EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.140-147
SANA ACADEMIC PRESS

A Study on Building A Secured Environment for Value-Added Services in VANET's using ABAKA

P. Caroline Anitha [1], S.Brindha[2]
[1]*Research Scholar, Dept. of Computer Science & Applications, St.Peter's University, Chennai.*
[2]*Asst.Prof., Dept. of Computer Science & Applications, St.Peter's University, Chennai*
carolineanitha@gmail.com

Abstract: *To achieve efficient routing protocol for vehicular ad hoc networks (VANETs); existing system employs intersection-based Geographical Routing Protocol (IGRP) in city environments. IGRP is based on an effective selection of road intersections through which a packet must pass to reach the gateway to the internet. The selection is made in such a way that guarantees with high probability and network connectivity among the road intersection while satisfying quality-of-service (QoS) constraints on tolerable delay, bandwidth usage and error rate. To deal with security and privacy issues in VANET the proposed scheme builds a secure environment for value-added services in VANET's using An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks (ABAKA). ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message.*

Keywords: *VANET, IGRP, ABAKA, QoS.*

I. INTRODUCTION

Due to the recent technological advancements, many cities are upgraded to smart cities. In smart cities, every single thing will be connected with one another with the help of wired or wireless connections. VANETs are emerging new technology to integrate the capabilities of new generation wireless networks to vehicles. In this paper; our focus will be mainly on the user's and vehicle's safety. Recently the usage of vehicles has increased drastically. So most of the major cities are facing a heavy traffic jam during peak hours and also many accidents are taking place. The world today is living a combat, and the battle field lies on the roads, the estimated number of deaths is about 1.2 million people yearly worldwide and injuries about forty times of this number, without forgetting that traffic congestion that makes a huge waste of time and fuel. VANETs can enable vehicles to communicate with each other so that drivers can have better awareness of what is going on in their driving environment and take early action to respond to an abnormal situation.

VANET Routing Protocol

In VANET, the routing protocols are of five classifications.

Topology based Routing Protocols

These routing protocols use links information that exists in the network to perform packet forwarding. They are subdivided into two types.

Proactive Routing Protocols

The proactive routing means that the routing information like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of proactive routing protocol is that there is no route discovery since the destination route is stored in the background.

Reactive Routing Protocols

Reactive routing opens the route only when it is necessary for a node to communicate with each other. It maintains only the routes that are currently in use; as a result it reduces the burden in the network.

Position based Routing Protocols

Position based routing consists of class of routing algorithm. They share the property of using geographic positioning information in order to select the next forwarding hops. The packet is sent without any map knowledge to the one hop neighbour, which is closest to destination. This type of routing is beneficial since no global route from source node to destination node need to be created and maintained.

Cluster based Routing Protocol

In cluster based routing; a group of nodes identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Virtual network infrastructure must be created through the clustering of nodes in order to provide scalability.

Geo Cast Routing Protocol

Geo cast routing is basically a location based multicast routing. It's objective is to deliver the packet from source node to all other nodes within a specified geographical region.

Broadcast Routing Protocol

Broadcast routing is frequently used in VANET for sharing, during traffic and emergency. It is also used for delivering advertisements and announcements.

APPLICATIONS

In VANET; the applications that increase the vehicle safety on roads are called safety applications and the applications that provide value added services like entertainment are called user applications. Vehicular applications are classified as

- Active road safety applications.
- Traffic efficiency and management applications.
- Comfort and infotainment applications.

Safety applications can significantly decrease the number of road accidents. Sixty percentages of road accidents can be avoided if a driver is provided with a warning , half a second before the moment of collision.

