IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. VI (Feb. 2014), PP 93-98
www.iosrjournals.org

A High Secure And Efficient Data Acquistion Mechanism In Vehicular Ad Hoc Networks(Vanets)

J.Jeyanthy Lizy [1], M.Varghese[2]
[1(]*Infant Jesus College Of Engineering & Technology)*
[2(]*Assistant Professor Infant Jesus College Of Engineering &Technology)*

Abstract:*Recent advances in wireless inter-vehicle communication systems enable the establishment of Vehicular Ad-hoc Networks (VANET) and create significant opportunities for the deployment of a wide variety of applications and services to vehicles. VANETs enable vehicles to communicate with each other and with road side units (RSU). The deployment of vehicular communication systems is strongly dependent on their security and privacy features. Security and privacy are major research concerns in VANETs due to the frequent vehicles movement, time critical response and hybrid architecture of VANETs that make them different than other Ad hoc networks. In order to meet performance goals, it is widely agreed that vehicular ad hoc networks must rely heavily on node-to-node communication, thus allowing for malicious data traffic. At the same time, the easy access to information afforded by VANETs potentially enables the difficult security goal of data validation. Here a suite of novel security and privacy mechanism is proposed using the HARDY function, i.e. hierarchical-based encryption function, and thus evaluating and improving the performance.*

I. Introduction

WIRELESS NETWORKS

Wireless network operates on a specific set of radio frequencies. It operates on a special band of radio frequencies around 2.4 GHz that have been reserved in most parts of the world for unlicensed point-to-point spread spectrum radio services. The wireless network is broadly classified into two types, viz.,

- Infrastructure Networks
- Infrastructure less Networks

Infrastructure Networks

The infrastructure network implements a point to point links between computers or networks at two locations, often using dedicated microwave or laser beams. It is often used in cities to connect networks in two or more buildings without physically wiring the buildings together. AP refers to the access points.

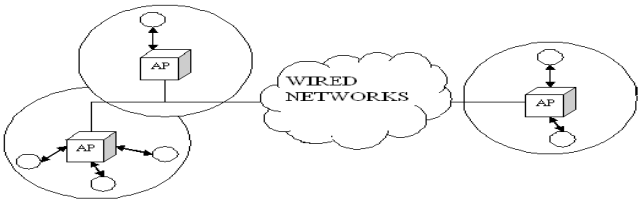

Fig 1: Infrastructure Networks

- Fixed access points connected to a backbone network
- Mobile connects to the net via these access points (base stations)
- RFID and Cellular networks
- Coverage based on placement of access points

Infrastructure-Less Networks

All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. Adhoc networks are very useful in emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in inhospitable terrain.

- No wired backbone
- All nodes are capable of movement
- All nodes serve as routers(multi-hop routes)
- Reduced administrative cost
- Ease of deployment

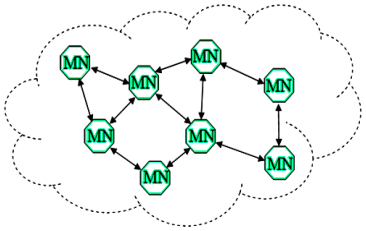

Fig 2: InfrastructureFig 2: Infrastructure-less networks

Security Attacks In VANETS

VANET needs security to implement the wireless environment andservers users with safety and non safety applications. Attackers generate different attacks in the life saving vehicular network. Classes of attacks have been discussed here.

Basically there are two types of attacks, active and passive attacks.. They are not intended to harm the end-user. Some of the more common attacks against privacy are:

- Monitoring and Eavesdropping: This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.
- Traffic Analysis: Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. This can potentially reveal enough information to enable an adversary to cause malicious harm to the network.

