IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

GSN: GACVO– Based Secure Navigation for VANETs

C. Kiruthika[1], Prof. N. Gugha Priya[2]

PG Scholar, Department of Computer Science and Engineering, KIT- Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[1]

Assistant Professor, Department of Information Technology, KIT- Kalaignar Karunanidhi Institute of Technology, Coimbatore, India[2]

Abstract: The vehicular ad-hoc networks are described by high mobility of nodes, which resulting in regular and rapid changes in the network topologies. A trust based framework is proposed for safe and reliable information dissemination in vehicular networks. Group Based Receiver-Driven Protocol divides the network into clusters or groups, where nodes are grouped using the same search query like the same direction or same destination route, or so on. Each cluster has a cluster head (Group Leader), its task is to manage communication processes inside, and to outside its cluster. The proposed scheme has the benefit of using real-time road environment to figure a better route and at the same time, the information source can be correctly authenticated. Protecting the privacy of the drivers, the query (destination) and the driver who issues the query are assured to be unsinkable to any party including the trusted authority.

Keywords: Vehicular ad hoc networks, Group based receiver-driven Protocol, Request and reply propagation, Clustering.

I. INTRODUCTION

A vehicular ad hoc network (VANET) uses vehicles as mobile nodes in a MANET to create a mobile network. A VANET turns every participating vehicle into a wireless router or node, permitting vehicles approximately 100 to 300 meters of each other to connect and, in turn, build a network with a broad range. When vehicles fall out of the signal range and drop out of the network, other vehicles can join in, linking vehicles to one another so that a mobile Internet is formed. It is expected that the first systems that will combine this technology are police and fire vehicles to communicate with each other for safety purposes. Vehicular ad hoc networks can be analyzed as a component of the intelligent transportation systems (ITS). As supported by ITS, vehicles communicate with each other via inter-vehicle communication (IVC) and with roadside base stations via roadside-to-vehicle communication (RVC). Recent advances in electronics and wireless communication allow researchers to form a network of cars connected to each other using cheap wireless devices. This, in turn, opens up some fascinating opportunities like intelligent transportation systems (ITS). An ITS enables us to deal with the traffic and its huge cost, e.g., pollution and waste of time, in a much more efficient way using fast and reliable communication between the traffic control center and cars[2].

Characteristics of VANET are High mobility nodes, Predictable topology (using digital map), Critical latency requirements, slow migration rate, No problem with power and Security and privacy. Vehicular Networks contains a large number of nodes (for vehicles).Here, every vehicle can communicate with other vehicle using short radio signals DSRC (5.9 GHz), within 1 KM range area.

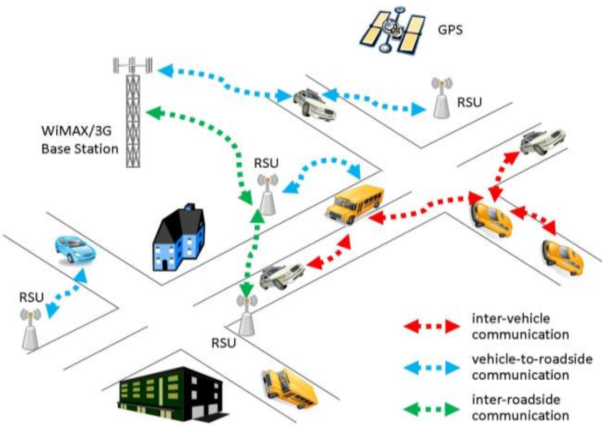

GPS
RSU
WiMAX/3G Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig.1.Architecture of vehicular networks

The communication between each vehicle is an Ad Hoc communication that means each connected node can move freely, there are no any wires required, the routers used is called Road Side Unit (RSU), the RSU worked as a router between the vehicles on the road and connected to other network devices. Typically, in a VANET each vehicle is assumed to have an onboard unit (OBU), and there are roadside units (RSU) are installed along the roads.Application servers and trusted authority (TA) are installed on the back end. The onboard unit and road-side units communicate with each other by using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a securely fixed network (Internet).