II. SYSTEM MODEL

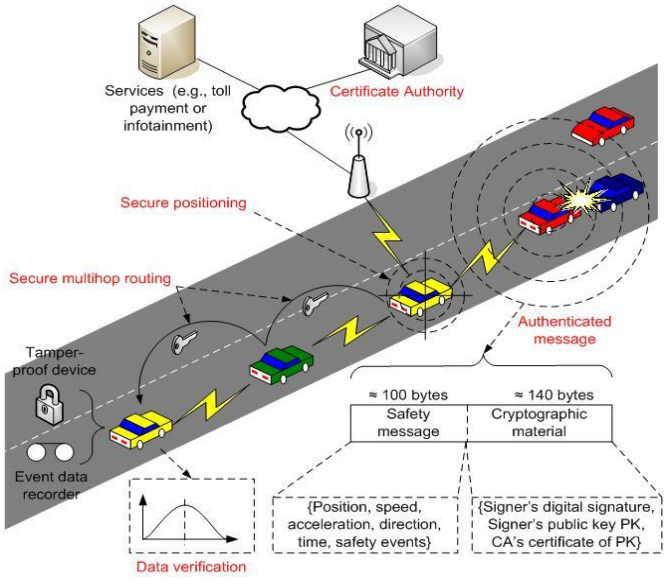


Figure 2. Network Architecture in VANET

VANET consists of moving vehicles commun icating with each other as well as with some nearby RSU. A VANET is different than a MANET in the sense that vehicles do not move randomly as nodes do in MANETs, rather moving vehicles follow some fixed paths such as urban roads and highways. While it is easy to consider VANETs as a part of MANETs, it is also import ant to think of VANETs as an individual research field, especially when it comes to designing of network architecture. In VANET architecture, an on board unit (OBU) in a vehicle consists of wireless transmitter and receiver.

In a broad sense, we can loosely define three possible communication scenarios for vehicles. One possibility is that all vehicles communicate with each other through some RSU. This architecture may resemble wireless local area networks (WLAN). Second possibility is where vehicles directly communicate with each other and there is no need of any RSU. This can be classified as Ad-hoc architecture. In third possibility, some of the vehicles can communicate with each other directly while others may need some RSU to communicate. This can be referred as hybrid scenario. Understanding of network architecture is important in order to realise the full potential of vehicular communication. Most of the researchers have based their studies by dividing VANET scenarios in three categories namely Urban, Rural and Freeway/Highway. One of the reasons to investigate in such a manner is to make sure that it will eventually cover the need of inter -networking for entire vehicular environment. Each environment has its own specific challenges to overcome. For example, in a sparse network like highways, the low density of vehicles remains the prime issue. Even in some urban environments, low penetration ratio and low traffic at night times can cause long network delays.

III. LITERATURE REVIEW

Hanan Saleet et al., 2011, identified, despite better path stability, geographical forwarding does not perform well in a city environment either. Its problem is that, many times, it cannot find a next hop (i.e., a node closer to the destination than the current node). The recovery strategies proposed in the literature are often based on planar graph traversals, which were shown not to be as effective in VANETs due to radio obstacles and high node mobility. A number of road-based routing protocols, have been designed to address this issue. However, they fail to factor in vehicular traffic flow by using the shortest road path between source and destination. It is possible indeed that the road segments on the shortest path are empty. They fail to factor in vehicular traffic flow by using the shortest road path between source and destination. It is possible indeed that the road segments on the shortest path are empty. To overcome these limitations; they proposed in their paper an Intersection-based Geographical Routing Protocol (IGRP) consisting of successions of road intersections that have, with high probability, network connectivity among them. Geographical forwarding is still used to transfer packets between any two intersections within the path, reducing the path's sensitivity to individual node movements. The selection of the road intersections is made in a way that maximizes the connectivity probability of the selected path while satisfying quality-of service (QoS) constraints on the tolerable delay within the network, bandwidth usage, and error rate.

