iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** Issue I **Month of publication:** May 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Group based receiver driven protocol for Efficient and scalable multicasting

K.Subramanian[1]
[1]II M.E Computer Science and Engineering (Specialization in Networks)
Pannai College of Engineering and Technology, Anna University

Abstract- vehicular adhoc network (VANET) becomes increasingly popular in many countries. VANET, each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the back end. The traffic control center to adjust traffic lights for avoiding possible traffic congestion. As such, a VANET can also be interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. provide a security analysis and a simulation study to evaluate our scheme. Through the simulation, we find that a query can be completed in a reasonable amount of time. a navigation scheme that utilizes the online road information collected by a VANET to guide the drivers to desired destinations in a real-time and distributed manner. Communication networks, security issues have been widely addressed in VANETs. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol [5] over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications.

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have grown out of the need to support the growing number of wireless products that can now be used in vehicles. These products include remote keyless entry devices, personal digital assistants (PDAs), laptops and mobile telephones. As mobile wireless devices and networks become increasingly important, the demand for Vehicle-to-Vehicle (V2V) and Vehicle- to-Roadside (VRC) or Vehicle-to-Infrastructure (V2I) Communication will continue to grow . VANETs can be utilized for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet

II. LITERATURE SURVEY

Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang presented An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. It propose a security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, non repudiation, message integrity, and confidentiality. It propose a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication .It show the fulfillment and feasibility of our system with respect to the security goals and efficiency.

J.P.H.M. Raya, P. Papadimitratos presented securing vehicular communications. Vehicular networking protocols will allow nodes, that is, vehicles or roadside infrastructure units, to communicate with each other over single or multiple hops. In other words, nodes will act both as end points and routers, with vehicular networks emerging as the first commercial instantiation of the Vehicular ad hoc networking technology. The road to a successful introduction of vehicular communications has to pass through the analysis of potential security threats and the design of a robust security architecture able to cope with these threats.

Yong Hao, Jin Tang presented Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks. It develop an application layer data sharing protocol which coordinates the vehicles to relay data for sharing according to their positions. Such coordinated sharing can avoid collisions in the medium access control (MAC) layer and the hidden terminal issue in multi-hop transmissions. A salient feature of the proposed sharing protocol is that it can guarantee the receipt of the requested data file for each applicant vehicle passing a road side unit. It also address security and privacy issues in the process of data downloading

and sharing, ensuring applicants' exclusive access to the applied data and privacy of the vehicles involved in the application.

Yilin Zhao presented Vehicular Phone Location Determination and Its Impact on Intelligent Transportation Systems. In this paper why locating Vehicular phones becomes a hot topic among telecommunications giants, what technologies are being studied and standardized, when we are going to see the actual deployment, and what services they may provide. It consider its potential impact on future intelligent transportation systems (ITS), including telematics and public transit systems. Many of us have already recognized how important a role the communications systems play in modern transportation.

Zhengming Li, Congyi Liu, and Chunxiao Chigan presented On Secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control. VAAD provides an incentive-centered architecture for the involved parties to trade off their conflicting requirements regarding ad dissemination. Given realistic advertising effect and cost requirements of an SP, VAAD adopts a distance-based gradient ad dissemination algorithm to maximize the achievable ad effect by emulating the ad-posting patterns in the physical world. To facilitate vehicular nodes' participation in VAAD, efficient, secure, and privacy-preserving incentive cash-in is ensured to support financial transactions in VAAD. Thus, with proper cost and effect control, VAAD is a novel and comprehensive solution to secure ad dissemination in VANETs.

G.Danezis presented Statistical Disclosure Attacks: Traffic Confirmation in Open Environments. The statistical disclosure attack is computationally efficient, and the conditions for it to be possible and accurate are much better. The new attack can be generalized easily to a variety of anonymity systems beyond mix networks. It is computationally cheap. Its scales very well. The statistical disclosure attack only relies on collecting observations and performing trivial operations on vectors. Its not solving an NP-completeness problem.

Y. Zhang, W. Liu, W. Lou, and Y. Fang presented MASK: Anonymous OnDemand Routing in Vehicular Ad Hoc Networks. An anonymous on-demand routing protocol, termed MASK, which can accomplish both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes under a rather strong adversary model. MASK offers the anonymity of senders, receivers, and sender-receiver relationships in addition to node unlocatability and untrackability and end-to-end flow untraceability.

Y. Qin and D. Huang presented OLAR: On-Demand Light weight Anonymous Routing in MANETs. OLAR is an identity-free routing scheme, which provides source and destination anonymity, end-to-end communication relation anonymity, as well as route anonymity. This scheme highly decreases the overhead of data transmission, while making packets more untraceable compared to the previous solutions. Some of these are alien nodes, which enter the network during its establishment or operation phase , while others may originate indigenously by compromising an existing benevolent node. These malicious nodes can carry out both Passive and Active attacks against the network.

S. Seys and B. Preneel presented ARM: Anonymous Routing Protocol for Vehicular Ad Hoc Networks. Anonymous on demand routing scheme for MANETs. It identifies a number of problems of previously proposed works and proposes an efficient solution that provides anonymity in a stronger adversary model. It provides stronger anonymity properties while also solving some of the efficiency problems. It does not give the security to the network.

III. SYSTEM ANALYSIS

Routing is the most fundamental aspect for multi-hop MANETs. Unlike the Internet and infrastructure-based wireless networks, MANETs are characterized by the lack of a dedicated routing infrastructure. MANET nodes depend on each other to forward traffic. This requires nodes to forward traffic on behalf of other nodes, which opens the door for selfish behavior. Selfish behavior can significantly degrade performance of routing protocols that assume honest nodes. In addition, MANETs topology undergoes continuous reconfiguration due to the dynamic nature of wireless links and node mobility. Most of these protocols can be classified as follows:

A. Proactive Routing

In proactive routing protocols nodes periodically exchange routing control messages and establish routes to all other nodes. Proactive routing can be implemented based on either: (1) link-state or (2) distance-vector.

