IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 86-92
www.iosrjournals.org

Improved Key Based Security Framework for Vehicular Ad Hoc Networks

Satyam Bestaramunboena[1], Srinivas Sandiri[2]
[1]*Pursuing M.Tech in Wireless and Mobile Communication at Vardhaman College of Engineering (Autonomus) Hyderabad, India*
[2]*Assistant Professor in Electronics and Communication at Vardhaman College of Engineering (Autonomus) Hyderabad, India*

Abstract: *Vehicular ad hoc networks (VANETs) are a subgroup of mobile ad hoc networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. This implies that node movement is restricted by factors like road course, encompassing traffic and traffic regulations. Nodes are expected to communicate by means of North American DSRC standard that employs the IEEE 802.11p standard for wireless communication. To allow communication with participants out of radio range, messages have to be forwarded by other nodes (multi-hop communication).A web based secure registration process that allows a user to create an account with RSUs. During the registration, users provide all required information that enables them to have the benefit of secure connectivity starting from the first packet that they send to the RSUs. We propose a novel cryptographic function that enables users and RSUs to apply the required security level of exchanged messages by adjusting the number of iterations of the function. We derive a set of encryption keys that are used to encrypt the next packet from part of the data in the current packet.*

Keywords: *VANET, Security, RSU, Communication.*

I. Introduction

Inter-Vehicular Communications (IVC) also known as vehicular ad hoc networks (VANETS) have become very popular in recent years. A Vehicular Ad hoc Networks is a special type of Mobile Ad hoc. Networks (MANETs is a kind of wireless ad hoc networks and is self configuring network of mobile routers connected by wireless links) which use vehicles as nodes. The main difference is that mobile routers building the network are vehicles like cars or trucks. Several different applications are emerging with regard to vehicular communications. For example, safety applications for safer driving, information services to inform drivers about the driving hazards and other business services in the vicinity of the vehicle. Governments, corporations, and the academic communities are working on enabling new applications for VANETs. A main goal of VANETs is to increase road safety by the use of wireless communications.

To achieve these goals vehicles acts as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glazes. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology; therefore; VANETs require secure routing protocols. "Numerous Applications are unique to the vehicular setting. These applications include safety applications that will make driver safer, mobile commerce, roadside services that can intelligently inform drivers about congestion, businesses, and services in the vicinity of the vehicle". "VANETs, especially compared to MANETs are characterized by several unique aspects. Nodes move with high velocity, resulting in high rates of topology changes". "Because of rapidly changing topology due to vehicle motion, the vehicular network closely resembles an ad hoc network.

The constraints and optimizations are remarkably different. From the network perspective, security and scalability are two significant challenges". "A formidable set of abuses and attacks become possible. Hence, the security of vehicular networks is indispensable". "The growing importance of inter-vehicular communications (IVC) has been recognized by the government, corporations, and the academic community. Government and industry cooperation has funded large IVC partnerships or projects such as Advanced Driver Assistance Systems and CarTALK 2000 in Europe, and FleetNet in Germany.

VANETs pose many challenges on technology, protocols, and security which increase the need for research in this field".

II. Security Vulnerabilities Of Vanets:

Vehicular ad hoc networks are also prone to several vulnerabilities and attacks. These vulnerabilities can cause small to severe problems in the network and also poses some potential security threats which can deteriorate their functioning. The following section gives a general overview of Vehicular Communications vulnerabilities.

A. Jamming: The jammer deliberately generates interfering transmissions that prevent communication within their reception range. Fig. 1 illustrates that an attacker can relatively easily partition the vehicular network. As the network coverage area (e.g., along a highway) can be well-defined, at least locally, jamming is a low effort exploit opportunity.

B. Forgery: The correctness and timely receipt of application data is major vulnerability. The attacker forges and transmits false hazard warnings which are taken up by all vehicles.

C. Impersonation: Message fabrication, alteration, and replay can also be used towards impersonation. For example, an attacker can masquerade as an emergency vehicle to mislead other vehicles to slow down and yield.

D. Privacy: The inferences on driver's personal data could be made, and thus violating his or her privacy. The vulnerability lies in the periodic and frequent vehicular network traffic: Safety and traffic management messages, transaction based communications (e.g., automated payments).

E. Authentication: Authentication and the inherent integrity property counter the in-transit traffic tampering and impersonation vulnerabilities.