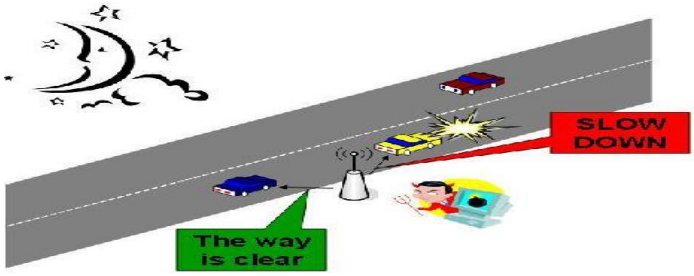

Fig 3: An attack outline

Data Confidentiality:

A vehicular network should not leak sensitive data to neighboring networks. In many applications (E.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality. Given the observed communication patterns, secure channels between nodes and base stations can be set up and later bootstrap other secure channels as necessary.

Data Authentication:

Message authentication is important for many applications in vehicular networks. An adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism.

Data Integrity:

In communication, data integrity ensures the receiver that the received data is not altered in transit by an adversary. Data integration involves combining data residing in different sources and providing users with a unified view of these data.

Data Freshness:

Data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. There are two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation.

The contributions of this paper include:

- A novel approach for users to start their connections in the VANET in a secure way.

- A new cryptographic approach and a handover scheme that provides much higher security measures compared to existingones and analyze the performance using simulation means.
- A novel mechanism for data confidentiality and users location privacy.

II. Existing Scheme

In this project, first a framework that allows users to create accounts with RSUs and connect to them in secure sessions is discussed. Then security features of the framework are described which employs multiple packet keys for encryption, and also describe a new approach for providing location privacy to users by using packet-based pseudonyms and mix zones. Analysis of new cryptographic scheme is also done.. Finally, it is proved through simulations that in this system it provides firm security while ensuring a high success ratio and low latency and calls the system as secure andefficient data acquisition in VANETs.

SYSTEM AND SECURITY MODELS

Although the primary purpose of VANET standards is to enable communication-based automotive safety applications, they allow for a range of comfort applications. Many services could be provided by exploiting RSUs as delegates to obtain data on the user's behalf. These services span many fields, from office on- wheels to entertainment, downloading files, reading e-mail while on the move, and chatting within social networks.

REGISTRATION AND SESSION MANAGEMENT

Each user is considered as a distinct member and gives him/her a unique account with the RSUs. It is required for the users to register with the RSUs at the beginning through the web before they start connecting from their vehicles. 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.

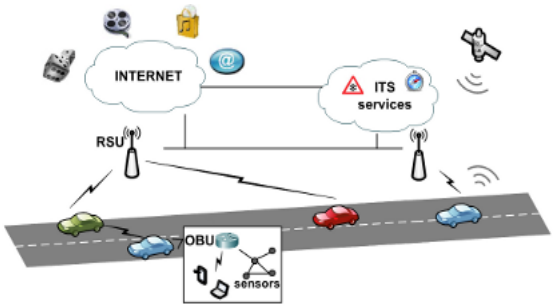

Fig 4: Typical VANET environment

Participating in a Session

Each time a user connects to an RSU, he/she starts a new session. To preserve users' locationprivacy, the scheme makes 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 K_c from the user.

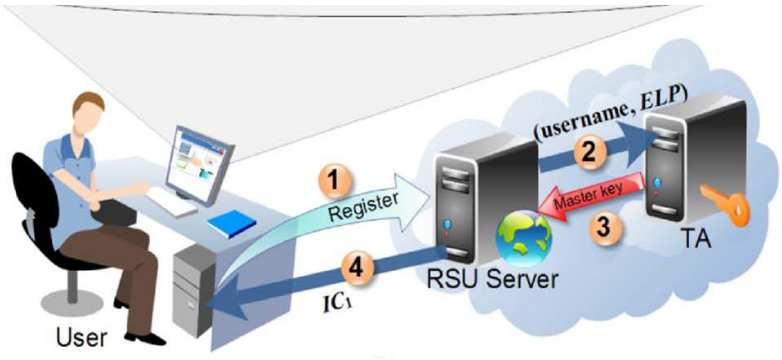

Fig 5: Sample online registration

After the RSU has authenticated the user, it obtains from the TA a packet key K_s, encrypts K_s with the user's K_m, and sends it to the user in a Packet Key packet. Ks will be used by the users to encrypt thefirst packet after they have received the Packet Key packet.Then, each packet will be encrypted using a new set of keys