Borcea et al., 2009, Vehicular ad hoc networks (VANETs) are expected to support a large spectrum of mobile distributed applications ranging from traffic alert dissemination and dynamic route planning to context- aware advertisements and file sharing. Considering the large number of nodes participating in these networks and their high mobility, debates still exist about the feasibility of applications using end-to-end multi-hop communication. The main concern is whether the performance of VANET routing protocols can satisfy the throughput and delay requirements of such applications. The RBVT routing protocols leverage real-time vehicular traffic information to create road-based paths. RBVT paths can be created on demand or proactively. The RBVT protocols assume that each vehicle is equipped with a GPS receiver, digital maps and a navigation system that maps GPS positions on roads. RBVT-R discovers routes on demand and reports them back to the source, which includes them in the packet headers. RBVT-P generates periodical connectivity packets that visit connected road segments and store the graph that they form. This graph is then disseminated to all nodes in the network and is used to compute the shortest paths to destinations.

Panichpapiboon et al., 2008, presented an analytical framework to determine the connectivity requirements for distributing the traffic information in a self-organizing vehicular network. One and two-way street scenarios were considered and some of the important physical –layer parameters considered were fading, propagation path loss, transmit power and transmission data rate. Most traffic information systems rely on a centralized communication model, where the collected traffic data are sent to a central processing unit before being distributed back to the drivers on the street. This is quite inefficient, particularly in terms of delay. In addition, the infrastructure required for the centralized communication model can be costly. In a VANET, vehicles can self-organize and forma network to exchange information. Messages from a source vehicle can be relayed to a distant vehicle, which may be multiple hops or several blocks away. A time-critical message from a source should be able to propagate and reach all the vehicles on the road segment without any delay due to the unavailability of the vehicles to forward the message. Clearly, this requires the road segment to have a certain number of vehicles equipped with communication devices.

Zhang et al., 2008, declared that security and privacy are the most fundamental issues in determining the applicability of all the VANET based protocols and devices. The creation of VANET's is obviously a great plus to the traffic management and road safety. Malicious behaviour of users, such as a modification and replay attack with respect to the disseminated messages, could be fatal to the other users, and should be identified and rejected from the networks. In addition to the user related privacy information such as the driver's name, license plate, speed, position; travelling route should also be protected and inaccessible by the public. Furthermore, in the case of a dispute such as a crime or car accident scene investigation; the authorities should be able to reveal the identity of the message senders. Such a privacy preservation requirement is also referred as conditional privacy.

Ghassan Samara et al., 2010, the various challenges faced by Vehicular Networks are:

Mobility: The basic idea from Ad Hoc Networks is that each node in the network is mobile, and can move from one place to another within the coverage area, but still the mobility is limited, in Vehicular Ad Hoc Networks nodes moving in high mobility, vehicles make connection through their way with another vehicle that maybe never faced before, and this connection lasts for only few seconds as each vehicle goes in its direction, and these two vehicles may never meet again. So securing mobility challenge is a hard problem. Many researchers have addressed this challenge but still this problem is not solved.

Volatility: The connectivity among nodes can be highly ephemeral, and maybe will not happen again, vehicles travelling through coverage area and making connection with other vehicles, these connections will be lost as each car has a high mobility, and maybe will travel in opposite direction. Vehicular networks lacks the relatively long life context, so personal contact of user's device to a hot spot will require long life password and this will be impractical for securing VC.

Privacy Vs. Authentication: The importance of authentication in Vehicular Ad Hoc Networks is to prevent Sybil attack. To avoid this problem we can give a specific identity for each vehicle, but this solution will not be appropriate because most of the drivers wish to keep their information protected and private.

Privacy Vs. Liability: Liability will give a good opportunity for legal investigation and this data can't be denied (in case of accidents), in other hand the privacy should not be violated and each driver must have the ability to keep his personal information from others (Identity, Driving Path, Account Number for toll Collector etc.).

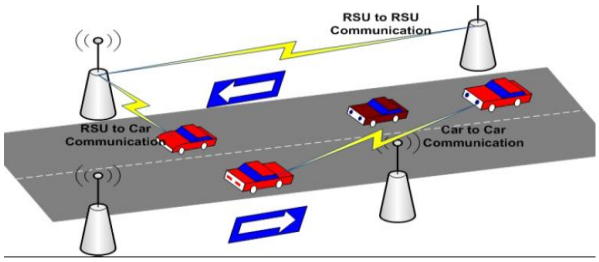
Network Scalability: The scale of this network in the world approximately exceeds 750 million nodes and this number is growing, Another problem which arises is that there is no global authority to govern the standards for this network.