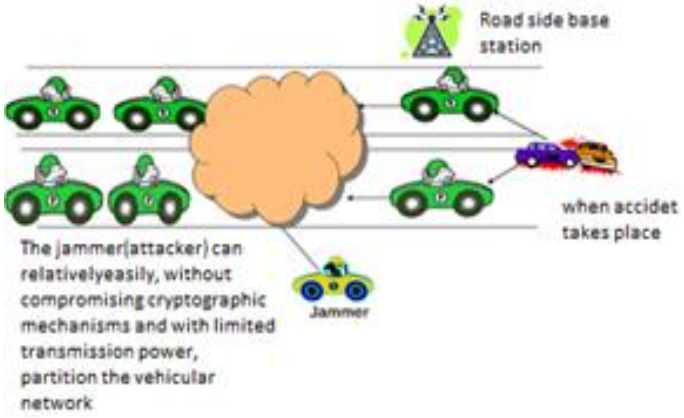

Figure.1. Jamming

2.1 False Position Information:

In VANETs, one critical issue is that when nodes send false position information in their beacon messages, which can severely impact the performance of the network. A potential source for such false position data is malicious nodes. Hence Security in VANETs relies upon the potentially more challenging problem of detecting and correcting malicious data.

VANETs have special requirements in terms of node mobility and position-dependent applications, which are well met by geographic routing protocols. One critical issue is that when nodes send false position information in their beacon messages, this can severely impact the performance of the network. A potential source for such false position data is malicious nodes. The intents of an adversary may range from simply disturbing the proper operation of the system to intercepting traffic exchanged by ordinary users, followed by a potential modification and retransmission.

This section outlines the effects presented in which are caused by falsified position information. Fig. 2 shows an example scenario where node A claims to be at two additional (faked) positions Avi and Avr. Based on a greedy forwarding strategy nodes always select the node nearest to the destination as the next forwarding node. Assuming that F wants to send a packet to node K, it will first send the packet to its only direct neighbor G. G will then forward the packet to the node nearest to the destination from which it received beacons. This seems to be Avr, so the packet ends up at node A, which can now forward, modify, or discard it at will. In the opposite direction, the packet from K will go to I, which will again send it to the assumed best node Avi. So faking only two positions, A is able to intercept all traffic along the road.

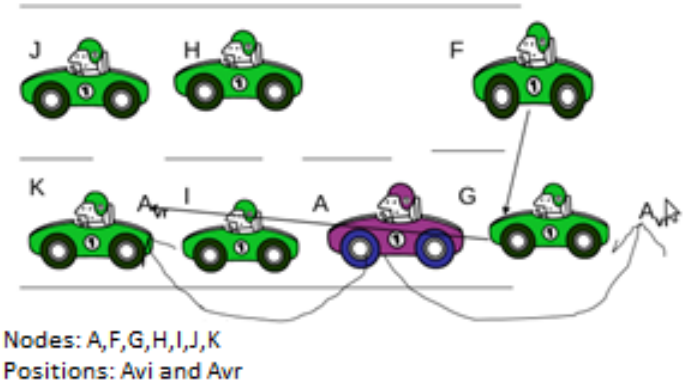

Figure.2. Falsified position Information

III. Related Works

In this paper (1), author identified a new wireless location privacy attack correlation attack in the context of wireless LAN system, and he provided a solution silent period to defeat this attack.

Pros and cons:

In this paper author identifies correlation attack as a threat that cannot be defeated using existing periodical pseudonym update solutions and proposed the new concept of a silent period to combat correlation attacks but there are still some other unsolved issues before random address can be integrated into wireless communication protocols such as 802.11. Silent period protocol is the first step for us to realize wireless location privacy protection by random address.

In this paper (2), In this paper, authors have studied a technique to discover services using roadside units. In this approach, they utilize the network layer routing protocols to determine whether or not the service provider is reachable. If a route to the service provider is not available, they propose to utilize a backbone network, such as the Internet, to find a route.

Pros and cons:

In this paper author have proposed a new service discovery approach and exploits the presence of roadside units in order to increase the efficiency of service discovery. The results confirm the feasibility of this approach for service discovery in vehicular ad-hoc networks but in this paper author not considered about the security issues in service discovery.

In this paper (3), author discusses about Misbehaving or faulty network nodes, which have to be detected and prevented from disrupting network operation, a problem particularly hard to address in the life-critical VN environment. Existing networks rely mainly on node certificate revocation for attacker eviction, but the lack of an omnipresent infrastructure in VNs may unacceptably delay the retrieval of the most recent and relevant revocation information; this will especially be the case in the early deployment stages of such a highly volatile and large-scale system.

Pros and cons:

In this paper to achieve the revocation author designed two protocols tailored to the characteristics of the VN environment. To eliminate the vulnerability window, due to the latency for the authority to identify faulty or misbehaving nodes and distribute revocation information, we designed a scheme that can robustly and efficiently achieve their isolation, as well as contribute to their eventual revocation but author not discussed on each of the individual components of our framework.

