An Efficient Secured Data Acquisition and hand over scheme in service oriented VANET

P.Sathya[1], S.Pushpalatha[2]
[1]*PG Scholar, Department of Computer Science and Engineering,*
PSNA college of Engineering and Technology,
Dindigul -624619, India.
[1]p.sathyadgl@gmail.com
[2]*Associate Professor, Department of Computer Science and Engineering,*
PSNA college of Engineering and Technology,
Dindigul -624619, India.
[2]pushpa_pushpa@yahoo.com

***Abstract*— Vehicular ad hoc networking is an important component of Transportation Systems. Vehicular Ad hoc Networks (VANETs) which comprises of vehicles like cars as their mobile communication points used in MANET to produce a mobile network. It enables vehicular communication using Road Side Units (RSU). However, a peculiar case of VANETs endures 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. So we proposed a framework for the secure and efficient data acquisition in VANET. It encrypts 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. The proposed system performance is evaluated using the ns2 software. We are comparing its feasibility and efficiency to another system.**

***Keywords*— Vehicular ad hoc network (VANET), RSU (road side unit), HARDY (Hierarchical password base key derivation function), TA (Trusted authority), service oriented VANET (SOV).**

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks (MANETs). VANET is one of the influencing areas for the improvement of Intelligent Transportation System (ITS) in order to provide safety and comfort to the road users. VANET assists vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation through Vehicle to Vehicle communication e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. For example, weather information, mobile e-commerce, internet access and other multimedia applications.

A VANET turns every participating car into a wireless router or node, allowing cars each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. The major research challenges in the area lies in design of routing protocol, data sharing, security and privacy, network formation, etc.

Higher node mobility, speed and rapid pattern movement are the main characteristics of VANET. The information provided by other vehicles and stationary infrastructure might also be used for driver assistant systems like adaptive cruise control (ACC) or breaking assistants. To achieve this, the vehicles act as sensors and exchange warnings or more generally telematics information (like current speed, location or ESP activity) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motors, Toyota, Nissan, DaimlerChrysler, BMW and Ford promote this term. There are three types of communication in VANETs, namely V2V (Vehicle to Vehicle), V2R (Vehicle to Roadside) and V2I (Vehicle to Infrastructure)

In VANET, 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 VANETs are referred to as service oriented VANET, which are expected to virtually provide all types of data to drivers and passengers. Service-oriented vehicular networks provides infrastructure-based commercial services including Internet access, real-time traffic concerns, video streaming, and content distribution. The success of service delivery in vehicular networks depends on the underlying communication system to enable the user devices to connect to a large number of communicating peers and even to the Internet. This poses many new research challenges, especially in the aspects of security, user privacy, and billing.

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 Work

In the existing system [1], author has proposed the security framework for efficient and secure data acquisition in Service Oriented VANETs. The system talks about the secure the communication between vehicles and RSUs. They have proposed new encryption scheme called HARDY. Proposed scheme uses different set of keys to encrypt each and every packet sent by the vehicle to RSU. The key for the next packet is calculated using the previous key and so on. Thus to ensure the secure communication there is a need to store the each and every key of communication. Thus the memory at RSU must be large enough to store all the keys of all the packets in the

ongoing session with vehicle. There may be numbers of vehicles connected to the RSU and it requires different tables to store all the key of all the vehicles. Disadvantages of the existing system are increase packet delay, Communication cost increase, Need more memory for storage and Increase computation cost. To overcome these disadvantages I have proposed a model that has a new concept of session time for the key where the packets are encrypted and decrypted. When the session time gets over the new key will be generated by the previous key only.

The authors [1] have proposed in the REACT protocol for secure and efficient data acquisition in Service Oriented VANET. They have used asymmetric key cryptography. While user communicates with RSU it uses the different keys for each and every packet sent and/received. They proposed HARDY (hierarchal password-based key derivation) for the key generation. Thus using this algorithm they generate the all the keys on both the sides. Thus it will require computation time at both the side in RSU and vehicle. And to identify the intruders they used the table which stores all the keys generated during the session for all the packets exchanged. This will need more memory at RSU side. Thus this will affect the performance of the system. Here is the scope of the improvement the system. There is no need to encrypt each and every packet with different keys. We can set timestamp for the key being used in the session. On the expiration of the timestamp, new key will be generated on both the side and will be used. The advantage of the proposed work are

- Require less memory to store the key in a table
- Data exchange will be faster.
- Increase efficiency and throughput.

A. Registration

User register with RSU online, user send name, address, password, ELP to RSU for authentication. RSU store this information in data base. TA (trusted authority) and RSU connected through wired link. RSU send user name and ELP to TA for verification, user send "HELLO" packet to RSU, if user already registered with RSU, send password to TA from its database and generate Km (master key) and IC1 (iteration count 1). RSU send Km and IC1 to user. Who save it and use it as an input to the hierarchical password base key derivation (HARDY function). RSU will use HARDY to generate a sequence of encryption keys.

