Distributed Security & Profile Rate QOS in Handover Scheme

Mrs Janaki A
ME Student, Department of Communication & Networking
Trichy Engineering College
Trichy

Mrs Priyadharshini K
Assistant Professor, Department of ECE
Trichy Engineering College
Trichy

***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. To allow communication with participants out of radio range, messages have to be forwarded by other nodes (multi-hop communication) and security is the major issue in VANET because of its open nature paving way for hackers to easily enter the network. We propose a hybrid cryptosystem for secure network. (ECDH) using a one-time identity-based aggregate signature technique to avoid time-consuming CRL checking and to ensure the integrity of messages before batch group authentication. We adopt cooperative message authentication among entities in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden. The security and performance analysis show that our scheme is more efficient in terms of authentication speed, while keeping conditional privacy in VANETs. For enhancement, we deploy Elliptic Curve Cryptography Based Deffie-Hellman Algorithm**

Keywords*— *VANETs, MANETs, Wireless Security

I. INTRODUCTION

A computer is a data network or telecommunications network that allows computers to exchange data. In computer networks, networked computing devices (network nodes) pass data to each other along data connections. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Network devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as servers and personal computers, as well as networking hardware. Two devices are said to be networked when a device is able to exchange information with another device. Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent

II. EXISTING METHOD

Main goal of VANETs is to increase road safety by the use of wireless communications. Vehicles acts as sensors and inform each other about abnormal and potentially hazardous conditions like accident, traffic jams and glaze. Vehicular networks closely resemble ad hoc networks because of their rapidly changing topology; therefore; VANETs require secure routing protocols

III. SECURITY VULNERABILITIES

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. An attacker can relatively easily partition the vehicular network.

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).

IV. DISADVANTAGES

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. This scheme mainly focus on navigation problems in VANET, it will cover small range such as covered by three different RSU in a specific area. It will guide the vehicle to a spatial area to park the vehicle in parking yard. All three RSUs installed in indoor and it will monitored. The key disadvantages of the existing system are given below.

- It will only suitable for small coverage area. We can use only three RSUs
- Pseudonyms refill
- Privacy leakage by a malicious group leader
- Long computation delay

- Leading to high message loss
- Customer Willingness/Consent
- Involves user interaction
- Involves manual intervention from the users

V. PROPOSED SYSTEM

We propose a one-time identity-based aggregate signature techniquefor users to start their connections in the VANET in a secure way. A new handover scheme is illustrated that is particularly suitable for VANETs and a new authentication approach that provides much higher security measures are compared to existing ones and analyzes the performance of our approach using mathematical and simulation means. There are two novel mechanisms for data confidentiality and users' location privacy in VANETs

VI. ADVANTAGES

- Data security is enhanced
- Load overhead in RSU is reduced by distribution using time slots
- Performance is improved
- Time consumed in checking
- Re-batch time in authentication is reduced
- More securable
- It will monitor huge amount of area

VII. ALGORITHM AND TECHNIQUES

A. Hashing Algorithm

Message from the source to destination is sent in encrypted form. Even though message confidentiality is achieved through encryption, it could be modified by the intermediate attacker. Hence to ensure message integrity, hashing algorithm is applied in which encrypted message is sent along with its hash value. At the receiver end, message is decrypted and hash value computation is performed. If the received hash value and the computed hash value is same then the message integrity is ensured.

Using a simple hashing algorithm to get hashed value from a string of plain text. The hash value will be attached to packet header for data integrity checking. At the other end of communication, after decryption, the decrypted text will be hashed again to get new hashed value. This new hashed value will be compared to the value attached within packet header. If they are equal, the data integrity is ensured and decrypted text is accepted; otherwise the packet is discarded. In either case, an acknowledge packet will be sent back to sender to inform of the status of the packet. The algorithm for the hash function can be any kind of algorithm like SHA-1, MD5

B. Encryption/Decryption Functions

For encryption and decryption feature we implement CESAR cipher with pre-shared key of 3. These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text three positions. Any encryption/decryption algorithm with symmetric key can be implemented here. Some examples for encryption/decryption algorithms that can be implemented are DES, 3DES, EAS, Blowfish.