In Vehicular Networks System each vehicle has OBU (onboard unit), that is connected to the vehicle with RSU

DOI 10.17148/IARJSET.2016.3638

via DSRC radios, and another device is TPD (Tamper Proof Device). Tamper Proof Device (TPD) holds the vehicle secrets; that is all the information about the vehicle like keys, driver's identity, trip details of that vehicle, the speed of the vehicle, route, etc.

II. RELATED WORK

Secure routing, privacy, and trust in VANETs have gained concentration from the research society over past few years. One of the most recent protocols is FACT framework [1], which consists of two modules. One applies the three safety checks to construct definite the message is trusted. The security measures are, 1) Originated from a trusted region and traversed a trusted path; 2) was not under attack on its path; and 3) Has a suitable content. Second looks for a not hazardous path. A vehicle-assisted data delivery (VADD) [3], which is based in the scheme of caching techniques and carry and forward, where nodes carry the packet when routes do not be present and forward the packet to the newest addresses that move into its locality. The proposed VADD protocols give the best performance regarding data packet delay.

The proposed mechanism [5] described the challenges of extending the conventional view of confidence to data-centric. Using the data-centric trust Establishment framework, trust value of each piece of the message is calculated and interconnected but may be differing information are combined. The Dempster-Shafer theory is used to estimate information reports with correlated trust values. The trust model proposed by Wang et al. [6] is designed for senders. A sender finds vehicles to forward the message. Finding similar nodes based on energy, location, and brand is not practical and does not guarantee of being a better candidate.

Broadcasting messages is the scope of a VANET reputation system (VARS) [8]. X.Li et al. [7] proposed protocols of AOTDV, AOMDV, and AODV; these protocols were capable of deciding multiple loop-free paths as nominees in single route detection. AOTDV advances packet delivery ratio, and it is against multiple attacks from malicious nodes, containing the black-hole attack, modification attack, fabrication attack and impersonation attack than other two protocols.

The PMBP, PKI-based multi-hop dissemination protocol in [9] described authenticated, integrated, non-repudiated vehicular connections. The PKBP protocol describes the ECDCA-based key administration, message signing and verifying process and multi-hop dissemination system.

III. PROPOSED SYSTEM

In this section, we present a group based receiver-driven protocol which reduces the load of RSUs and to communicate more than one vehicle at a time. The overview of the proposed protocol is shown in the fig.2. GACVO- Group based receiver driven protocol RSU- Road Side Units

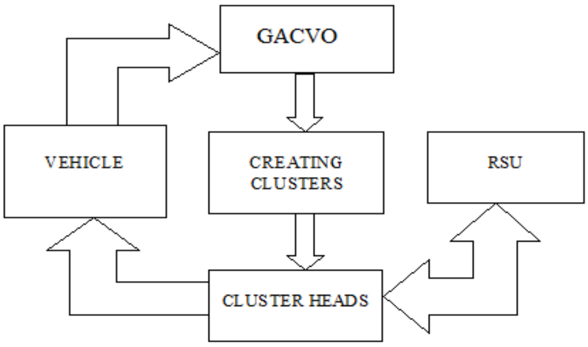


Fig.2. Architecture of the GACVO protocol

A. Overview

Group Based Receiver-Driven Protocol (GACVO) is proposed, which divides the network into clusters or groups A query message with node ID and location information is sent to all nodes in the network. This protocol forms cluster by same query information and selects the cluster head based on the node value. Every RSU can send a reply to more than one vehicle at a time. So it reduces the query traffic and load of RSU. The node value calculated based on the updated neighbor nodes list using parameters such as Degree difference, Mobility of the node and remaining battery power of the node. Every node that is in clusters has a different identification mark from another one. And all the danger messages propagate in the network by the only head of the cluster known as a cluster head in the sub-network. When a node goes out from the communication range of cluster heads than that, join another one, or a new cluster is formed. One common approach to resolving possible privacy leakage is to use a different authenticable, but unrelated identity [9] to communicate with a different RSU.