Switching Connection BetweenRSUs

The handover process is explained using the following scenario. Suppose that a user U is connecting with RSU R1 and wants to switch to RSU R2. U sends to R1 a HandoverRequest that contains the ID of R2. This prompts R1 to send to R2 a Handover packet that contains U's username, his next pseudonym with R1 (p_n), and his next packet key (K_n). Next, R1 sends to U a Handover Confirm that contains $p_n$and K_n. This last packet will be encrypted with the user's current packetkey at R1.U then sends to R2 a Hello message (encrypted with K_n) that contains his username and p_n. R2 decrypts the Hello message, checksthat the username and $p_n$are valid, and then assigns to U a newpseudonym and sends it to him in an ID packet.

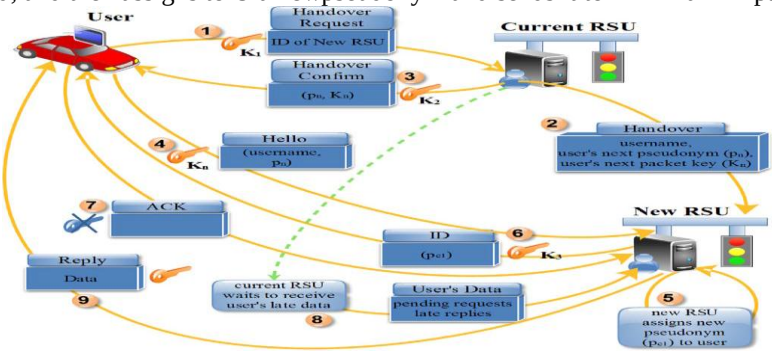

Fig 5: Sequence diagram for hand over scheme

III. Security And Privacy

HARDY Function

To provide data confidentiality, encryption is used to allow only the legitimate user to read and process the transmitted data. Cryptographic schemes are either symmetric or asymmetric, where symmetric schemes use a single key for both encryption and decryption, whereas asymmetric schemes use a public key for encryption and a private key for decryption.

In this paper, an algorithm for securing data messages based on using a symmetric scheme for cryptographic operations is designed. The algorithm is used by the source to generate a sequence of keys from a secret input string (S) and uses these keys to encrypt the next packet. The input string (S) is specified as part of the data in the current packet. This algorithm is also used to transfer the master key of the user to him/her, where the input string (S) to the algorithm will be the user's password using password-based key derivation functions in designing modern password-based encryption schemes with the PBKDF2 function. The hardiness of cracking the final message is much increased at the expense of slight overhead in executing the algorithm.

HARDY is executed by the source to generate nencryption keys. The first key is calculated as K_1 = PBKDF2 (S, S_1, IC_1, L). Each of the other n – 1 keys is calculated as K_i = PBKDF2 (K_i−1, S_i, IC_i, L). In other words, the first key K1 is obtained by executing the PBKDF2 function that passes to it S (a secret sequence of characters of constant size), S_1 (a random salt of size Ss b, e.g., Ss = 128), L (length of packet) and IC_1 (the initial iteration count). IC_1 will be sentonline by the RSU to the user and will be a common secret between them.

Each of the other n − 1 keys (K_2 up to K_n) is obtained by executing the PBKDF2 function that passes to it K_i−1 (which is the key from the previous iteration), S_i (random salt), and IC_i (random iteration count). After generating the n keys, the source executes a for loop, in which the last key (K_n) is used to encrypt the plain-text message M_p, whereas each of the other keys is hierarchically used to encrypt the salt and iteration count of the next stage in addition to the last encryption. Hence, the final cipher message will be:

$$M_c = S_1 || Ek_1[IC_1 || S_2 || Ek_2[IC_3 || S_3 || \ldots\ldots\ldots$$
$$Ek_n\text{-}1[IC_n || S_n || Ek_n[M_p]]]] \qquad (3.1)$$

IV. Results And Discussions

PERFORMANCE EVALUATION

To evaluate the performance of the existing schemes, the main performance metrics used for comparison are success ratio, message delay, handover traffic and hand over delay. Message success ratio (MSR), which is the percentageof messages that are successfully received at theirdestinations. Average overhead traffic (AOT), which is the extra traffic (mainly due to security packets and to the increase in the size

of packets due to cryptographic operations) sent or received by a vehicle. Message delay or the message response time is the total time required to send a request from a vehicle to a service provider and to receive the answer.