In this paper (4), In this paper, authors introduce an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. In vehicular ad hoc networks (VANETs), the speed of a vehicle is changed from 10 to 40 m/s (36–144 km/h); therefore, the need for efficient authentication is inevitable.

Pros and cons:

In this paper author proposed a novel ABAKA scheme for value-added services in VANETs. With ABAKA, an SP can simultaneously authenticate multiple requests and establish different session keys with vehicles. ABAKA considers not only scalability and security issues but privacy preservation as well and to deal with the invalid request problem, a detection algorithm has also been proposed but author not considered about the issues like mobility model and predicable routing, to design novel schemes to gain more efficiency.

In this paper (5), In this paper, author mainly address the problem of mitigating unauthorized tracking of vehicles based on their broadcast communications, to enhance the user location privacy in VANET and propose a scheme called AMOEBA, that provides location privacy by utilizing the group navigation of vehicles.

Pros and cons:

In this paper author proposed a scheme, called AMOEBA that provides location privacy by mitigating the location tracking of vehicles, and protects user privacy by providing vehicles with anonymous access to LBS applications and he discussed about the robustness and liability of the proposed scheme, against active attacks on vehicle safety but here author not considered about mobility of vehicles that will incorporate intersection behavior due to traffic signs and the effects of congested streets, combined with map data and with communication traffic models.

IV. System Analysis:

4.1 Existing System:

There have been several proposals for privacy preservation in VANETs. If VANET 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 hacks their privacy. Hence, pseudonyms were proposed to deceive attackers. The techniques of mix zones, silent period, and ad hoc anonymity were proposed.

Disadvantages:

- Pseudonyms refill
- Privacy leakage by a malicious group leader
- A user may not find other users that are willing to enter into mix zone

4.2 Proposed System:

In this project, we propose a novel approach for users to start their connections in the VANET in a secure way. We illustrate a new handover scheme that is particularly suitable for VANETs. We explain a new cryptographic approach that provides much higher security measures compared to existing ones and analyze the performance of our approach using mathematical and simulation means. We suggest two novel mechanisms for data confidentiality and users' location privacy in VANETs.

Advantages:

- Data security is enhanced
- Load overhead in RSU is reduced by distribution using time slots
- Performance is improved

V. Model Diagram:

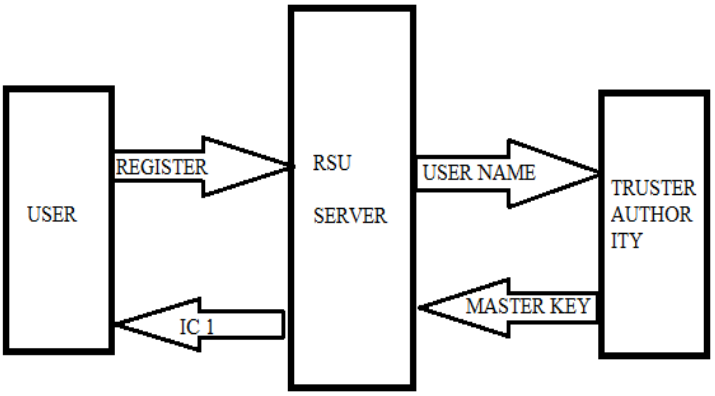

Figure.3. Model Diagram

1. Modules

- Creating the VANET environment
- Route discovery
- Route request
- Route reply
- Registration process in the RSU
- Vehicular communication using RSU

1.1 Creating the VANET environment:

We are going to build the vehicles that are inbuilt with the sensors. Setup the RSU's for the particular coverage area of the vehicles. Build the TA (Trusted Authority) which will check the vehicle entering into the particular coverage area and provide authentication to the user. Fig.4.Representing that how to create VANET environment in

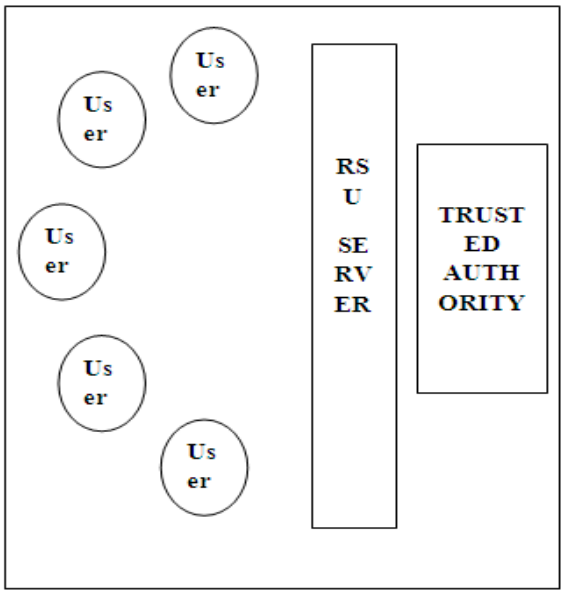

Figure .4. Creating the VANET

1.2 Route discovery:

If the source vehicle has no route to the destination vehicle, then source vehicle initiates the route discovery in an on-demand fashion

After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor vehicle toward the destination vehicle.