B. Creation of nodes as vehicles and RSUs

Vehicular ad hoc network (VANET) is a significant element of the Intelligent Transportation Systems (ITSs). In a typical VANET, each vehicle is assumed to have an On Board Unit (OBU), and there are Road-Side Units (RSU) installed along the roads. Each node formed for VANET setup is considered as a vehicle. And nodes are kept in different locations to show that the vehicles are in different locations and they need minimum traveling delay in a distributed manner using the online information about the road condition and the security system.

In this module, create OBU or Tamper-proof device and RSU. In the simulation, assume sensor nodes as a vehicle and RSU. The RSU has information about vehicles; the information is already stored in RSU (like vehicle license key). RSU tracks the vehicle and routes in the network. This network defines the most efficient route for vehicles and saves the travel time.

C. Navigation requests and replay propagation

In this module, the vehicle’s navigation query is propagated across the network of RSUs and describes how the result is sent back to the vehicle. RSU takes up the role of beginning the route searching process by composing the route request message and broadcasts it to all neighbors

DOI 10.17148/IARJSET.2016.3638

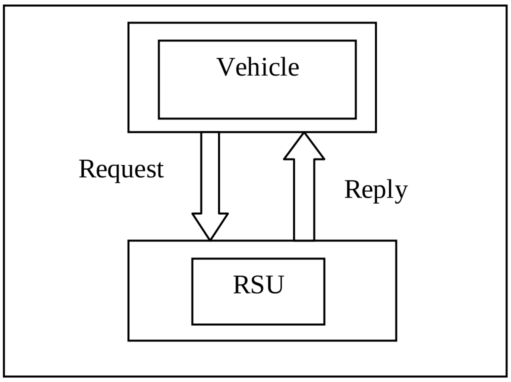
that are closer to the destination than itself. Each RSU includes information corresponding to its hop into the route reply message. And also stores the next hop of the forward path (i.e., the identity of the RSU from which it receives the route reply message) into its routing table for guiding a vehicle later on. Now, let us go back to RSU, the RSU that initiates the route searching development. Upon receiving a navigation reply, RSU will not forward it to the vehicle immediately. Instead, it waits for a threshold (which is a system parameter) amount of time for more replies (possibly from RSUs on other directions).

Query creation:

A query message with node ID and location information is sent to all nodes in the network.

Cluster formation:

This protocol forms cluster by same query information and selects the cluster head based on the node value. Some low-speed vehicle in a cluster with high-speed vehicle makes reason of high end to end delay and losses of data packets. The cluster is a subgroup of an interconnected network. In VANET network, the vehicle moving at road takes the form of cluster. In past decades, many researchers propose several cluster based routing approaches for improving communication pitfalls in between high-speed moving vehicle. In this cluster based approach cars that move on roads are selected as a dynamic node that behaves as a source or intermediate node and by these nodes communication range. The network is separated as groups of nodes that are directly in the communication range of them or another nodes group that are in the roadside unit communication range to reduce re-clustering rate. Every node that is in clusters has a different identification mark from another one.



RSU- Road Side Unit

Fig.3. Generation of request and reply

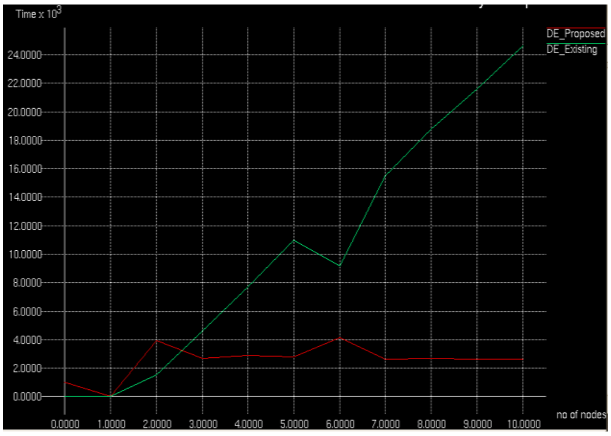
D. Verification of hop information

In networks, a hop is a midway connection in a string of connections involving two devices. Whenever a router or gateway is a mediator device between two different and remote hosts, nodes or networks, it is identified as a hop. For example, on the internet, most data packets need to go through a number of routers before they achieve their final destination. Every time the message is forwarded to the next router, a hop occurs. The more hops, the longer it takes for data to go from source to destination. Recall that the reply contains a set of identities, a set of locations, a set of certificates, and a set of hop information (average speed and road condition), every corresponding to an RSU along the route returned. Verifying the average speed and road condition provided by an RSU, its identity is verified. In turn, to verify an RSU's real identity, its certificate has to be verified using TA's identity. That the verification process may take an excessive amount of time it is carried out by a tamper-proof device with today's technology.