Jiun-Long Huang et al., 2011, proposed a novel ABAKA scheme for value-added applications in VANETs. ABAKA consists of the following three phases: 1) the system initiation phase; 2) the pseudo identity generation phase; and 3) the batch authentication and key agreement phase. A new vehicle first performs the system initiation phase to preload the system parameters. Then, the pseudo identity generation phase is used to generate the pseudo identity and corresponding private key for privacy issue. Finally, the batch authentication and key agreement phase is executed when the vehicle wants to access services provided by SPs. Due to batch verification, ABAKA enjoys several advantages such as lower verification delay and transmission overhead. However, the expense of the batch verification is that, once an invalid request exists in a batch of requests, the batch verification may lose its efficacy. Note that the invalid request could come from a variety of reasons such as packet loss, wireless channel interference, or the involvement of malicious attackers. This problem commonly accompanies other batch-based verification schemes.

Sanjay Batish et al., 2015, proposed that Intersection-based Geographical Routing Protocol (IGRP) is suitable for dense traffic environments. It considers efficient selection of road joints along which a packet travels to arrive at the gateway. Vehicles have access to a digital map (e.g. Map Mechanics, Smart View to find the location of its neighbouring road intersections. Internet gateway gives information to source node to pass on a packet to gateway. Each moving node gives its present information to the gateway when it goes out of its communication range. Internet gateway builds different set of paths between itself and each node. To raise intermediate node's constancy, IGRP makes paths by considering adjacent road joints toward the gateway. These paths are called as backbone paths which are located as succession of joints. Based on these backbone routes, the Internet gateway will choose the most linked route. Source node receive selected path and store it in packet headers. Intermediate nodes forward packet to next node by using information located in packet header. IGRP achieves better performance, selects routes that are highly connected and assures less end-to-end delay.

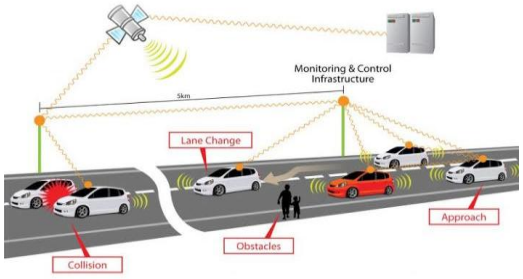
IV VANET

Vehicular Ad hoc Network (VANET) belongs to wireless communication networks area. VANET is a special kind of network that is mainly concerned about the safety of users and its focus is to reduce the accidents.



VANET is the emerging area of MANETs in which vehicles act as the mobile nodes within the network and the communication takes place through wireless links mounted on each node (vehicle). Each node within VANET acts as a participant and also as a router of the network. VANET are self-organizing network. It does not rely on any fixed network infrastructure. Higher node mobility, speed and rapid pattern movement are the main characteristics of VANET.

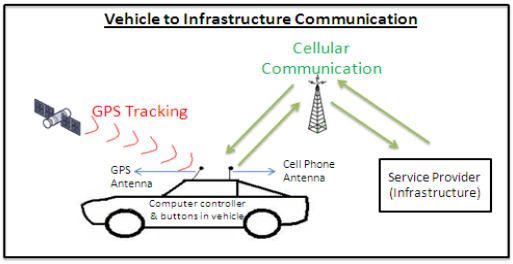
Vehicle to Vehicle Communication (V2V)



Vehicle to Vehicle communication approach is most suited for short range vehicular networks. It is fast, reliable and provides real time safety. It does not need any road side infrastructure. V2V does not have the problem of Vehicle Shadowing in which a smaller vehicle is shadowed by a larger vehicle

preventing it to communicate with the Roadside infrastructure. Location based broadcast and multicast are the proper communication methods for collision avoidance in V2V Communication.

