ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

An Efficient Data Acquisition and Delivery in Service Oriented Vehicular Adhoc Networks

S.Nidhyalakshmi, Mrs.R.Sabarimala

ME Compurter Networks, GKM College of Engineering and Technology, Chennai, India

Dept. of Computer Science and Engineering, GKM College of Engineering and Technology, Chennai, India

***Abstract*—**Vehicular mesh networks aim at enhancing security and provide various types of services to the VANET users. Service oriented VANETs are type of Vehicular ad hoc networks that support various services including traffic data management, access to multimedia files, email and news. Various types of attacks have emerged that threaten the security of service oriented vehicular ad hoc networks. Security and privacy in service oriented VANETs depends on the ability to defend against various types of attacks that exist in VANET. This paper deals with the design of secure roadside infrastructure that is connected to the internet and provide various types of information to VANET users. The performance of the proposed system is evaluated using network simulator and efficiency is obtained by comparing the result with another systems.

Index Terms—Roadside infrastructure or roadside units (RSUs), security, service-oriented vehicular ad hoc networks (VANETs)

1.INTRODUCTION

The development and wide utilization of wireless communication have lead to the conceptualization of intelligent communicating machines. Vehicular ad hoc network (VANET) is recognized as an important component of Intelligent Transportation Systems. VANETs are considered as an off-shoot of Mobile Ad hoc Networks (MANETs), however they have some distinguishing characteristics. In VANET vehicles are node that are dynamic and because of their high mobility and speed the network topology changes fast.On the contrary, in VANET vehicles move only on predetermined roads, and they do not have the problem of resources limitation in terms of data storage and power.VANETs are used in commercial applications, and improves traffic level safety on roads. Real time communication among vehicles and roadside units can help the driver to have full information on road conditions and this will enhance traffic safety and efficiency.

In VANET, each vehicle is equipped with the communication devices, global positioning system and digital map that allows the drivers to communicate with each other as well as with roadside infrastructure to enhance easier and safety transportation. Each vehicle contains On-Board Units (OBUs), to communicate with each other vehicles (V2V) as well as with RSUs (V2I). VANET is a high capacity mesh network that connects the vehicles and RSUs, and the RSUs can be connected to a backbone mesh network, so that vehicles provide many other network applications and services, including Internet access to the VANET users.

2 .OBJECTIVE

The previous work of service oriented VANET have done with various aspects such as user privacy or data confidentiality, location privacy. None of the previous work proved to provide security of data and location privacy of users in service-orientedVANETs while ensuring efficient throughput and acceptable end-to-end latency. This paper deals with the study of secure data exchange between users and RSU and location privacy of users who exchange the data messages.

Main contributions of the paper- 1) A Novel approach for users to start their connection in the VANET in a secure way. The security of the users is required to exchange sensitive data between the users and RSU. 2) A symmetric encryption scheme such as advanced encryption standard is proposed along with hierarchical based encryption function to strengthen the security of the message to a high extent.We call our

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

secure and efficient data acquisition and delivery system in VANET (REACT).

3.PROPOSED FRAMEWORK

A. Registration and Session Management

The security of users are accounted starting from the initial contact between the user and the RSU. In VANET vehicles are occupied by several users, where each user is considered as a distinct member of their own interest. Hence a secure web-based registration process is needed to create a unique account with the RSU before the user start communication. User registration enable users and RSUs to exchange credentials and keys which helps to start their connection in the VANET in a secure way.

1) Registration: During user registration the user specifies the personal details plus username, password for authentication when the user connects to the nearest RSU from the vehicle. User also choose a default RSU in which the user accounts are store in its database. When user connect in VANET and send a Hello packet to the nearest RSU, the default RSU is notified to the user. The default RSU retrieves the interest from the database and collects the required data from the user.

2) Transferring Master Key: After user registration, the user accounts are stored in default RSU database. When the user connects to the vehicle for the first time RSU contacts the Trusted Authority (TA) and obtains the master key (Km). To achieve this, we propose a technique known as hierarchal password-based key derivation (*HARDY*) function which is used to securely transfer the master key to the user. HARDY function derives a group of encryption keys from the user password

3) Participating in a Session: To preserve users' location privacy, RSU assign to a user a new pseudonym in each packet when user connects to RSU each time for starting a new session. To start a new session the User send a Hello packet containing the username to the nearest RSU. Each packet includes the timestamp used to resist against replay attacks. Once the RSU receives the Hello packet from the user, it prepares the user interest that do not require authentication. . Although the RSU prepares users' data, it assigns them a pseudonym and sends it to them in an *ID* packet. The packets are encrypted using Km.