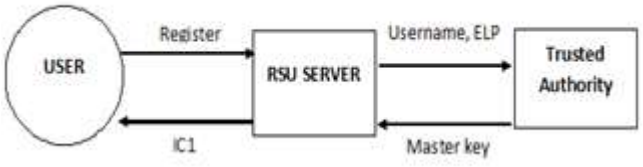

Fig. 1 User Registration

B. 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*1012 dollars per year, so it is most secure algorithm. HARDY algorithm is described below,

At the source:
Input: constant-size string S, plain text message Mp, initial iteration count IC1, encryption function E[], number of algorithm rounds n, size of encryption key: L bits.
Output: cipher message Mc.

```
(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 IC1 (random integer above 1000)
(6)              generate Si (random Salt of size Ss bits)
(7)              calculate Ki= PBKDF2 (Ki-1, Si, IC1, 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 || m1
(12)             return Mc
(13) end
```

At the destination:
Input: constant-size string S, cipher text message Mc, initial iteration count IC1, decryption function D[], number of algorithm rounds n, size of encryption key: L bits.
Output: plain text message Mp.

```
(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  DKi [mi] to obtain ICi+1, Si+1 and mi+1
(6)      calculate KI+1 = PBKDF2 (Ki-1, Si+1, IC1+1, L)
(7)        apply DKn [mn] to obtain Mp
(8)        return Mp
(9)  end
```

C. Packet exchanged between user and RSU

After Registration, user start new session with an RSU, it obtain packet key (Ks) from TA. And send to user by encrypted with his master key (Km). Password based key set

will be used to encrypt a single and resist replay attack, because it is not sent from RSU to user, it is derived from the encrypted content of the current packet. When packet exchange between user and RSU each packet will be encrypted using current_key and decrypted using next_key. Symmetric key (128 bit) is use for encryption and decryption.

D. Proposed Algorithm

In paper [1], authors have proposed a protocol for secure communication between the user and RSU. While user and RSU communicate with each other they use key to encrypt the packets. While in proposed work no need to use different key for all the packets. First the user will send the request to the nearest RSU to use the services. Then the user is authenticated and allowed to use the services. Now afterwards they need to follow the following steps to communicate:

Step 1: Fetch Ks (secret key) of User from TA.
Step 2: RSU generates the Session Packet key Kp.
Step 3: Send the generated key Kp using Ks.
Step 4: User sends acknowledgement using the Ks.
Step 5: Start the timer at the RSU
Step 6: Use the Kp until the timer expire to communication
Step 7: After the time expires, repeat the steps 2 – 6 until the session ends.

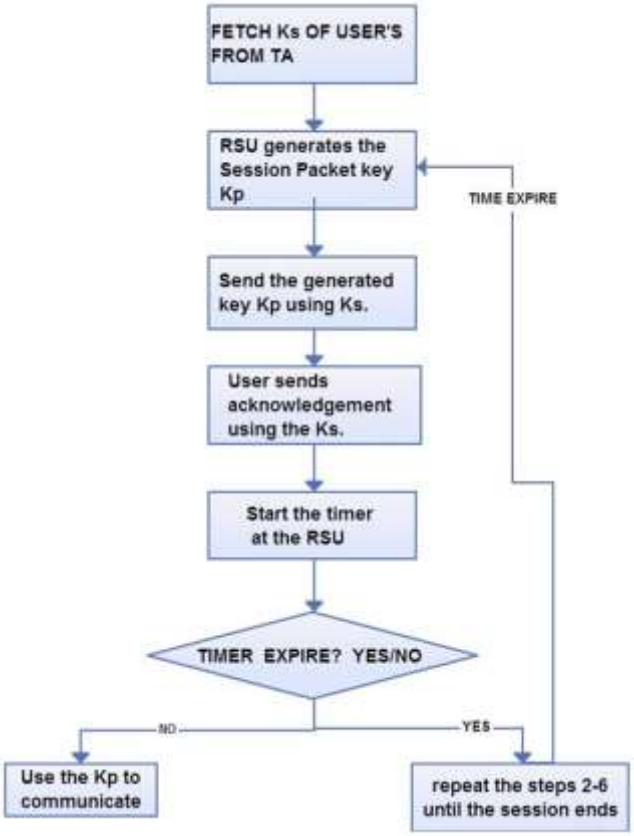

Fig. 2 Flowchart for the proposed work

IV. Simulation Results

Message success ratio (MSR) and Message Response time (MRT) are the metrics used to evaluate the proposed work. These metric will be checked by varying the parameters namely Request Rate, Number of Vehicles and Number of keys.

A. Message Success Ratio (MSR)

MSR is the percentages of massages that are successfully received at their destinations. Fig 3 shows that the MSR of REACT [1]. Whenever user requests a data item that exists in the RSU cache, the RSU generate packet key and send item to him without contacting the SP. This fact increases the value of the MSR in REACT [1]. Simulation time is 120 seconds. Message success ratio for session key is greater than packet key. Timestamp value is set for each key is 10 sec.

