SECURE COMMUNICATION IN VANETS USING PRIVACY PRESERVING TECHNIQUE

Shruthi.M.H¹, Shashidhar.V²

¹PG Student, Dept of CSE, RRCE, Shru409@gmail.com
²Asst. Prof, Dept of CSE, RRCE, shashigowd@gmail.com

ABSTRACT

VANET (Vehicular adhoc network) this provide intelligent service to the real time road information by using navigation service. Service support is required to reach specific destination. The RSU (road side unit) is use to find best route and also source information can be authenticated using real-time road information. Security services provide protection to driver and support to query of driver guaranteed to any party including valid authority. The security requirement supports authentication and privacy for driver. Road map conducts analysis for simulation and shows effective terms of processing delay and providing short distance routes.

Keywords: RSU, Security

1. INTRODUCTION

VANET is a vehicle to vehicle (Inter-vehicle communication-IVC) and roadside to vehicle (RVC) communication system. VANET provides continuous connectivity by integrating cellular and Ad Hoc networks. The ad hoc network provides service traffic congestion alarm, Collision warning, lane-change warning which are safety related services to vehicle users. The major research challenges are design of routing protocol, data sharing, security and privacy, network formation etc. VANET supports wireless products like remote keyless entry devices, laptops and mobile telephones) which are used in vehicles. As wireless devices and networks become extremely important, there is a great demand for communications between Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I). VANETs also supports a wide range of safety and non-safety applications, Value added services such as safety for vehicles, automated toll payment, managing traffic, better navigation. Location-based services such as finding the closest petrol bunk, hotel or lodge and television applications such as providing access to the Internet. VANET routing protocol not based on MANET protocols variations, but based on the characteristics of urban environments from the very beginning. Junction-based Multipath Source Routing or JMSR for short.

2. LITERATURE SURVEY

Here we describe how the earlier protocols were used to transfer the data from one vehicle to the other vehicle.

A. Intelligent inter-vehicle communication to achieve road traffic safety and to improve efficiency

F. Li and Y. Wang proposed Vehicular network is an emerging new technology integrating ad hoc network, wireless LAN (WLAN) and cellular technology to accomplish intelligent inter-vehicle communications and also to achieve road traffic safety and to improve efficiency. VANETs are differentiated from other types of ad hoc networks using hybrid network architectures, node movement characteristics and new application scenarios. Therefore, VANETs show many networking research challenges uniquely .The design of VANETs efficient routing protocol is very critical. In this paper, we discuss the VANETs research challenge of routing and survey recent routing protocols and VANETs related mobility models.

B. VANETs research challenge of routing and survey recent routing protocols

I. Broustis and M. Faloutsos proposed Vehicular network is an emerging new technology integrating ad hoc network, wireless LAN (WLAN) and cellular technology to accomplish intelligent inter-vehicle communications and also to achieve road traffic safety and to improve efficiency. VANETs are differentiated from other types of ad hoc networks using hybrid network architectures, node movement characteristics and new application scenarios. Therefore, VANETs show many networking research challenges uniquely .The
design of VANETs efficient routing protocol is very critical. In this paper, we discuss the VANETs research challenge of routing and survey recent routing protocols and VANETs related mobility models.

C. Position-based routing For VANETs

Lochert, M. Mauve, H. Füßler, and H. Hartenstein proposed the Position-based routing, as it is used by protocols like Greedy Perimeter Stateless Routing, is very well suited for highly environments like inter-vehicle communication on roads. However, it has been discussed that media player obstacles, as they are found in city areas, have a bad impact on the performance of position-based routing. In prior work presented a position-based approach which alleviates this problem and is able to find robust routes within city areas. It is similar to the idea of position-based source routing as proposed for terminate routing. The algorithm needs global knowledge of the city topology as it is provided by a static street map. From this information the sender determines the junctions that have to be traversed by the packet using the Dijkstra shortest path algorithm. Then using position-based fashion forwarding between junctions are done. In this short paper we show how position-based routing can be applied to a city scenario without assuming that nodes have access to a static street map and without using source routing.

D. Highway traffic position-based routing approaches in VANETs

Lochert, H. Hartenstein, J. Tian, H. Fuessler, D. Hermann, and M. Mauve proposed the Routing of data in a vehicular ad hoc network is a challenging task due to the high dynamics of such a network. Highway traffic position-based routing approaches can very well deal with the high mobility of network nodes. Baseline position-based routing has difficulties to handle two-dimensional scenarios.

In this paper we analyze a position-based routing approach that makes use of the navigational systems of vehicles. Simulation we compare with non-position-based ad hoc routing strategies. The Video traffic simulator makes use of highly realistic vehicle movement patterns derived from Daimler-Chrysler’s. While DSR’s performance is limited due to problems with scalability and handling mobility, both AODV and the position-based approach show good performances with the position-based approach outperforming AODV.

3. PROPOSED SYSTEM

The majority of routing protocol for VANETs so far, such as Greedy Perimeter Coordinator Routing, Geographic Source Routing or Connectivity-Aware Routing, use only one single route from the source to destination. GPSR handles each packet separately. Some of its variations, like GPCR-MA, exploit the use of additional information, like electronic maps and traffic, in order to improve GPSR’s performance. However, the advantages and disadvantages of multiple nodes disjoint routes in VANETs. Some of their main conclusions were that: single-path and multipath have similar performance when source and destination are only a few (2-3) hops away, but for larger source-destination distances (4-5 hops) some difference is observed; route coupling plays a significant role;

VANET routing protocol not based on MANET protocols variations, but based on the characteristics of urban environments from the very beginning. Junction-based Multipath Source Routing or JMSR for short. JMSR is a geographic routing protocol, in the sense that it exploits the location of the nodes and also of the street junctions, known via digital street maps. It maintains concurrently two paths from the source to the destination as a series of junctions the packets should pass through, and not as a series of nodes-relays.

A new routing is designed exclusively for VANETs and presents some initial performance. The algorithm was named Junction-based Multipath Source Routing (JMSR). Its main characteristics comprise the multiple routes towards the destination, the junction-centric logic.
4. CONCLUSION

In this paper, we design an authenticated and anonymous routing protocol for VANETs. VANET-based secured privacy-preserving navigation scheme. We utilized speed conditions of data and road collected by RSUs. Our plan adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities.

2) Navigation queries and results are secured from eavesdroppers. Besides, with the idea of unknown user, nobody can link up a vehicle’s navigation query and its identity including TA.

3) Information provided by RSUs can be properly authenticated before the route is used and satisfying all requirements of security and privacy, this 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 our plan can lead to savings of up to 57 percent of traveling time compared with the offline map data searching approach. Our plan provides lower route blocking rate in practice. Note that our VSPN can apply to the situation where the route searching process is done by a central server, which collects and verifies speed conditions of road and data from RSUs. At vehicle authentication process is simpler because a vehicle only needs to check against the central server’s signature on the processed result. However, such centralized approach is not scalable, for big cities. We are implementing our VSPN test to further verify its performance.

REFERENCES