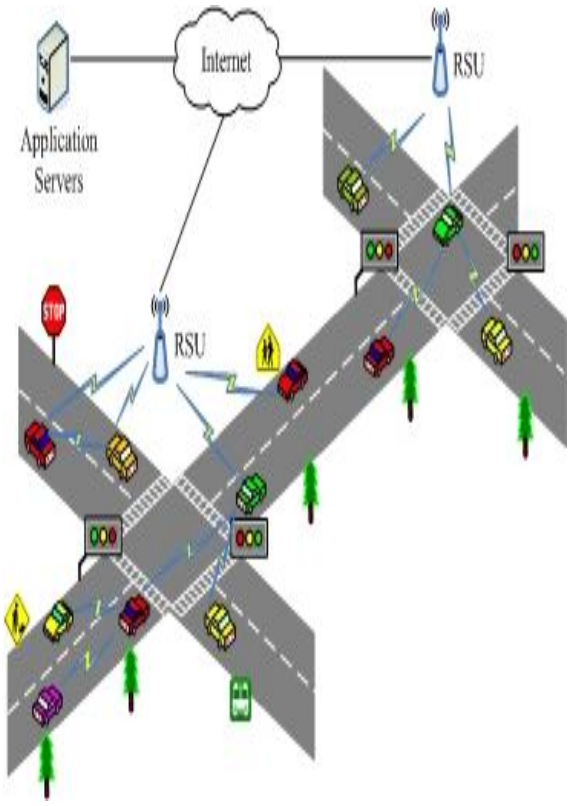

Figure 1: Sample REACT architecture

4) Switching Connection Between RSUs (Handover):

Handover scheme is particularly suitable for VANET. When a vehicle wants to switch over from current RSU to nearest RSU. Vehicle is notified about its current location and calculates the distance from all its nearby RSU using digital map. Vehicle switches over from current location to a new location when it finds it is closer to the nearest RSU. Handover in VANETs is similar to that of handover in wireless networks, where in cellular network the communication between the mobile node and the access point is in single hop manner. In VANET the communication between the vehicle and the RSU could traverse in multihop manner. The handover in REACT is performed using efficient routing protocol which is specifically

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 3, Special Issue 3, April 2014

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

designed to route packets by combining store-and-forward and location-based-routing techniques.

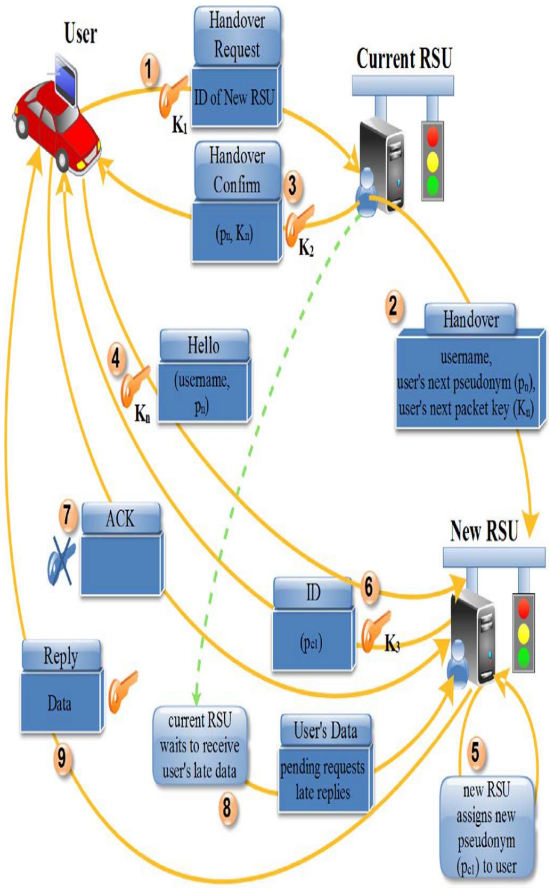

Fig. 2. Sequence diagram for switching connection between RSUs.

C. Security and Privacy

1) HARDY Function: To provide data confidentiality, encryption is used to allow only the genuine user to read and process the transmitted data. In REACT, we propose HARDY that uses the password based key derivation (PBKDF2) function in several iterations to strengthen the security of the encrypted message. The hardness of cracking the final message is much increased at the expense of slight overhead in executing the algorithm. After user registration the user password is sent to RSU for authentication, the user can not send the password in plain text to the RSU instead a set of encryption keys is generated for user password using PBKDF. HARDY function uses plain text as input and generates cipher text with several iterations to preserve message secrecy. The user can only decrypt the message when he/she knows the password and initial iteration count. Themessage security is coupled with the user password and the initial iteration count.

