Abstract

A vehicular ad hoc network (VANET) is an emerging new technology developed by integrating ad hoc network, wireless LAN (WLAN) and cellular technology to enable intelligent inter-vehicle communications and to improve road traffic safety and efficiency. VANET is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among vehicles. Collecting the needed data is difficult because vehicles are continuously moving and generating a significant amount of events and data. Data Collection is considered as an inherent challenging problem to Vehicular Ad-Hoc networks. Information's are received dynamically at handoff processing. Intermediately, there may be data loss due to some malicious. Strong security and authentication methods are needed to mitigate the security threats. Conversely, the network QoS should not be degraded while enhancing security. Elliptic Curve Diffie–Hellman (ECDH) protocol is proposed to ensure better QoS and to provide security for vehicular data.

I. INTRODUCTION

Vehicular communication networks are emerging as a key technology for next-generation wireless networking which is developed by integrating ad hoc network, wireless LAN (WLAN) and cellular technology to enable intelligent inter-vehicle communications and to
improve road traffic safety and efficiency. The subclass of mobile adhoc network is vehicular adhoc network which is self organized without any physical infrastructure. VANET is a technology that uses moving vehicle as a nodes in network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and in turn create a network with a wide range

Ad hoc networks also called infrastructure less networks are complex distributed systems consist of wireless links between the nodes and each node also works as a router to forwards the data on behalf of other nodes. The nodes are free to join or left the network without any restriction. Thus the networks have no permanent infrastructure. In ad hoc networks the nodes can be stationary or mobile. In VANET, Communication is of two types: Vehicle to vehicle(V2V). Vehicle to fixed infrastructure on the roadside called roadside unit(V2I). See fig 1. To provide communication between vehicles and road side units, each vehicle equipped with some radio interface or On Board Unit (OBU) that enables short-range wireless ad hoc networks to be formed.

Figure 1: VANET Communication

WiMAX is a standard technology empowering the delivery of last mile wireless broadband access as an alternative to wired broadband like cable and DSL. Fixed, nomadic, and portable are provided by WiMAX, mobile wireless broadband connectivity without the need for directs view with a base station. A range of WiMAX is up to 31 miles, which is mainly aimed at making broadband network access widely available without the expense of stringing wires (as in cable-access broadband) or the distance limitations of Digital Subscriber Line. The trickiest task in VANET is quality of services. In wired networks, the QoS parameters are normally specified in delay and throughput. QoS parameters of vanet include data latency, packet delivery ratio, and bandwidth utilization. Challenges of vanet
communication include security, integrity, authentication, confidentiality, accessibility, scalability, reliability, media access control.

In this paper, we propose QoS based security architecture using Elliptic Curve Diffie Hellman (ECDH) protocol.

II. LITERATURE SURVEY

- W. Drira and F. Filali (2016) introduced a comparison of proactive and reactive data collection schemes is conducted whereas Proactive schemes results the lowest delay and bandwidth usage but the highest loss ratio. Adaptive data collection approach is schemed to efficiently use the available bandwidth. Adaptive data collection scheme is subjected to proactive scheme using variable polling periods based on the vehicle positions in the network and travel time to provide accurate traffic and travel time information to the Traffic Management Center (TMC). An adaptive data collection algorithm is used by each vehicle to aggregate and reduce the amount of data sent to the TMC [1].

- X. Tang and J. Xu (2008) works out to maximize the accuracy of data collected by the base station over the network lifetime. An offline algorithm is devised to compute the optimal data update strategy. Adaptive strategy is developed that makes data update decisions based on sensor readings to meet network lifetime requirements. History and Expected are developed for the adaptive strategy to cope with message losses in wireless transmission. The aim is to make use of the energy budgets of the sensor nodes to improve the quality of collected data][2].

- Ahmed Soua and Hossam Afifi (2013) proposed a distributed Q-learning technique is used to make the collecting operation more reactive to nodes mobility and topology changes. ADOPEL is based on a distributed learning approach where vehicles adaptively choose the forwarding relays to maximize the ratio of collected data without losing the way to the destination node [3].

- Fernando Terroso-Sáenz, Mercedes Valdés-Vela, Cristina Sotomayor Martínez, Rafael Toledo-Moreo, and Antonio F. Gómez-Skarmeta (2012) introduced an event-driven architecture as a novel mechanism to derive vision into beacon messages to detect different levels of traffic jams. The system can be either in the TMC or distributed in vehicles. Event-driven architecture performs a CEP processing of the incoming beacon messages. In that sense, the system takes advantage of enhanced maps (Emaps) which allow vehicles, under certain circumstances, to position themselves at lane-level detail. As a result, the EDA might infer the particular lanes involved in a traffic jam; besides, the EDA can process information from other external data sources, e.g., web services or onboard sensors, which inform about environment conditions of the road an influence on the traffic jam detection. In this way, it can detect different degrees of traffic congestions, regardless of the underlying communication protocol[4].

