International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.1, January 2015 DOI:10.15693/ijaist/2015.v4i2.237-241

An Efficient High Secure Data Acquisition Mechanism In Vehicular Adhoc Network

S.Mahalakshmi
P.G scholor
P.S.R.R College of Engineering For Women,Sivakasi(TN),India

Mrs.N.Thenmoezhi
Assistant professor
P.S.R.R College of Engineering For Women,Sivakasi(TN),India

Dr.K.Ramasamy
Principal
P.S.R.R College of Engineering For Women,Sivakasi(TN),India.

Abstract—**Vehicular ad hoc networks (VANETs) enable vehicles to Communicate with each other and with Roadside Units (RSUs). Vehicular mesh networks aim at enhancing security and providevarious types of services to the VANET users. Service orientedVANETs are type of Vehicular ad hoc networks that support various services including traffic data details, transferring multimedia files, access email and news. The success of data acquisition and delivery systems depends on the different types of securityand privacy attacks in service-oriented VANETs. All the vehicles and RSUs are connected through mesh network. RSUs are connected to Internet to download maps, traffic data etc. Service-oriented VANET provides security of data and location privacy of users. Cryptographic approach is used toprovide unique key for all the users connected to RSU and evaluate its performance using the ns2 simulator.**

Keywords- Privacy; Security, VANET, Road Side Unit (RSU), RSAAlgorithm.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) enable vehicles to communicate by using wireless ad- hoc networks and exchange traffic information to significantly improve road safety. In VANET vehicles are nodes that are dynamic and because of their high mobility and speed the network topology changesfast.VANETs are used in commercial applications, and improve traffic level safety on roads. Real timecommunication 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 allow the drivers to communicate with each other as well as withroadside infrastructure to enhance easier and safety transportation. Each vehicle containOn-Board Unit (OBUs), tocommunicate with each othervehicles (V2V)as well as with RSUs (V2I).VANET is a high capacity mesh

Network that connect the vehicle and RSUs, and the RSUs can be connected to a mesh network, so that vehicles provide many other network applications and services, including Internet access to the VANET users.

II. RELATED WORK

Existing systems used some techniques in order to increase the security between vehicles to reduce the accident in transportation system. Some problems occur in each technique. Hence to reduce this problems Road Side Unit is used, which increases security in transportation system. Road Side Unit connects to the internet and provides the security information to the user and hence accidents can beprevented. The authenticated user can only access to get the information.

A. Mix Zone and Silent Period

A mix zone is an area in which several vehicles change their pseudonyms together so that an attacker will not be able to distinguish the new pseudonym of each vehicle [2]. The Silent Period approach enables amobile user changing his pseudonym jointly with other approaching users through entering a silent period simultaneously, in which all nearby users suppress their location updates and wield new pseudonyms [3].A major disadvantage in the mix zone approach is the process of pseudonyms refill and user might not always find other near users that are willing to enter a mix zone.

B. Group Signature (DCS)

For the group signature technique, group member can sign messages on behalf of the group without revealing its real identity[5] Signatures can be verified using the group public key, it providing good Privacy for the users, as the identities of the users are revealed in neither signing nor verifying a message. The delay incurred in this technique to verify a signature is linearly proportional to the number of revoked vehicles. Therefore, this technique may not achieve good performance in a large scale network such as VANETs, where the number of revoked vehicles may be large.

C. Pseudonyms

Pseudonym schemes do not support the secure functionality of authentication, integrity, and non-repudiation, an anonymous signing protocol [4] is proposed to provide such functions as privacy. In the protocol, each vehicle preloads a large number of certificated anonymous public and private key pairs. Key pair is used for a short period of time and then be discarded. Each key pair is assigned to one user, and authorities maintain the distribution of key records which can be used to trace the possible malicious vehicles. The shortcoming of this protocol is that it requires vehicles to store a large number of pseudonyms and certifications, where a revocation scheme for abrogating malicious vehicles is difficult to implement in pseudonyms scheme.