2) Ensuring Location Privacy:

In REACT, the problem of pseudonym refill and unknown adversary are overcome by using pseudonym. RSU assigns the pseudonym to the user when it sends the 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.

3) Packet-Based Keys: REACT uses concept of packet-based keys, where each set of keys is used to encrypt a single packet. The packet-based key is derived from the encrypted content of the current packet rather sending the key from the RSU to the user. There are two main reasons for use of packet-based keys: a) Using a single key throughout the session would enable eavesdropper to relate the key with the source. b) Periodic renewal of keys enable eavesdropper to capture the packet and apply brute-force attack to revoke the keys.

4. COMPARE PROTOCOL

Existing system: ABAKA Protocol

ABAKA protocol is used as authentication and key agreement scheme for VANETs. It uses elliptical curve cryptography (ECC) at the RSUs to authenticate requests from multiple vehicles at the same time. 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. In ABAKA, when a vehicle communicates with another vehicle a single master key throughout the session. Hence use of single key throughout the session would

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

enable the adversary to easily identify the source and capture the message.

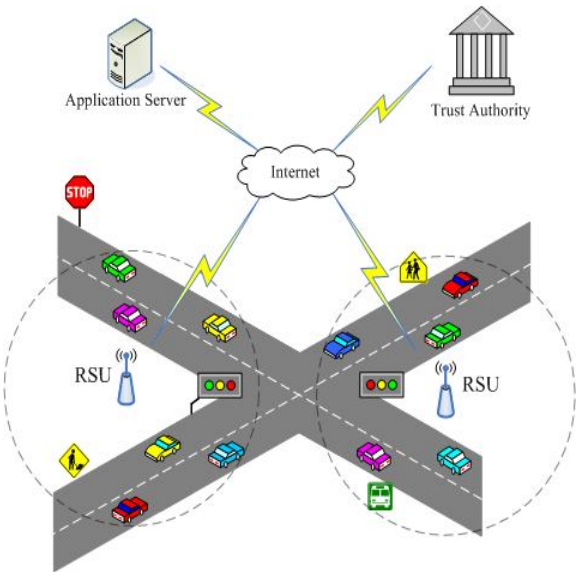

Fig.3 ABAKA Architecture

Proposed system: REACT Protocol

The drawback of ABAKA protocol are overcome by the use of session key that are used for establishing the session.In REACT, when a vehicle communicates with another vehicle session keys are used only for current session and expires at the end of each session. Timeslots are used to resist against replay attacks. REACT does not require TA to generate session key for each requested services, instead RSU perform all operation on behalf of user. ABAKA experiences high overhead traffic due to its dependence on broadcasting operations (because "Hello," "Request," and "Reply" packets are broadcast in ABAKA), whereas REACT avoids broadcasting by using pseudonyms and unicasting.

5. Simulation Results

Simulation results are obtained comparing REACT and enhancement of REACT system. We call enhancement of REACT as mREACT. mREACT overcomes the drawback of reconnection and session expiration caused in REACT.

The metrics used for comparing the two systems are given asfollows:

a) Message success ratio (MSR), which is the percentage of messages that are successfully received at their destinations.

b) Initialization phase time (IPT), which is the system security initialization time, i.e., the average time between the instance a vehicle starts a session to the instance it sends the first packet encrypted with a session key.

c) Average overhead traffic (AOT), which is the extra traffic sent or
received by a vehicle.

