Secure and Efficient Transmission Mechanism for Emergency Data in Vehicular Ad Hoc Networks

Madhukar S[1], Dr. M N Sreerangaraju[2]

[1]*M.Tech Student, Dept of ECE, Bangalore Institute of Technology*
[2]*Professor, Dept of ECE, Bangalore Institute of Technology*

Abstract - *The Vehicular Ad Hoc Network (VANET) is an emerging mobile Ad Hoc network, which is a vital component of the Internet of Things (IoT) and has been widely used in smart based transportation systems in recent years. For large scale VANETs, it is important to design efficient transmission schemes for time-critical emergency data. In this paper, we propose Transmission Mechanism for Emergency Data (TMED) in vehicular ad hoc networks, in which Geographical information system (GIS) is established. In this mechanism, the request and confirmation signals are sent out to obtain the transmission path from source vehicle to destination vehicle to improve the packet delivery ratio and average transmission delay. We have used NS2 to simulate TMED in city scenario with an implementation of security in VANETs by using Cryptographic technique like SHA 1 algorithm and with an enhanced feature of increasing Data rate to reduce end to end delay, increased throughput and Packet delivery ratio.*

Key Words: *Vehicular Ad Hoc Network, emergency data transmission mechanism, VANET routing, Authentication.*

1. INTRODUCTION

The Vehicular Ad-hoc Network(VANET) is one of the most vital technology in Intelligent Transportation System(ITS).VANET aims to connect together people, roads, and vehicles in ITS through the Global Position System, Geographic Information System, wireless communication, sensor networks, etc. The applications in ITS fall into three categories: road safety, traffic efficiency, and information service. VANET enables real-time communication through Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) which implements these applications. In VANET, V2V communication can implement On-Board Units (OBUs) only. However, Roadside Units (RSUs) are needed in V2R which are costly making the government implement these in limited numbers especially in suburbs. Besides in disaster-affected areas where existing communication infrastructure including RSUs have been knocked out, V2V is more suitable. Therefore, V2V is more flexible when compared to V2R. Data generated from the application may result in traffic congestion which results in packet losses and end-to-end packet delays. The data in the network is classified as ordinary and time-critical emergency data which should be delivered before the deadline for it to be of some use, in case of some urgent events. Examples of such urgent events include traffic accidents, road damages, and construction, the information transmitted between police and/or ambulance. Therefore, emergency data transmission in VANET becomes a challenging problem.

In VANETs, malicious vehicles may interfere with network performance in case of emergency data transmission. In order to avoid such threats, two basic requirements that should be met in VANET which are

- Authentication: authentication means verifying the identity of a vehicle and distinguishing legitimate vehicles from unauthorized vehicles.
- Integrity: Integrity is to assure that messages do not suffer from active attacks, and that all sent messages are not altered.

In order to provide the above requirements, we have use Elliptic curve cryptography mechanism and SHA-1 algorithm for generating Hash value to protect emergency data

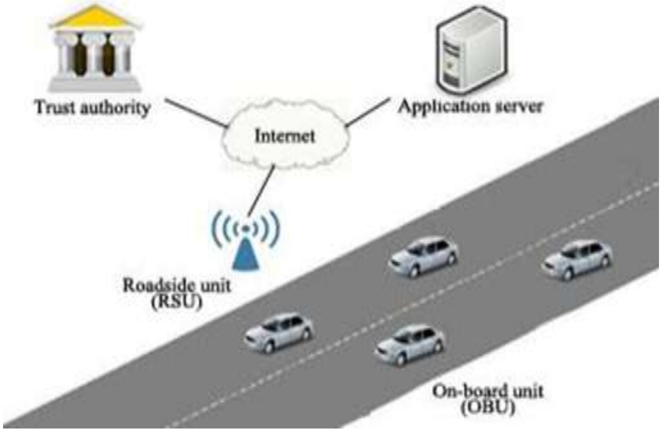

Fig -1: System Architecture

From System Architecture shown in Fig-1, there are four components such as Trust authority, Application server, Roadside unit (RSU) and On-board unit (OBU) which is installed on the vehicle.

Trust authority is the main unit which contains all the information about Roadside unit and vehicle details and it is the responsibility of the trust authority to broadcast the master key to all RSUs.