VIII. IMPLEMENTATION

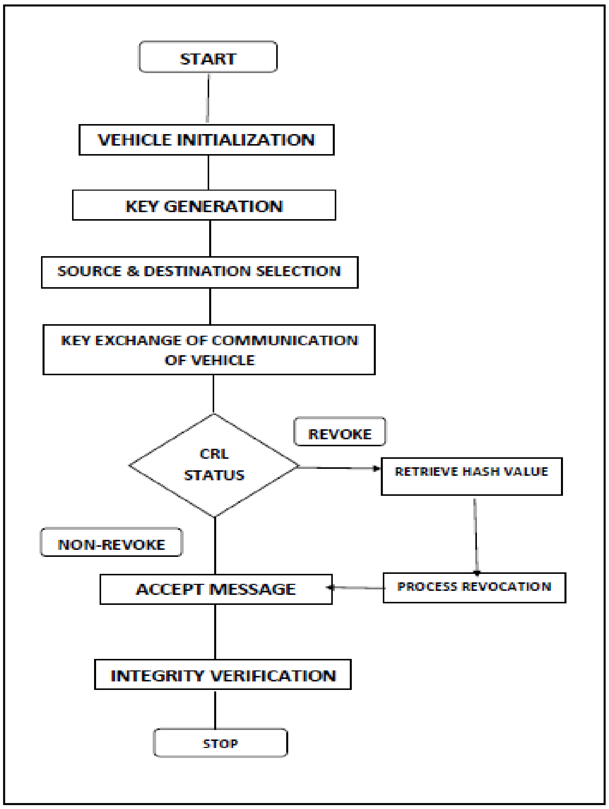

Fig.1 Implementation Diagram

IX. CONCLUSION

The proposed framework ensures better QoS and achieves better QoE throughout the time of the received service and the mobility path of the user. So we can improve packet delivery radio in the network. Because, we can dynamically receive the information at handoff processing. Suppose intermediately we lose some data while induced malicious now we can consider security authentication approach.

Strong security architecture and hasty authentication methods are needed to mitigate the existing security threats in 4G multi-hop wireless networks. Conversely, the network QoS should not be degraded while enhancing security. X

Distributed security architecture for 4G multi-hop wireless networks is presented. QoS-aware base security architecture using the Elliptic Curve Diffie–Hellman (ECDH) protocol is proposed.

X. FUTURE ENHANCEMENT

For future enhancement, a distributed security architecture for 4G multi-hop wireless networks is presented. We propose QoS-aware base security architecture using the Elliptic Curve Diffie–Hellman (ECDH) protocol. For multi hop (n_{th} hop)connectivityusing ECDH, the cell-edge RS broadcasts its public key, ECDH global parameters, RS-ID, and system parameters in the DCD (Downlink channel Decryptor) broadcast message.

REFERENCES

[1] K. Daniel Wong, K.E Tepe, Wai Chen, Mario Gerla, "Inter Vehicular Communications," IEEE Wireless Communications, Vol 13, no 5,October 2006, pp.6.

[2] 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.

[3] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux EPFI, "Seuring Vehicular Communications," IEEE Wireless Communications, Vol 13, no5, October 2006, pp.8-13

[4] 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.

[5] S. Corson, J. Macker. "Mobile Ad hoc Networking (MANET): Routing protocol performance issues and evaluation considerations,". 1999.RFC 2501.

[6] Klaus Plobl, Thomas Nowey, Christian Mletzko, "Towards a Security Architecture for Vehicular Ad hoc Networks," First International Conference on Availability, Relaiability and Security (ARES'06). pp. 374-381.

[7] Valrey Naumov, Rainer Baumann, Thomas Gross. "An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces," In Proc. of the 7th ACM international symposium on mobile ad hoc networking and computing, 2006, pp. 108-119.

[8] Bin Xio, Bo Yu, Chuanshan Gao., "Detection and Localization of Sybil nodes in VANETs," Proc. Wksp. Dependability issues in wireless Ad hoc Networks and Sensor Networks, 2006, pp. 1-8.

[9] P. Golle, D. Greene, and J. Staddon. "Detecting and Correcting Malicious data in Vanets," In Proc. of the 1st ACM international workshop on vehicular ad hoc networks (VANET 2004), pp. 29-37, 2004.

[10] Jeppe Bronstead, Lars Michael Kristensen. "Specification and performance evaluation of two zone dissemination protocols for vehicular ad hoc networks," In Proc. of the 39th annual symposium on simulation, 2006, pp. 68-79.