY is hierarchical password based key derivation function[1] in this users password pass as a constant string s, Ic1,L=128 bit(symmetric key) and master key pass as MP(plain text message), encryption function E[], number of round n, all are pass as a input. PBKDF2function calculate S,S1,L,Ic1 and generate key=Kn, it is use to encrypt Mp and produce cipher text Mc

and send to the destination. New key is generated from the previous key. HARDY use several iteration to encrypt Mp. It is difficult to crack Mp for attacker because it is very expensive operation, cost around $160*10^{12}$ dollars per year, so it is most secure algorithm.

Hierarchal password-based key derivation function (*HARDY*)

At the source:

Input: constant-size string S, plain text message M_p, initial iteration count IC_1, 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 S1 of size Ss bits.
(3)      calculate K1 = PBKDF2 (S, S1, IC1, L)
(4)      for (i=2; i<n; i++)
(5)          generate ICi (random integer above 1000)
(6)          generate Si (random Salt of size Ss bits)
(7)          calculate Ki = PBKDF2 (Ki-1, Si, ICi, L)
(8)      encrypt Mp using Kn to get mn = E_Kn[Mp]
(9)      for (i=n; i>1; i--)
(10)         calculate mi-1 = E_Ki-1[Si||ICi||mi]
(11)     calculate final cipher message Mc = S1 || m1
(12)     return Mc
(13) end
```

At the destination:

Input: constant-size string S, cipher message M_c, initial iteration count IC_1, decryption function D[], number of algorithm rounds n, size of encryption key: L bits.

Output: plain text message M_p.