Roadside Unit (RSU) and On Board Unit (OBU) which are essentially stationary and mobile devices respectively. RSUs and OBUs can be either a provider or a user of services and can switch between such modes.

NTRU is a lattice-based public key cryptosystem proposed in 1996. It has recently received more attention because of the high-security level, moderate key size, and asymptotic performance. Unlike conventional public key schemes, such as RSA and ElGama, NTRU is based on finding small solutions to a system of linear equations over rings. NTRU encryption scheme can be used on lightweight devices. Security and performance are better than the existing RSA and ECC based solutions. However, NTRU requires larger key size and cipher text size. The communication cost is an issue of NTRU in low power networks.

2. RELATED WORK AND PROBLEM STATEMENT

2.1 Related Work

An approach based on Greedy Perimeter Stateless Routing Protocol (GPSR), which is a typical geographic based routing protocol. The nodes know their geographical location and each node forwards the data packets in a greedy way first. A node selects the node in its neighbor list which has the shortest Euclidean distance to the destination node as the next hop. If there is no neighbor closer to the destination node than the current node, GPSR then changes into peripheral forwarding mode. This greatly increases the route forwarding hops and degrades its performance. The Greedy Perimeter Coordinator Routing Protocol (GPCR) is a typical map-based routing protocol proposed by Lochert et al. GPCR is based on GPSR protocol and improved for using in VANET in urban environment.

Anshel et al. proposed a lightweight key agreement protocol (AAGL for short) based on AE. The protocol provides high performance which is better than existing public key based solutions to low-cost platforms. AE introduces a new operation called E-multiplication. It is a one-way function that an adversary cannot reveal the input from a given output. The complexity of E-multiplication increases linearly with the security level. It allows the AAGL protocol to significantly improve efficiency. The underlining mathematical foundations of AE are different from that of traditional public key cryptosystems.

The original specification of the security algorithm was published in 1993 as the Secure Hash Standard, FIPS PUB 180, by US government standards agency NIST (National Institute of Standards and Technology). This version is now often referred to as SHA-0. It was withdrawn by NSA shortly after publication and was superseded by the revised version, published in 1995 in FIPS PUB 180-1 and commonly referred to as SHA-1.SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. Weaknesses have subsequently been reported in both SHA and SHA-1.SHA-1 appears to provide greater resistance to attacks, supporting the NSA's assertion that the change increased the security.

2.2 Problem Statement

Existing routing algorithms for VANET have a drawback in the case of large scale ITS with the high workload when emergency events occur, these protocols cannot deal with the time-constrained delivery of emergency packets.

In VANETs, there are two types of packets namely ordinary packets and emergency packets with different priorities. For example, during natural disaster rescue and traffic accidents, pieces of information like pictures and videos needs to be immediately sent to police cars, ambulances or other official vehicles near the accidents which might be remote areas as well. In case of emergency, the packets need to be transmitted as fast as possible over an efficient path. When a source vehicle needs to transmit packets to a destination vehicle during transmission neighbor vehicles mislead the packets or drop the packets. Hence Providing security to emergency data is one of the important factors to be looked into i.e., no malicious node receives the emergency data.

3. IMPLEMENTATION

3.1 Existing system

In Existing to fulfil the real-time constraints of emergency data an (TMED) transmission mechanism for emergency data as follow by using geographic information system(GIS). Source vehicles send out request message and destination vehicles send confirmed message in this restricted area to establish efficient transmission paths. TMED can reduce the data transmission delay of emergency messages by using the dynamic multi-priority queue management method to process packets. In this method, the high-priority emergency messages are processed first and the deadlines of the packets are also considered. When forwarding data packets, we use restricted greedy forwarding strategy to choose the next hop.

Disadvantages

- More overhead
- No security for emergency data
- Attacker can hack the data

3.2 Network Module

This section includes description of functionality of the scripts used in building topology. This module involves building Wireless Network topology, topology consisting of mobile nodes, each node working with multiple channels.