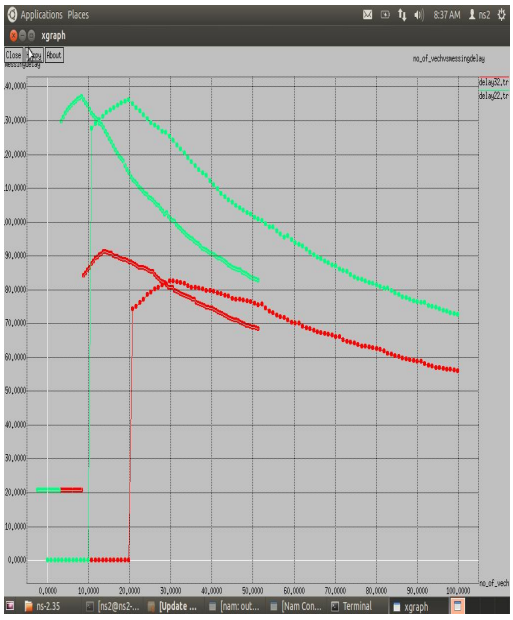

Fig. 4 Messaging Delay

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

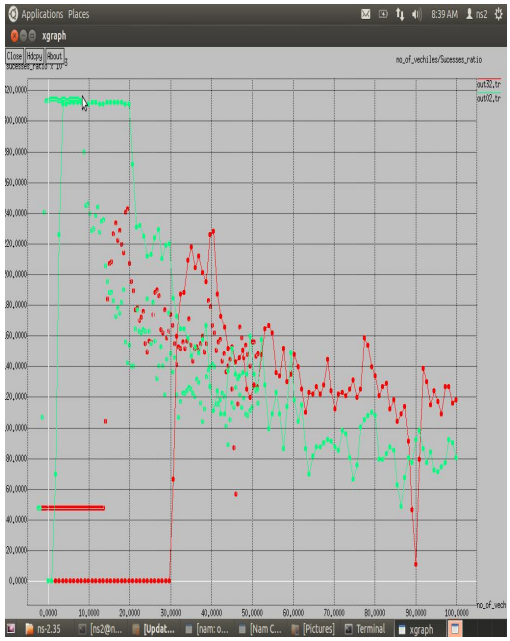

Fig.5 Message Success Ratio

Fig.6 Initialization Phase Time

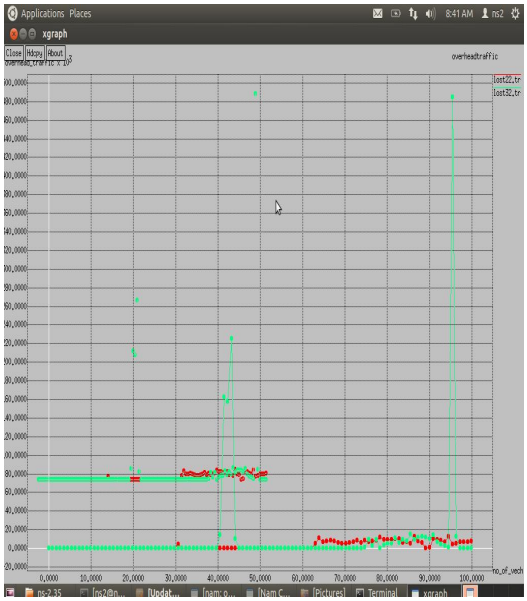

Fig .7 Average Overhead Traffic

From the simulation results mREACT system yield less messaging delay, high success ratio and initialization phase time, and less average overhead traffic when compared to REACT. mREACT provide better results than REACT.

6.CONCLUSION AND FUTURE ENHANCEMENT

The paper address the issues involved in ensuring secure and privacy in service-oriented vehicular adhoc networks. The proposed system deals with novel cryptographic key generation and encryption algorithm. Drawbacks of user privacy and data confidentiality is overcome by use of packet-based keys or short-lived keys. Further Challenges exist due to use of timestamp during session management, henceforth the delay caused in REACT is slightly higher than ABAKA. The ongoing work on REACT focuses on implementing a scheduler to expand the session and reduce the time delay. REACT focus on vehicle-to-vehicle or vehicle-to-infrastructure communication, work on group communication in service-oriented VANETs are implemented in future work.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

REFERENCES

[1] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Proc. ESAS*, Cambridge, U.K., pp. 129–141,Jul. 2007,.

[2] 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.

[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] 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.

[5] G. Calandriello, P. Papadimitratos, A. Lioy, and J. P. Hubaux, "Efficient and robust pseudonymous authentication in VANET," in *Proc. ACM Mobicom*, Montreal, QC, Canada, Sep. 2007, pp. 19–28.

[6] Mohamed Salah Bouassida, "Authentication vs. Privacy within Vehicular AdHoc Networks", *International Journal of Network Security, Vol.13, No.3, PP.121-134, Nov. 2011.*

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

[8] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (2007) 39–68 39.

[9] Vivek Katiyar ,Prashant Kumar ,Narottam Chand ,"An Intelligent Transportation Systems Architecture using Wireless Sensor Networks", *nternational Journal of Computer Applications (0975 – 8887) Volume 14– No.2, January 2011.*