```
(1)  begin
(2)      separate Mc to get S1 and m1
(3)      calculate K1 = PBKDF2 (S, S1, IC1, L)
(4)      for (i=1; i<n; i++)
(5)          apply D_Ki[mi] to obtain ICi+1, Si+1, and mi+1
(6)          calculate Ki+1 = PBKDF2 (Ki, Si+1, ICi+1, L)
(7)      apply D_Kn[mn] to obtain Mp
(8)      return Mp
(9)  end
```

Fig.2. HARDY function[1]

Packet Key

After registration user start his session with RSU, they use packet key which is generated from encrypted content of the current packet [1]. RSU obtain packet key from TA and encrypt packet key using master key and store in its table then transmit to the user. User decrypt packet using master key and store in his table as next_key and use it to encrypt next packet which user send to the RSU. If packet lost then user same request using previous key, so RSU come to know packet was lost and resist replay attack. Every time each packet is encrypted by generating new key. As number of key generation ratio increase delay will increase and require more memory for storage

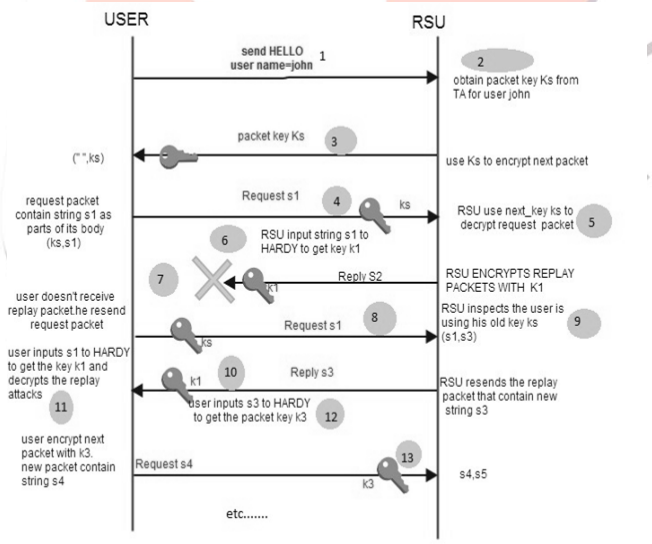

Fig.3 assigning packet key by the RSU [1]

Limitations of previous work[6]

- Increase packet delay
- Required more memory for storage
- Need more processing time

III. PROPOSE SCHEME

The REACT protocol uses different packet key to encrypt different packets [1], each packet will be encrypted will be encrypted with different key. The propose scheme will set one time of the session during which the same key will be used to encrypt/decrypt the packets sent and received [9]. Thus on the both the sides the as session timer expires the new key generated event will take

place. The new session key generated will be from previous packet key only. In the case of the drop of the packet the RSU will get the same request again with the different time stamp on the packet from the same receiver so it can come to know that the previously sent packet was not delivered to the vehicle. In case of the replay attack the receiver of the packet can always check the time stamp of the packet and replay attack will be avoided.

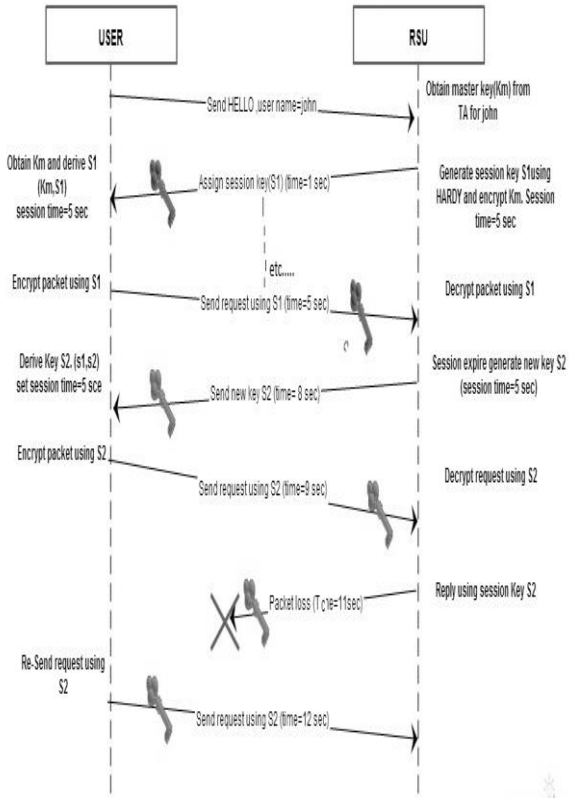

Fig.4. Assigning session key by the RSU and the user

IV. SIMULATIONS

To evaluate performance Ns3 software is used and following parameters are considered for obtaining results.

TABLE 1 Basic Simulation Parameters

Parameters	values
High way length	5000m
Number of vehicles	30-300
Number of RSU	5
Size of packet	256 bit
Size of master key(Km)	128 bit
Size of packet key(Ks)	128 bit
Number of phase of HARDY	2-20
Salt (Ss)	128 bit
Request rate	10-60 (req/min)

Following metrics used for comparing the two system [1]

- Message success ratio (MSR)
- Total delay
- Message response time (MRT)

Message success ratio (MSR): which is the percentages of massages that are successfully received at their destinations.

Total delay:In this record the both the processing and communication delays. The processing delay is the average of all encryption and decryptions during simulation, where as communication delay is the delay of routing packet to its destination. Delay is mostly due to encryption and decryption of the first packet is sent by the RSU to the user at the beginning of each session. Key =128 bit.

Message Response Time which is total time to require to send a request vehicle to RSU and to receive the answer

V. SIMULATION RESULT

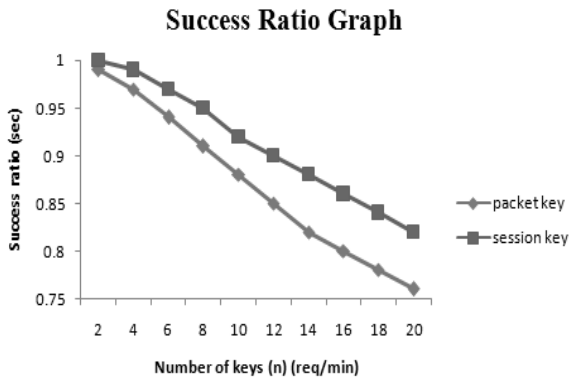

Fig.5. MSR of REACT for different number of keys