D. Ad hoc anonymity

Road Authority (RA) is responsible for the road network. RA uses RSUs to communicate with the vehicle. Some users generate false (dummy) address to prevent their location [4]. The false address and original location sends to the service provider. Because the original location cannot be found by service provider. If attackers intercept to find the location they cannot easily find the true location. In this scheme the communication cost is reduced. But still the dummy location is so far to the user of the vehicle.

III PROPOSED FRAMEWORK

1. Objective

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 RSA based encryption function to strengthen the security of the message to a high extent. We call our secure and efficient data acquisition and delivery system in VANET (REACT)

2. System and Security Models

The system provides security while ensuring high success ratio and low latency .we call our system is secuRe and EfficientdAtaaCquisiTion in VANETs (REACT). This system produces internet facilities to the users who are connected to Road Side unit (RSU). To provide confidentiality the cryptographic algorithm is used which provides unique private key for all users who are registered in RSU. The algorithm used in serviceoriented VANET is RSA(Rivest–Shamir-Adleman).In REACT, a user registers once with the RSUs online (via the Internet) before he starts connecting to the RSUs from his vehicle. After registration, the RSUs obtain from a trusted authority (TA) a master key (Km) for the user. The user gets his Km the first time he connects to an RSU from his vehicle and describes a novel algorithm that uses the user’s password from his account to securely transfer his Km to him. Km will be used to encrypt the initial packet-key which is assigned to the user at the beginning of each session. After that, each packet will be encrypted by a set of derived keys.

A. Registration

RSU is placed at each corner of the road. When the user of the vehicle needs to connect to RSU, first user must register to RSU When a user registers using the RSU website; he specifies his personal details (i.e., name, address, phone, etc…) plus a username and password to use for authentication when he connects to the RSU network from his vehicle. The user also chooses a default RSU, which will save his account in its database.

B. Providing master key to the user

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 (RSA) function which is used to securely transfer the master key to the user. RSA functionderives an encryption keys from the user password.

C. *Participating in session*

Before starting the session, the user sends the hello packet containing the username to the nearest RSU.Timestamp is used to reduce the attack in each packet. The master key to verify whether the user is authenticated matches then the RSU sends the needed information to the user. Once the RSU receives the Hello packet from the user, it prepare the user that do not require authentication. If the username and password matches then the RSU sends the information to the user.