SIMULATION RESULTS

Fig 5 shows the simulation with source and destination for the transmission. It illustrates the vehicle to vehicle communication and vehicle to infrastructure communication. Here the network shows has 25 nodes. Among that one is taken as the sink acting as the default RSU i.e. node 0. Nodes 1 to 5 are the fixed access points acting as the RSUs. And the remaining nodes are the mobile nodes acting as the vehicles.

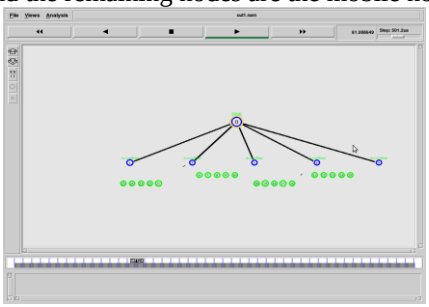

Fig 6: Simulation showing nodes in networks

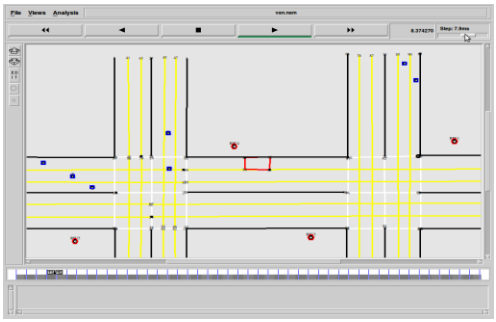

Fig 7: Simulation showing the transmission environment

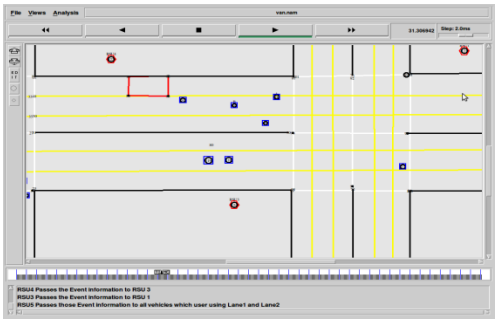

Fig 8: Simulation showing the data transmission.

Figure 6 has different lanes and their intersection, vehicles moving and the fixed RSUs. It shows 4 RSUs labelled in red circle. Moving vehicles are shown in blue circle.

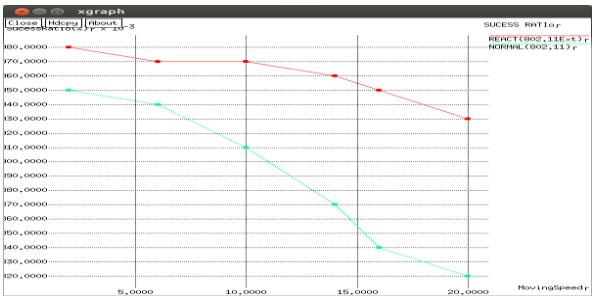

Fig 9: Simulation showing success ratio

In the scenarios in this section, the maximum speed of vehicles is varied between 5m/s to20m/s. It can be seen that the message success ratio in this work drops drastically from 15m/s to 20m/s, mainly because of the cipher messages present in this needs long transmission times, which will not be available when the speed is high, because vehicles will contact each other for shorter periods of time. Simulation result shows that the probability of successful data retrieval through the network is higher than through the normal network with 802.11.

Delay may differ slightly, depending on the location of the specific pair of communicating nodes. Figure shows that this work produces less message delaywhen the speed of the vehicles is small to medium. The simulation shows that the message delay is less when compared to the normal network.

Hand over traffic is the extra traffic, which is mainly due to security packets and to the increase in the size of packets due to cryptographic operations, sent or received by a vehicle. By varying the number of vehicles, it is found that hand over traffic is increasing as increasing the number of vehicles.