This module consists of following steps:

- Setting up Wireless Network Topology
- Setting the MAC protocol
- Identifying the neighbours for particular node, Euclidian distance concept used.
- Specifying the data transmission through single and multi-hop
- Specifying the simulation start time and end time that takes place within fraction of seconds and transaction can be viewed through the NAM window at any time.

The vehicle-to-roadside(V2R) communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the vicinity.

Vehicle-to-vehicle (V2V) communications comprises a wireless network where automobiles send messages to each other with information about what they're doing. This data would include speed, location, and direction of travel, braking, and loss of stability.

3.3 Proposed System

In the proposed system an security for the emergency data is provides because of an unsafe wireless communication channel. To protect the security and privacy of vehicle communication, it is necessary to design an effective key agreement scheme. By negotiating a dynamic session secret key using a fixed roadside unit (RSU), which has stronger computational ability than the on-board unit (OBU) equipped on the vehicle, the designed scheme can help to provide more stable communication performance and speed up the encryption and decryption processes. To effectively implement the anonymous authentication mechanism and authentication efficiency, we use ECC (Elliptical Curve cryptography) and SHA-1 to generate symmetric key for authentication and a shared secret key mechanism among the vehicles, RSUs and trusted authority (TA). We design an efficient secret key agreement scheme, which satisfies the above communication and security requirements, protects the privacy of vehicles, and traces the real identity of the vehicle at a time when it is necessary. Computational analysis shows that the proposed scheme is secure and more efficient than existing schemes.

Further we also tune-up the MAC layer protocol 802.11 for higher data processing rates, we define 802.11g standards for processing data and achieve higher packet delivery, lower delay and less computational overhead.

3.4 Security in VANETS

Initially, the sensitive data which are transmitted must be sent to the right destination which provides a secure data transmission. This is achieved by using a cryptographic technique like SHA-1 algorithm. The cryptographic mechanisms used to achieve message authenticity and data integrity is the usage of symmetric primitives. Authentication takes place by using ECC(Elliptic curve cryptography) mechanism, key generation is important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver public key and receiver will decrypt its private key. The size of key is 32bits. Before transmitting emergency data Vehicle signing and RSU verification has to be done along with generation of Hash value.

Vehicle signing:

In this module, the RSU authenticates the vehicles by verifying the signature which sent by vehicle. Vehicle V_i selects a random nonce r_i, which is used to prevent an attacker from tracing the vehicle. Then, it generates a pseudo identity of vehicle PID_i that is composed of $PID_{i,1} = r_i P$ and $PID_{i,2} = VID_i \oplus H(b_i \cdot PID_{i,1})$.

Then, it provides the information $D_i = r_i||PID_i||\sigma_i||T_i$ to the RSU through a secure channel, where T_i is the signing time. σ_i is the signature which contain shared secret key and hash value, b_i is the shared secret between vehicle and RSU.

RSU verification:

This module enables the RSUs to verify the vehicles' signatures. The verification can be performed as When the RSU receives the vehicle V_i's signature D_i, it decrypts D_i with its secret key SK_{RSU} and checks the freshness of time T_i. If T_i is fresh, that is, T_i is within the validity period, the RSU continues to find out V_i's verification public key VID_i and shared secret key b_i; then, it verifies whether the received $PID_{i,2}$ is equal to $VID_i \oplus H(b_i \cdot PID_{i,1})$. VID_i is composed of Vehicle Identities. After signature is valid then vehicle is said to be trusted vehicle

Here we used SHA 1 (Secure Hash Algorithm), it has fast computation process and also secure to transmit data. When sender sends the data, then receiver uses its private key and receiver verifies using sender's public key. It produces a hash value 160 bits and 80 rounds, which is enough for securing the data in VANET. Public key and private key gives input to SHA-1 along with message converts into block of bits which gives Hash value 32-bits.

Mechanism:

At the start of the mechanism, Trusted Authority broadcasts the master key to all the RSUs. Initially vehicles send out master key request to nearby RSUs where in authentication takes place to determine the secure line for data transmission. Before building a connection with TA/RSU, vehicles must be authenticated with the nearby RSU which is implemented using cryptographic technique like SHA-1, key generation and verification. Shared secret key between RSU and vehicle then the vehicle sends the signed request to RSU which contains the secret key. Then the responsibility of RSU is to make sure to validate the signature. If the signature (Key) is valid, then it is a trusted or authenticated vehicle else it is a malicious vehicle which drops the packet and misleads the vehicle. Once the signature is validated, acknowledgement is sent to the vehicle from the RSU and then the vehicle sends out the route request to the RSU. This procedure is repeated for all RSU to find out the authenticated vehicles. The mechanism is programmed in such a way to setup the topology of network as well as vanet nodes which will be used for transmission of critical data.