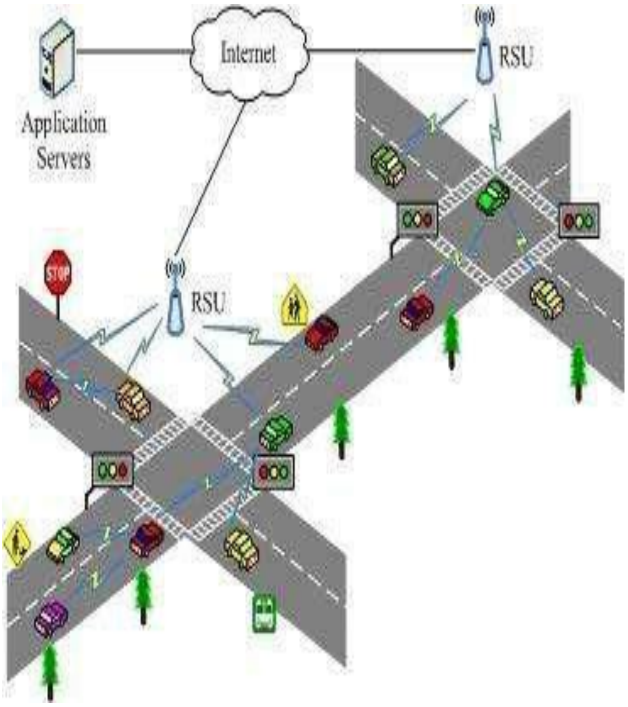


Figure 1. Sample REACT Architecture

D.*Switching Connection between RSUs (Handover)*

When a vehicle wants to switch over from current RSUto nearest RSU, the vehicle observes its current location and calculates the distance from all nearby RSUs using digital map. Vehicle switches over from current location to a new location when it finds it is closer to the nearest RSU. The old RSU sends thehandover packet to the new RSU with the username, master key, and pseudonym. After receiving the particular request the new RSU sends back the handover confirm message to the user connected to the new RSU. This process is called handover scheme. The new RSU verifies all the details of the user to check whether there is any illegal information. The packets send between vehicle and RSU is done through the multi-hop connection. This packet is smaller in size hence it can be sent easily in a small duration of time. The handover scheme done in REACT is reduce to 20m/s compared to ABAKA. The protocol used for transmitting the information from user to RSU and from RSU to user is ROAMER. For each and every request a pseudonym is assigned to enhance the location privacy. For each user a pseudonym is created by RSU, when a request is sent from the user thereply from the RSU sent along with that pseudonym is added and sent to user. Then the user uses that duplicate ID and sends for another request. Then again RSU sends reply with another duplicate ID. This process continues until there is a connection between RSU and user. If the user uses the old ID then RSU sends the alert message to the user, then the user reassigns the ID and back the previous request to RSU. Then the correct transformation occurs without any error or attacks.

3. Security and Privacy

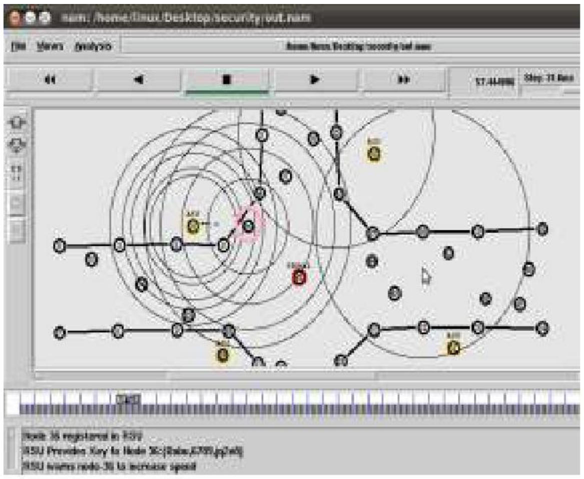
RSA(Rivest–Shamir-Adleman)

In order to provide data confidentiality, encryption is used to allow the user to read and process the data. Cryptographic mechanism are either symmetric or asymmetric, where symmetric schemes use a single key for both encryption and decryption, while asymmetric schemes use a public key for encryption and a private key for decryption. In RSA asymmetric encryption is used. Using RSA algorithm the master key (Km) is encrypted and decrypted using the user Password. In Public Key Cryptosystem Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriateknowledge.

IV SIMULATED RESULTS

A. Handover Mechanism.

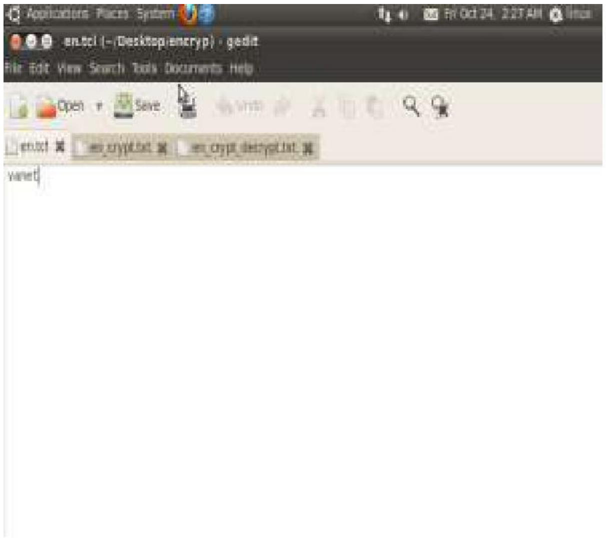
Simulation results are obtained using REACT system. In handover mechanism, if any RSU is closer than the current RSU then the vehicle switches to new RSU.This is done by sending the handover request to old RSU, the old RSU sends the handover packet to new RSU with the username, master key, Password.



```
Node 36 registered in RSU
RSU Provides Key to Node 36:(Eaba,6789,jp2w6)
RSU warns node-36 to increase speed
```