If a closer neighbor vehicle is available, the RREQ packet is forwarded to that vehicle. If no closer neighbor vehicle is the RREQ packet is flooded to all neighbor vehicles.

A destination vehicle replies to a received RREQ packet with a route reply (RREP) packet in only the following three cases:

1) If the RREQ packet is the first to be received from this source vehicle
2) If the RREQ packet contains a higher source sequence number than the RREQ packet previously responded to by the destination vehicle
3) If the RREQ packet contains the same source sequence number as the RREQ packet previously responded to by the destination vehicle, but the new packet indicates that a better quality route is available.

1.3 Registration process in the RSU:

- All the users in the VANET should register their details in the RSU.
- After registration the RSU will provide one initial packet key to the user.

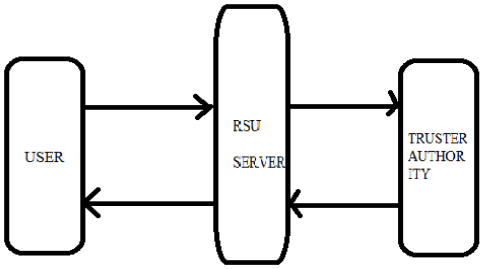

Figure.5. Registration process

- Using this initial packet key, the user will get information about the other nearby vehicles from the TA. Here Fig.5 shows that how the registration process will occur between USER, RSU and Trusted Authority.

1.4 Vehicular communication using RSU:

In this module, we are implementing a routing protocol to transfer messages between the vehicles through RSU. This communication should be service oriented so that the RSU is exploited from obtaining the various types of data. Fig.7. Illustrates that vehicular communication over RSU, vehicle-vehicle communication.

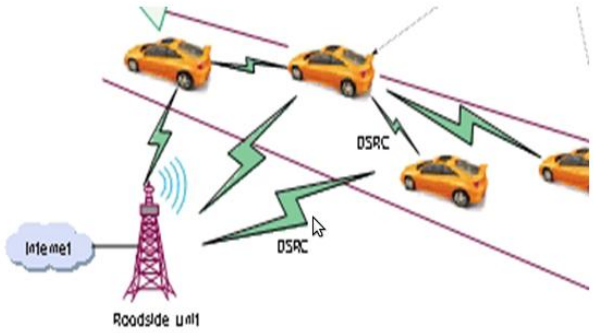

Figure.7. Vehicular communication between RSU and V2V communication

II. Algorithm:

1.5 For participating in a session

Step1: Initially User will send HELLO message to RSU
Step2: RSU prepares user interests and assigns a pseudonym to user
Step3: User identifies that pseudonym and forwards secret key to RSU
Step4: RSU authenticates user by using secret key
Step5: TA will assign packet key to user and user will give ACK
Step6: User will send data request using that packet key and will get data

1.6 For switching connection between RSUs

Step1: user will send handover request to current RSU
Step2: current RSU will send user next pseudonym and next packet key to new RSU
Step3: Current RSU will send handover confirm packet to user
Step4: User will send HELLO message to new RSU
Step5: new RSU assigns a new pseudonym to user and forwards id
Step6: user will give ACK
Step7: user pending data will access
Step8: new RSU will send data to the user

III. Results:

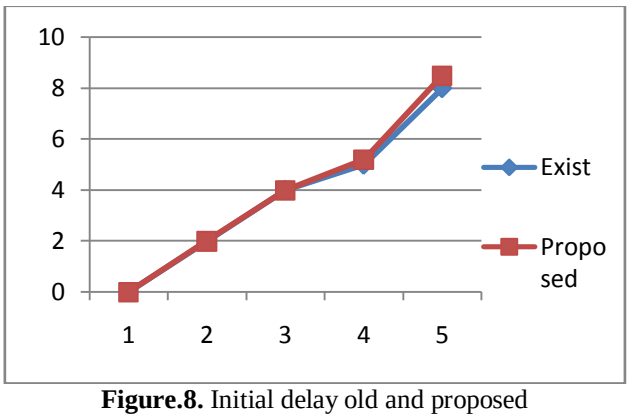

Figure.8. Initial delay old and proposed

The above graph (fig.8) represents the delay in network where x-axis is req/min and y-axis is delay in ms. Here red line represents proposed method and blue one indicates existing method. Because of hybrid cryptography the verification time will be more thats why delay is more in our method.