4. RESULTS AND PERFORMANCE ANALYSIS

We compare the performance of proposed system with an existing system. In the existing system to transmit emergency data from source to destination provides security with a Normal transmission. Where in Proposed system, we provide security with enhancing feature of increasing data rates. We also compare the performance of throughput, PDR, delay and overhead with Existing and Proposed system.

The project is implemented in the NS2 simulator. NAM window provides the graphical representation of the simulation. The results and performance analysis are discussed below. The dotted lines indicate the performance of proposed mechanism and straight line indicates that of existing mechanism.

Table -1: Comparison of Existing and Proposed system

	Existing system	Proposed system
Data rates	2Mbps	54Mbps
throughput	144.57 kbps	149.37 kbps
Packet delivery ratio	0.429	0.673
Delay	556.73 ms	221.43 ms
Overhead	6.41	4.30

1). Throughput: Throughput is the total number of packets processed per unit time.

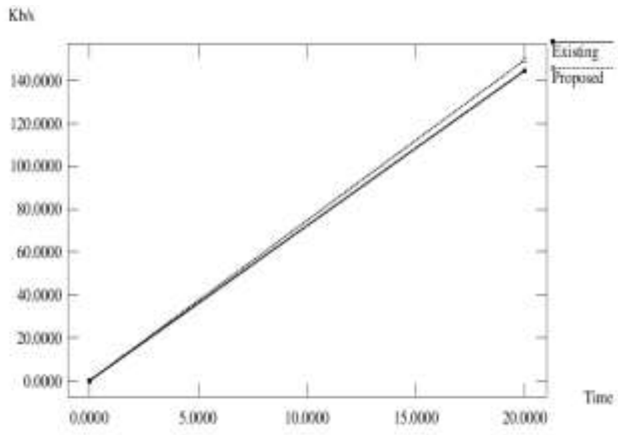

Chart -1: Throughput

From the above graph we increase data rate in the proposed system, throughtput processes faster data and deliver more number of packets per unit time which means better performance than existing system with respect to time, which is measured in kilobits per second.

2). Packet delivery ratio: Packet Delivery ratio is the ratio of number of sent packets to number of received packets.. When we increase data rate in proposed system it process fast data rate and more number packets are delivered to destination with respect to time.

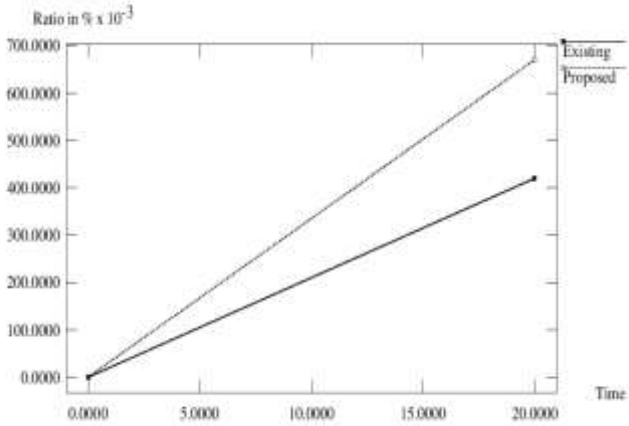

Chart -2: Packet delivery ratio

3). Delay: Delay is the time taken for each data packets to reach the destination from the source.

In proposed system data processing is faster delay consumption is less, where as in existing system no data rate is tuned up so it has more Delay. Lower value of delay means better performance of packet transmission with respect to time. In our proposed system, the delay is reduced with respect to time as shown below.