Figure 2. Switching Connection Between RSU

B.*Encrypt and Decrypt the Master key using RSA Algorithm*


Applications Places System
Fri Oct 24, 2:27 AM linux
en.tcl (~/Desktop/encryp) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
en.tcl
en_crypt.txt
en_crypt_decrypt.txt

```
vanet
```

Figure 3. Encrypt the master key

The master key is securly transferred from old RSU to new RSU using RSA algorithm.

C. *Performance Evaluation*

1.*Packet Delivery Ratio*

PDR is the ratio of amount of packets that can de deliver from the sender to receiver. PDR is nothing but the ratio of the number of delivered data packet to the destination. The greater value of packet delivery ratio means the better performance of the protocol.

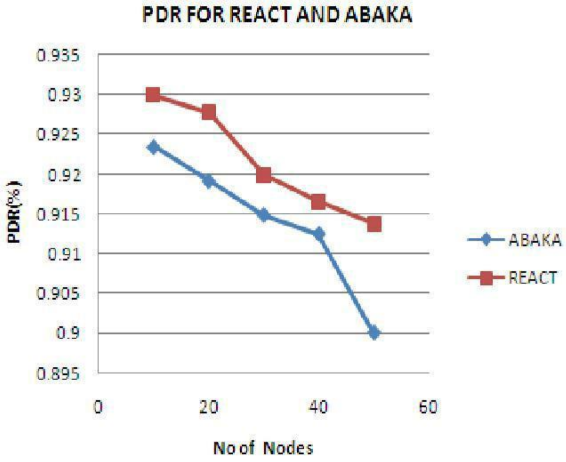


Figure 4. PDR for REACT and ABAKA

2. *Delay for REACT and ABAKA*

The time taken to transfer the packets from the sender to receiver is delay. Compare with the ABAKA protocol, REACT have less delay.

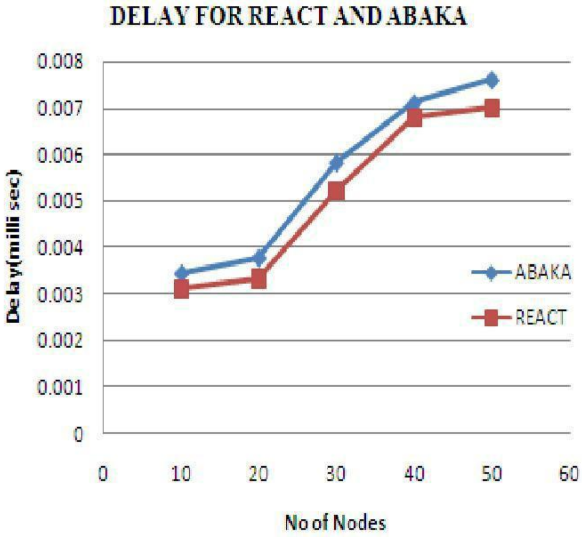


Figure 5. Delay for REACT and ABAKA

3. *Packet loss rate for REACT and ABAKA*

Packet loss is an error that can occur in data network when the data in the network is congested. This means that packets of the data are not able to be transmitted as well as in a normal case, or the fail to reach the destination. Packet loss is expressed as a percentage of the number of packets lost to the total number of packets sent.