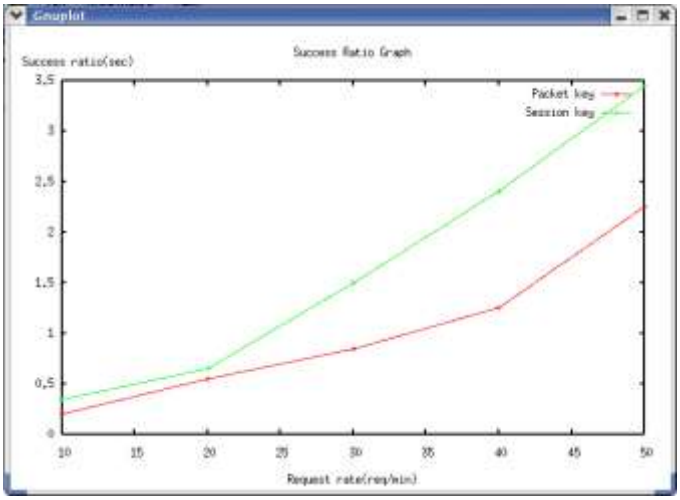

Fig. 3 MSR for different Request Rate

B. Message Response Time (MRT)

MTR is total time required to send a request from vehicle to an RSU and to receive the answer. Fig 4 shows that, In REACT [1], a vehicle sends packets to its nearest RSU, which is responsible for sending the request to the SP. Hence Packets with long routes are avoided in REACT [1]. So that the delay will be decreased because packet will have a higher probability of reaching the RSU. Session key produce less delay compared to packet key.

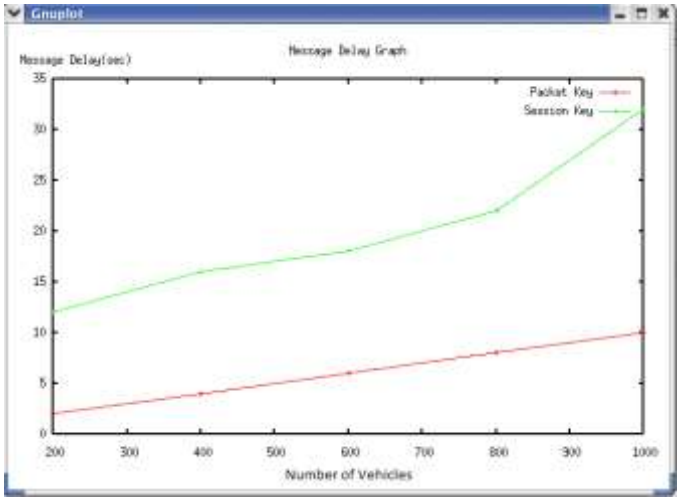

Fig. 4 MRT for different number of vehicles in the network

V. CONCLUSIONS

A service-oriented VANET is proposed to enhance the security and location privacy between the vehicles. Privacy preservation mechanism is used to make the location privacy. Hardy algorithm is used for generating key for each and every user who had registered in RSU. The effectiveness and deliver ratio are compared with the proposed system. In the Existing system, when the user communicates with RSU it uses the different keys for each and every packet sent and/received. Using HARDY algorithm all the keys are generated on both the sides. Thus it will require computation time at both the side in RSU and vehicle and also more memory will need at RSU side. So in the proposed work, timestamp for the key is introduced. There is no need to encrypt each and every packet with different keys. A timestamp for the key is used during the packet transmission. On the expiration of the timestamp, new key will be generated on both the side and will be used. By comparing the existing system, the proposed system will increase the performance of the system.

ACKNOWLEDGMENT

I would like to thank our respective head of the department Prof. Dr.D.Santhi, M.E, Ph.D and our respective guide Mrs. D. Pushpalatha, M.E, Associate professor and all who help us to complete the project successfully.

REFERENCES

[1] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" IEEE Trans. Veh. Technol., vol. 60, no. 2, pp. 580–591, Feb. 2013.
[2] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks," in Proc. 31st ICDCSW, Minneapolis, MN, Jun. 2011, pp. 323–331.
[3] T. W. Chim, S. M. Yiu, L. Hui, and V. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Netw., vol. 9, no. 2, pp. 189–203, Mar. 2011.
[4] 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.
[5] 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 networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.
[6] E. Coronado and S. Cherkaoui, "Service discovery and service access in wireless vehicular networks," in Proc. IEEE GLOBECOM Workshops, 2008, pp. 1–6.
[7] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Comput. Commun., vol. 31, no. 12, pp. 2803–2814, Jul. 2008.
[8] B. Mohandas, A. Nayak, K. Naik, and N. Goel, "ABSRP—A service discovery approach for vehicular ad hoc networks," in Proc. IEEE 3rd APSCC, Yilan, Taiwan, Dec. 2008, pp. 1590–1594.
[9] ITSSv6 Project. [Online]. Available: http://www.lara.prd.fr/projects/itssv6
[10] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short time certificate updating in VANETs," in Proc. IEEE ICC, Cape Town, South Africa, May 2010, pp. 1–5.
[11] http://www.isi.edu/nsnam/ns/ns-tutorial/index.html
[12] Tutorial – Marc Greis's tutorial