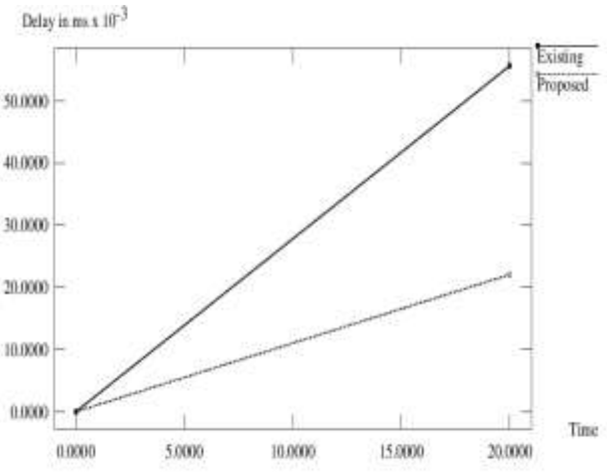

Chart -3: Delay

4). Overhead: Overhead is the ratio between the total number of bytes of routing packets transmitted and the cumulative number of bytes of data packets delivered to the destination.

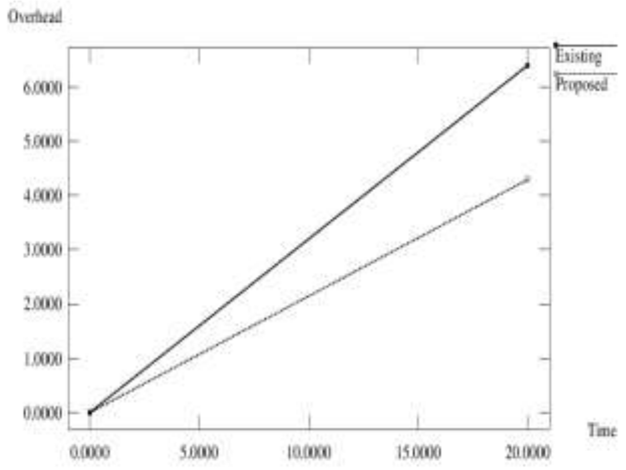

Chart -4: Overhead

From the above graph, we can see that the proposed system has a less overhead due to increase data rate as compared to the existing system with respect to time.

5. CONCLUSION

To keep up with the progress of the current technology in case of real-time constraints of emergency data, we proposed a secure and efficient Transmission mechanism for emergency data with providing security for data along with increased data rate. Source vehicle sends out request signal and destination vehicle confirms after verifying encrypted keys provided by trusted authority which ensures data authenticity and provides security for users. Simulation results show that our proposed TMED performs better in terms of throughput, packet delivery ratio, Delay and overhead with high Data rate.

The Future work, Light weighted key Management system can be implemented to reduce overhead of nodes while computing cryptography functions

REFERENCES

[1] Yu Wang and Fan Li. Vehicular ad hoc networks. In Guide to wireless ad hoc networks, 503-525.Springer, 2009.

[2] George Dimitrakopoulos and Panagiotis Demestichas. Intelligent transportation systems. IEEE Vehicular Technology Magazine, 5(1):77-84, 2010.

[3] Pratap Misra and Per Enge.Global Positioning System: signals, measurements and performance second edition. Massachusetts: Ganga-Jamuna Press, 2006.

[4] Kang-Tsung Chang. Geographic information system. Wiley Online Library, 2006.

[5] Stephane Manuel. Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1.

[6] Barrachina Javier, Garrido Piedad, Fogue Manuel, and J. Martinez Francisco. Road Side Unit Deployment: A Density-Based Approach.IEEE Intelligent Transportation Systems Council, 5(3):30 – 39, 2013.

[7] Lianhai Liu, Yujue wang , Jingwei Zhang and Qing yang. A Secure and Efficient Group Key Agreement scheme for VANET. Sensors 2019,19 482;doi:10.3390/s19030482.

[8] Ning Zhaolong, Xia Feng, Ullah Noor, Kong Xiangjie, and Hu Xiping. Vehicular Social Networks: Enabling Smart Mobility. IEEE Communications Magazine, 55(5):16 – 55, 2017.

[9] Sok-Ian Sou. Modeling emergency messaging for car accident over dichotomized headway model in vehicular Ad-hoc networks. IEEE Transactions on Communications, 61(2):802–812, 2013.