E. Guiding to destination

In VANETs, two notifications are sent to all vehicles whenever there is an incident in the network, such as accident or road problems once they join into the vehicular networks [1]. Incident notifications are sending at the beginning, and clearance notifications are sending when the incident is finished.

Having the returned route, if the vehicle has GPS device installed and it can receive GPS signals from the current location, it can simply search for each RSU based on the list. GPS device is not an assumption of our scheme. Even if the vehicle does not have GPS device installed, the GACVO scheme can make use of the VANET to guide the vehicle to the destination.



X-axis: Number of Nodes, Y axis: Time

Fig.4. Delay Comparison of FACT framework and GACVO protocol

IV. EXPERIMENTAL RESULT

On comparing the GACVO protocol with the existing protocol, the proposed method adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated using identities. 2) Navigation queries and results are sheltered from eavesdroppers. 3) Information given by RSUs can be properly authenticated before the route is being used. Besides satisfying all security and privacy requirements, the solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time. On the other hand, the route returned by the proposed scheme can saves travel time compared with existing framework.

V. CONCLUSION AND FUTURE WORK

Thus various protocols in VANETs for providing authenticated, integrated, non-repudiated vehicular connections have been reviewed. The existing systems consider a single vehicle at a time. However the proposed framework is focused on the clusters, that framework forms the vehicles as clusters so it can reply more the vehicle at a time. It reduces the RSUs load, query traffic, and delay. For enhancing the security in VANETs, robust learning methods against these attacks are required. The current VANET is not scalable, especially for large cities. It is feasible only for a small environment.

REFERENCES

[1] Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan and Victor C.M. Leung, “A Context-Aware Trust-Based Information dissemination framework for vehicular networks,” IEEE Trans. Veh. Technol., vol. 2, no. 2, pp. 3974–3982, April 2015.

[2] K. Rostamzadeh and S. Gopalakrishnan,“Analysis of message dissemination in vehicular networks,” IEEE Trans. Veh. Technol., vol. 62, no. 8, pp. 3974–3982, Oct. 2013.

[3] J. Zhao and G. Cao, “VADD: Vehicle-assisted data delivery in vehicular ad hoc networks,” IEEE Trans. Veh. Technol., vol. 57, no. 3, pp. 1910– 1922, May 2008.

[4] M.-C.Chuang and J.-F. Lee, “TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks,” IEEE J. Syst. vol. 8, no. 3, pp. 749–758, Jan. 2013.

[5] M. Raya, P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “On data-centric trust establishment in ephemeral ad hoc networks,” in Proc. IEEE 27th Conf. Comput. Commun. (INFOCOM’08), 2008, pp. 1238–1246.

[6] J. Wang, Y. Liu, X. Liu, and J. Zhang, “A trust propagation scheme in VANETs,” in Proc. IEEE Intell. Veh. Symp., 2009, pp. 1067–1071.

[7] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, “Trust-based on-demand multipath routing in mobile ad hoc networks,” IET Inf. Secur., vol. 4, no. 4, pp. 212–232, Dec. 2010.

[8] F. Dotzer, L. Fischer, and P. Magiera, “VARS: A vehicle ad-hoc network reputation system,” in Proc. 6th IEEE Int. World Wireless Mobile Multimedia Netw. (WoWMoM’05), 2005, pp. 454–456.

[9] D. Tian, Y. Wang, H. Liu, and X. Zhang, “A trusted multi-hop broadcasting protocol for vehicular ad hoc networks,” in Proc. Int. Conf. Connect. Veh. Expo. (ICCVE), 2012, pp. 18–22.

[10] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the CONFIDANT protocol,” in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput., 2002, pp. 226–236.

DOI 10.17148/IARJSET.2016.3638