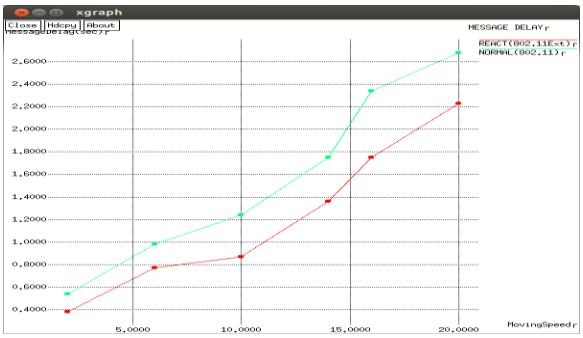

Fig 10: Simulation showing message delay

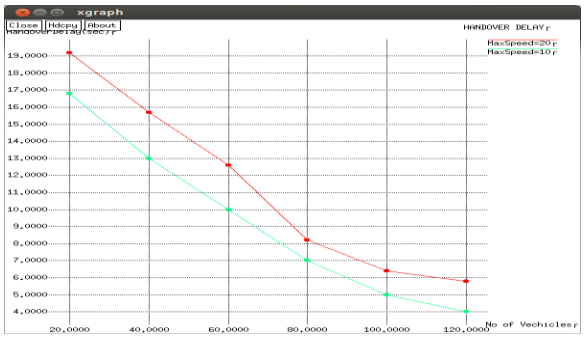

Fig 5.6: Simulation showing hand over delay

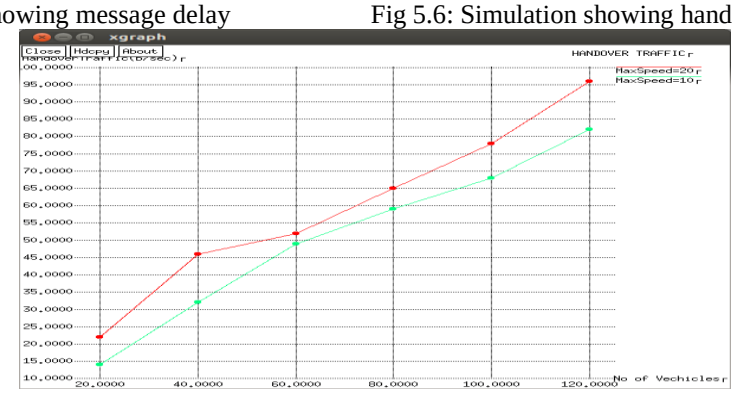

Fig 11: Simulation showing hand over traffic

In general, as number of vehicles increases, a vehicle will have a higher probability that it will find neighbours to forward the packet. So, the packet will be more forwarded and less queued. Hence, the hand over delay decreases and the traffic increases.It can be noticed that the delay and traffic of maximum speed of 20 are much higher than those of 10 because this work is sensitive to speed

V. Conclusion

INFERENCES

security and privacy in service-oriented VANETs which was a challenging issue have been ensured. Here privacy-preservingdata acquisition and forwarding scheme by introducing a noveland provable cryptographic algorithm for key generation andpowerful encryption is presented. A new 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 evaluation of proposed schemeconfirmed its effectiveness compared to a recent security mechanismfor VANETs.

References

[1] Biswas.S, J.Misic, and V.Misic(2011), "ID-based safety message authentication for security and trust in vehicular networks," in Proc. 31st ICDCSW, Minneapolis, pp. 323–331.

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

[3] Calandriello, et.al (2007),"Efficient and robust pseudonymous authentication in VANET," in Proc. ACM Mobicom, Montreal, QC, Canada, pp. 19–28.

[4] Chaum . D and E. van Heyst(1991), "Group signatures," in Proc. EUROCRYPT, vol. 547, pp. 257–265.

[5] Chim.T, et.al (2011), "SPECS: Secure and privacy enhancing communications schemes for VANETs," Ad Hoc Netw., vol. 9, no. 2, pp. 189–203.

[6] Coronado. E and S. Cherkaoui(2008), "Service discovery and service access in wireless vehicular networks," in Proc. IEEE GLOBECOM Workshops, pp. 1–6.