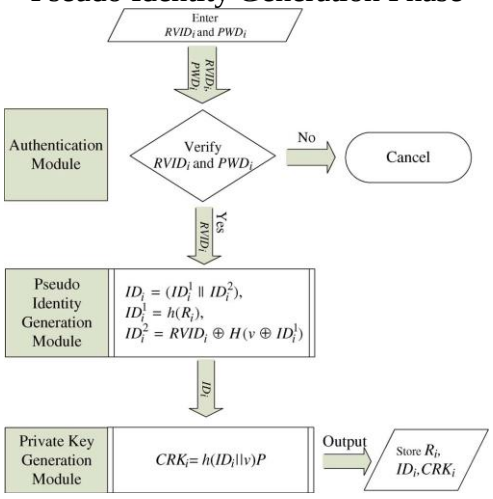
Vehicle to Infrastructure (V2I) / Vehicle to Roadside Communication (V2R)



Vehicle to Infrastructure provides solution to longer-range vehicular networks. It makes use of pre-existing network infrastructure such as wireless access points (Road-Side Units, RSUs). Communication between vehicles and RSUs are supported by Vehicle to Infrastructure (V2I) protocol and Vehicle to Roadside (V2R) protocol.

In this paper we are going to discuss about how a secured environment can be provided for value added services in VANET's using Anonymous Batch Authenticated and Key Agreement Scheme for Value- Added Services in Vehicular Ad Hoc Networks (ABAKA). To increase their stability, IGRP builds routes based on immediate and adjacent road intersections toward the gateway. These routes which are called backbone routes are represented as sequences of intersections. IGRP runs an intersection based routing protocol o find the optimal route. For securing the network, the system uses ABAKA scheme. With ABAKA we can simultaneously authenticate multiple requests andestablish different session keys with vehicles using Gateway. ABAKA considers not only scalability and security issues but privacy preservation as well.

Pseudo Identity Generation Phase



V. CONCLUSION

THE IGRP routing message approach improves the performance of routing in VANET's. It satisfies QoS constraints as a constrained optimization problem. IGRP achieves better performance in such a way it selects routes that are connected and at the same time satisfies thresholds on the end-to-end delay, hop count and BER. The proposed trusted routing framework is developed using ABAKA scheme.

VI. SCOPE FOR FUTURE WORK

In future, this work can be extended with the features of VANET's, such as the mobility model and predictable routing, to design novel schemes to gain more efficiency. Batch verification algorithm will be used to detect invalid signature detection problem in order to prevent the trusted authority from tracing its real identity.

REFERENCES

[1]. C. Borcea, G. Wang, J. Nzouonta, and N. Rajgure, (2009) "VANET routing on city roads using real-time vehicular traffic information," IEEE Trans. Veh. Technol., vol.58, no.7, pp.3609-3626.

[2]. Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, (2010) "Security Analysis of Vehicular Ad Hoc Networks," 2nd Int'l Conf. Network Applications, Protocols and Services.

[3]. Hanan Saleet, Rami Langar, Kshirasagar Naik, Raouf Boutaba, Amiya Naik and Nishith Goel, (2011) "Intersection-Based Geographic Routing Protocol for VANETs: A Proposal and Analysis," IEEE Trans. Veh. Technol., vol. 60, no. 9.

[4]. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien, (2011) "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," IEEE Trans. Veh. Technol., vol. 60, no. 1

[5]. S. Panichpapiboon and W. Pattara-atikom, (2008) "Connectivity requirements for self-organizing traffic information systems," IEEE Trans. Veh. Technol., vol. 57, no. 6, pp. 3333-3340.

[6]. Sanjay Batish, Manisha Chahal and Sanjeev Sofat, (2015) "Comparitive study of position based routing protocolas in VANET," ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 15.

[7]. C.Zhang, P.-H. Ho,X. Lin, X. Shen,X. Sun and X. Wang, (2008) "TSVC: Timed efficient and secure vehicular communications with privacy preserving," IEEE Trans. Wireless Commun., vol.7, no. 12, pp. 4987- 4998.