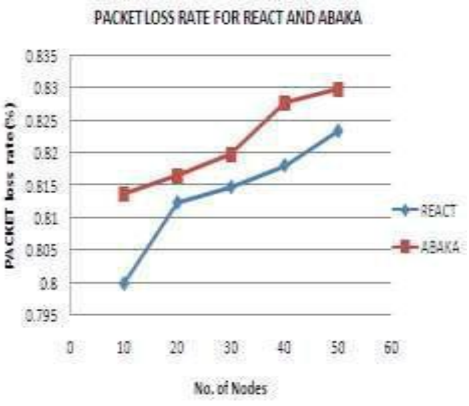


Figure 6. PLR for ABAKA and REACT

V CONCLUSION AND FUTURE WORK

Security and privacy in service-oriented VANETs which was a challenging issue have been ensured. Here privacy preserving data acquisition and forwarding scheme by introducing a novel and provable cryptographic algorithm for key generation and powerful encryption is presented. A cryptographic approach that provides much higher security measures compared to existing ones is introduced and analysis of the performance of the approach using simulation means is done.

The Future 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.

REFERENCES

[1] 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

[2] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, “Enhancing wireless location privacy using silent period”, Proc. of WCNC 2005, New Orleans, LA, pp. 1187-1192.

[3] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos and J. P. Hubaux, “Mix zones for location privacy in vehicular networks”, Proc. Int’l Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia, Aug. 2007.

[4] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A secure and privacypreserving protocol for vehicular communications,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[6] G. Calandriello, P. Papadimitratos, A. Lloy, and J. P. Hubaux, “Efficient and robust pseudonymous authenticationin VANET”, Proc. ACM Mo- bicom, QC, Canada, pp. 19-28, Sept. 2007.

[7]K. Sampigethava, L. Huang, M. Li, R.Poovendran, K. Matsuura and K. Sezaki, “AMOEBA: Robust location privacy scheme for VANET”, IEEE Journal on Selected Areas in Communications, Vol. 25, No. 8, pp.1569-1589, 2008.

[8]C. T. Li, M. S. Hwang, and Y. P. Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy pre- serving for vehicular ad hoc networks”, Computer Communications, Vol. 31, No. 12, pp. 2803–2814, Jul. 2008.

[9] C. Zhang, X. Lin, R. Lu, P. H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3357–3368, Nov. 2008.

[10] A. Wasef and X. Shen, “Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks.” IEEE Transactions on vehicular technology, vol. 58, no. 9, 2009

[11]Yipin Sun, Rongxing Lu, Xiaodong Lin, XueminShen, Jinshu Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications” IEEE Transactions on vehicular technology, vol. 59, NO. 7, 2010.

[12] Albert Wasef, Yixin Jiang, and XueminShen, “An EfficientDistributed-Certificate-ServiceSchemefor Vehicular Networks” IEEE Transactions on vehicular technology, vol. 59, no. 2, 2010

[13] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A Distributed Key Management Framework with Cooperative Message Authentication in VANETs”, IEEE Journal on Selected Areas in Communications, Vol. 29 (2011), No. 3, pp. 616-629.

[14] T.W. Chim, S.M. Yiu, L. Hui, and V. Li, “SPECS: Secure and privacy enhancing communications schemes for VANETs”, Ad Hoc Networks, Vol. 9, 2011, pp. 189–203.

[15] X. Dong, L. Wei, H. Zhu, Z. Cao, and L. Wang, “EP2DF: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Ve- hicular Ad Hoc Networks”, IEEE Transactions on Vehicular Technology, Vol. 60, No. 2, Feb. 2011, pp. 580-591.

[16]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 Transactions on Vehicular Technology, Vol. 60, No. 1, Jan. 2011, pp. 248-262

[17] K. Mershad, H. Artail, and M. Gerla, “ROAMER: Roadside Units as message routers in VANETs”, Ad Hoc Networks Journal, Vol. 10 (2012), pp. 479-496.

[18]KhaleelMershadAnd Hassan Artail,” A Framework For Secure And Efficient DataAcquisition In Vehicular AdHocNetworks”, IEEE Transactions On Vehicular Technology, Vol. 62, No. 2, January 2013.