Figure 5 shows MSR steadily decrease with the increase of number of keys. For packet keys MSR sharply decrease and reach 72% and for session keys, it is 82%Figure 6 and figure 7 shows that message delay increase with increase of n. These results are due to two reasons first, number of iteration of HARDY increase hence, the size of packet is increase and consequently, the delay increase. This reason corresponds to the increase in the processing delay. Second reason is that, when the size of cipher message increases above the MTU, the message will be dividing in to fragment and each fragment will be sent in a separate packet. Delay will become the maximum delay of all fragments. This reason corresponds to the increase in the communication delay. Delay produced by packet key is 270ms while delay Produced by session key is 247ms. With comparison of packet key session key produce less delay.

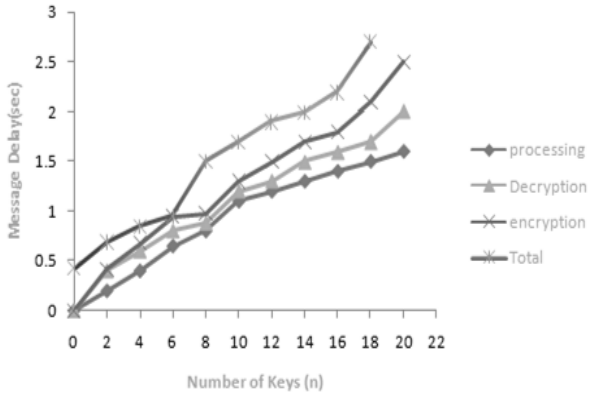

Fig.6. MRT of REACT for encryption and decryption using packet keys

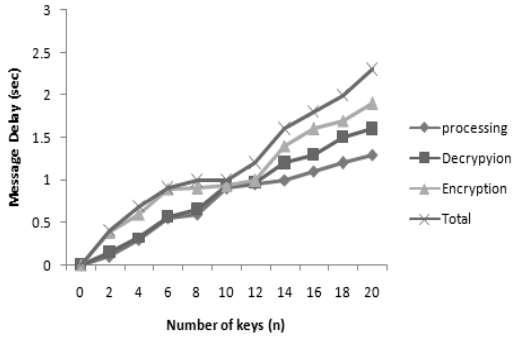

Fig.7. MRT of REACT for encryption decryption using session key

REFERENCES

[1] Khaleel Mershad And Hassan Artail," A Framework For Secure And Efficient Data Acquisition In Vehicular Ad Hoc Networks", Ieee Transactions On Vehicular Technology, Vol. 62, No. 2, February 2013.

[2] Manoj DiwakarAjay Kumar, Dhirender KumarNitin Thapliyal,"VANET (Vehicular Ad-Hoc Networks):Avoidance of Risk Factor in Secure Communication" International Journal of Engineering and Innovative Technology (IJEIT)Volume 3, Issue 1, July 2013

[3] Navdeep Kaur Randhawa," Design and Implementing PGP Algorithm in Vehicular AdhocNetworks (VANETs)", International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun 2012, pp. 647-650

[4] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012

[5] 1Rakesh Kumar, 2 Mayank Dave," A Comparative Study of Various Routing Protocols in VANET ",IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814.

[6] Bharati Mishra1, Saroj Kumar Panigrahy 2,Tarini Charan Tripathy 3, Debasish Jena 4, and Sanjay Kumar Jena 5," A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation", World Congress on Information and Communication Technologies 11 – 14 December 2011, Mumbai, India.

[7] Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen ·Angela Irwin · Aamir Hassan," Vehicular Ad Hoc Networks (Vanets): Status, Results, And Challenges", © Springer Science+Business Media, Llc 2010.

[8] Hadi Arbabi Michele C. Weigle," Highway Mobility And Vehicular Ad-Networks In Ns-3", Proceedings of the 2010 Winter Simulation Conference.

[9] Haojin Zhu, Shanghai Jiao Tong Universityrongxing Lu And Xuemin (Sherman) Shen,"Security In Service-Oriented Vehicular Networks", University Of Ontario Institute Of Technology, University Of Waterloo Xiaodong Lin, 1536-1284/09/$25.00 © 2009 IEEE.

[10] B. Kaliski," PKCS #5: Password-Based Cryptography Specification Version 2.0", RSA Laboratories September 2000.

[11] Maxim Raya And Jean-Pierre Hubaux, "The Security Of Vehicular Ad Hoc Networks", Laboratory for Computer Communications And Applications (LCA) School Of Computer And Communication Sciencesepfl, Switzerland{Maxim.Raya, Jean-Pierre.Hubaux} @Epfl.Ch.

[12] Yi Qian, And Nader Moayeri," Design Secure And Application-Oriented Vanet", National Institute Of Standards And Technology 100 Bureau Drive, Stop 8920 Gaithersburg, Md 20899-8920, Usa.

[13] Klaus Plobl and Hannes Federrath," A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks" University Regensburg, 93040 Regensburg, Germany.

[14] NS2 versus NS3: http://www.nsnam.org

[15] http://vnt.disi.unitn.it/usage.php