- Yoann Dieudonné, Bertrand Ducourthial, Sidi Mohammed Senouci (2012) proposed a dissemination mechanism is used for data collections in vehicular ad hoc networks where each vehicle periodically broadcasts information about itself. In the first case,
propagation is performed with the use of opportunistic diffusion of data that is messages are stored in each intermediate node and forwarded to every encountered node until the destination is reached. The second one consists in sending the message to the closest vehicle toward the destination until it reaches it. Likewise, many other types of dissemination exist such as peer-to-peer and cluster-based dissemination. The PIF algorithm works in two steps as Broadcast phase and Feedback phase which has been implemented and tested through the Airplug Software Distribution. It collects data produced by vehicles using inter-vehicle communications only. It is based on the operator ant allowing to construct a local view of the network and to collect data in spite of the network topology changes [5]. Congyi Liu, Chunxiao Chigan and Chunming Gao(2013) proposed a compressive Sensing based Data Collection(CS-DC) in VANETs to improve traffic efficiency. Compressive sensing based data collection (CS-DC), is developed to efficiently collect spatially correlated data in VANETs. The data collection in dense traffic, where numerous vehicles will report their spatially correlated data to an road side unit which serves as the data sink/center, through multi-hop transmissions. The data spatial correlations will make use to reduce information redundancy and improve communication efficiency. Meanwhile, the CS theory is applied to effectively encode/decode the in-network data in data collection, ensuring efficient communication and accurate data recovery [6].

Guillaume R´emy, Sidi-Mohammed Senouci and Mohamed Oussama Cherif(2010) introduced a data Collection and aggregation platform which is to collect a set of information delivered from different data sources (sensors, GPS, etc.) and aggregate them in a reliable manner. The vehicular platform supports an on-board computer connected to the Internet, temperature, humidity and acceleration data are sent by a crossbow sensor using ZigBee protocol, a Holux GPS receiver which sends GPS data using Bluetooth protocol. Collected data is then stored in MySQL database and presented through user-friendly webs interface. It presents useful information (such as traffic information or weather) that could be disseminated to vehicles through a dissemination protocol like ROD[7].

Bartłomiej Płaczek(2011) proposed a paper provides a significant reduction in data amounts transmitted through VSN. The main idea is to detect the necessity of data transfers on the basis of uncertainty determination of the traffic control decisions which uses on-time queries instead of periodical data sampling[8].

III. PROPOSED SYSTEM

The proposed framework for improving QoS is shown in Figure 3.1. The framework helps to ensures better QoS throughout the lifetime of received service and the mobility path of user. It improves packet delivery rate in network. Information are received dynamically at handoff processing so intermediately there may be data loss due to some induced malicious. Strong security architecture and authentication methods are proposed to mitigate security threats in networks. At the same time, network QoS should not be degraded while enhancing security.
A. Communication Model

VANET is created with number of nodes and base station. Nodes are grouped and formed as a network. The vehicles have GPS for finding the location of the vehicle. Drivers can easily know exactly where he is. GPS with map is help to drive the vehicle. Then, set a coverage area to all vehicles in network and node movement along the path. In VANET, all vehicles share its position to all networks in path through GPS. Vehicle user will update and retrieve their information via GPS to traffic management centre (TMC).

B. Network Selection

Node will request base station for network availability; it will always give priority to their own network. Node will check with bandwidth, number of user, mobility path and signal strength. Network will be selected by coverage area of the base station. Base station will serve the node and efficient network will be selected.

C. Fading Detection

Channel fading occurs mainly when the user moves from one station to other station. If the user is stationary almost no time variations of the channel will occur. The average fade duration quantifies how long the signal spends below the threshold. Due to fading, there will be delay. In this work, it is assumed that if node moves outside AP or BS, then fading will be more.

D. Vertical Handoff

When nodes enter different BSs area, previous BS will hand over the node to current BSs. In this work, BS wills handoff the node when it crosses the certain range of coverage. The range will set based on the signal strength of the base stations. If node and BS detects fading, then signal handoff will take into account. If handoff occurs in same network, then it is known as horizontal handoff. If handoff occurs in different network, then it is known as...
vertical handoff. In this work, vertical handoff is implemented. The handoff is implemented not only in signal fading but also when the number of user increased or delay is increased. Due to this type of handoff, network quality is improved.

**E. ECDH Protocol**

There is multi hop (nth hop) connectivity using ECDH. The cell-edge of RS broadcasts its public key, ECDH global parameters, RS-ID, and system parameters in the DCD (Downlink channel Decryptor) broadcast message. The node that wishes to join RS will start the ranging and connectivity process. After the initial connectivity, if the newly connected node is an RS, then the super ordinate RS will share the public key of the BS and the corresponding global parameters. The new RS will associate with the BS by sending its public key to the BS. Hence, the multi hop RS can send its traffic over the tunnel mode.

**IV. EXPERIMENTAL STUDY**

The proposed security architecture is implemented using Network Simulator version NS2.33. Creation of vehicles and base station is done using Tool Command Language.

**V. CONCLUSION**

The proposed system is used to ensure better QoS and to provide security using distributed security architecture. At the same time, network QoS should not be degraded while enhancing security. QoS based security is proposed using Elliptic Curve Diffie Hellman (ECDH) Protocol. The performance of the overall architecture was evaluated using computer simulations and interesting results were obtained.

**VI. REFERENCES**


**TO CITE THIS PAPER**