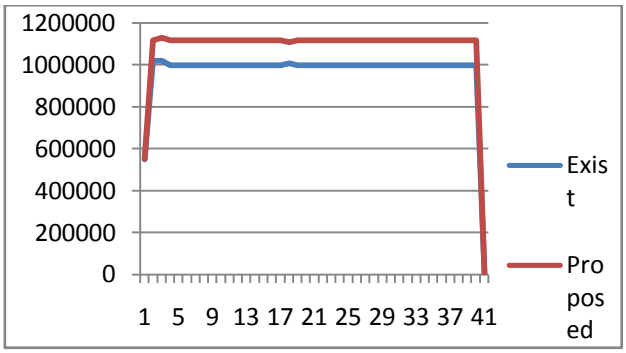

Figure.9. Throughput Comparision

The above graph (fig.9) represents the throughput in the network with respect to time. Throughput means number of bits transmitted per second. Here x-axis is time and y-axis is packet size.

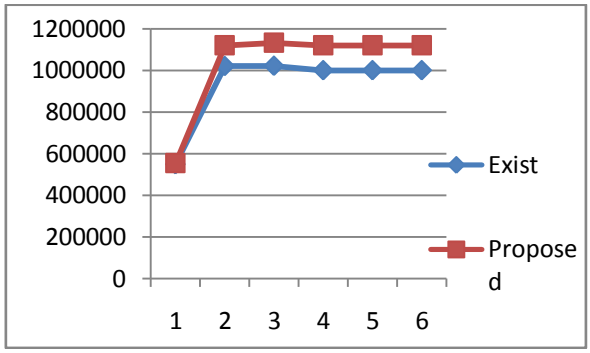

Figure.10. PDF comparison

The above graph (fig.10) represents the packet delivery fraction in the network with respect to time. PDF means number of ratio of received packets to send packets . Here x-axis is time and y-axis is PDF.

IV. Conclusion:

In this paper, we shown how to ensure security and privacy in service-oriented VANETs with our proposed privacy-preserving data acquisition and forwarding scheme by introducing a novel hybrid cryptographic algorithm for key generation and powerful encryption. The evaluation of our proposed scheme confirmed its effectiveness in security compared to a existing scheme. In our process we shown how effectively and quickly we can make handover from one RSU to another RSU with out delay.

From the results obtained we can observe that even though our method providing high security it is also showing more delay when compared with previous method because of more verification. In our future we will propose much more efficient method which will provide high security as well as less delay.

References:

[1]. Leping Huang, Kanta Matsuura, Hiroshi Yamane and Kaoru Sezaki "Enhancing Wireless Location Privacy Using Silent Period"IEEE Communications society/WCNC 2005.
[2]. Brijesh Kadri Mohandas, Amiya Nayak, Kshirasagar Naik and Nishith Goel "ABSRP - A Service Discovery Approach for Vehicular Ad-Hoc Networks" IEEE Asia-Pacific services computing conference, 2008.
[3]. Maxim Raya, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels and Jean-pierre Hubaux "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks" IEEE Journal on Selected areas in Communications, Vol 25, No.8, October 2007.
[4]. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu 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, January 2011.
[5]. Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran "AMOEBA: Robust Location Privacy Scheme for VANET" IEEE Journal on Selected Areas in Communications, Vol 25, No.8, October 2007.
[6]. K. Daniel Wong, K.E Tepe, Wai Chen, Mario Gerla, "Inter Vehicular Communications," IEEE Wireless Communications, Vol 13, no 5,October 2006, pp.6.
[7]. Tim Leinmuller, DaimlerChrysler AG, Elmar Schoch and Frank Kargl, ULM University "Position Verfication Approaches for vehicular Ad hoc Networks," IEEE Wireless Communications, Vol 13, no 5, October 2006, pp.16-20.
[8]. Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux EPFI, "Seuring Vehicular Communications," IEEE Wireless Communications, Vol 13, no5, October 2006, pp.8-13
[9]. J.P Hubaux, Srdjan, Capkun, and Jun Luo. "The security and privacy of smart vehicles," IEEE Security and Privacy, Vol 4, no.3, 2004, pp. 49-55.
[10]. S. Corson, J. Macker. "Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations,". 1999.RFC 2501.