1) *Link-State:* In link-state routing nodes periodically use "HELLO" and "TOPOLOGY CONTROL (TC)" messages to discover and disseminate learned information about node connectivity. This information describes the state of links

connecting different nodes. Each node, S, periodically broadcasts a "HELLO" message. Every one hop neighbor of S responds thus informing S they are neighbors. S then generates and broadcasts a TC message, which is flooded throughout the network. TC messages inform other nodes about the connectivity between S and its immediate neighbors. They allow each node to construct a network map and compute the next hop, or the entire path, to all destinations. This can be easily achieved using the Dijkstra shortest path algorithm. Routes (or next hops) to all destinations are pre-computed even if no communication will take place. This is useful for delay-sensitive applications because there is no delay associated with discovering a new route to a specific destination. Open Shortest Path First (OSPF) is an example of a link-state routing protocol that is used on the Internet. OLSR is a link-state based routing protocol tailored for MANETs with the goal of minimizing overhead of flooding topology information. Nodes running OLSR use "HELLO" messages to find one-hop and two-hop neighbors. OLSR allows nodes to perform a distributed election of a set of Multipoint Relays (MPRs). Nodes select MPRs such that there exists a path to each of their two-hop neighbors via an MPR.

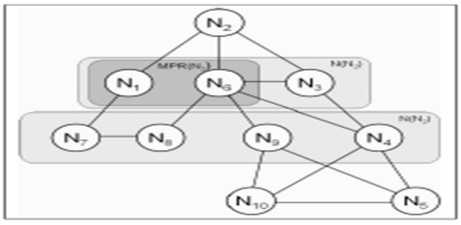


Figure 3.2: Example of OLSR MPR Selection

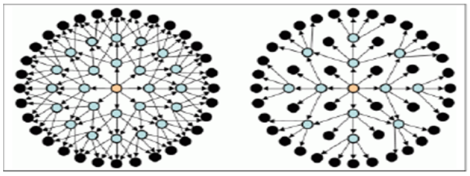


Figure 3.3: OLSR MPR Flooding Vs Blind Flooding

Despite being the best link-state based MANET routing protocol in terms of minimizing routing control overhead, OLSR has the following shortcomings:

a) In sparse networks, every neighbor of a node becomes an MPR. This reduces OLSR to a pure flooding-based link-state protocol.

b) OLSR does not include any mechanism for sensing and describing link quality. It assumes that a wireless link is up if more than a certain number of "HELLO" messages have been received during a certain period.

c) OLSR assumes link-states to be binary, either up or down. This is typically not the case in wireless networks where links often exhibit intermediate loss rates.

d) OLSR uses power and network resources in order to propagate data about possibly unused routes. This has been shown to work well and scale up to large scale MANETs in order of thousands of nodes with the OLSR implementation. However, OLSR is inefficient for larger-scale sensor networks with hundreds of nodes.

e) OLSR only uses MPRs to floods the topology information. This removes some of the redundancy of the flooding process, which may be a problem in wireless networks with medium to high loss rates.

2) *Distance-Vector:* In distance-vector, nodes periodically construct and broadcast routing tables containing the reachable destinations and the number of hops to reach them, or some other cost metric. Nodes continuously update their own routing tables based on tables they receive from their neighbors. A distributed variant of Bellman-Ford algorithm is at the core of most distance-vector routing protocols. The main disadvantages of distributed Bellman-Ford algorithm are:

a) It does not scale well.
b) Changes in network topology are not reflected quickly because updates are spread node-by-node.
c) The count to infinity problem.

Destination-Sequenced Distance Vector Routing (DSDV) is an adaptation of the distributed distance-vector routing protocol for MANETs. DSDV's main feature is that it is loop-free. Each node periodically broadcasts a new sequence number. This number has to be included in routing table entries in which the corresponding node is the destination. This prevents loops and ensures freshness of routes. Routing information is distributed by sending full routing tables infrequently and smaller incremental

updates more frequently. A node's routing table contains a description of all reachable destinations, along with the next hop, number of hops and the latest destination sequence number.

B. Reactive Routing

In bandwidth and power-limited environments, it is desirable to minimize routing control traffic when there is no data to be routed. Proactive routing is not particularly suitable for such settings. This is the main motivation behind reactive routing, also called on-demand routing. Such protocols do not maintain routes, but build them on-demand when communication to a certain destination is required. For example, the Ad-hoc On demand Distance Vector (AODV) protocol is a reactive adaptation of distance-vector. Other notable reactive protocols include Dynamic Source Routing (DSR).

C. Geographical Routing

In Geographical routing, also called geographic routing or geo routing, nodes rely on position information to forward traffic from a source to a destination. The main idea is that the source sends a message to a destination's geographic location, instead of its network address. This requires each node to determine its own location, and the source to be able to deduce that of the destination. A message can be routed based on the geographic destination, without knowledge of the network topology, or prior route discovery. A number of position-based routing protocols were developed in recent years. We concentrate on loop-free, localized protocols that utilize single-path strategy. Most single-path strategies rely on two techniques: Greedy forwarding and Face routing. The former progressively forwards the message closer to the destination relying only on local information. Each node forwards the message to a neighbor that is considered most suitable from a local point of view. This neighbor can be the one with the minimum distance to a destination. Alternatively, other measures of progress can be considered, e.g., the projected distance on the source-destination-line, or the minimum angle between neighbor and destination. Not all of these strategies are loop-free, i.e., a message can circulate among nodes in a certain constellation. Different cost metrics can also be used, e.g., hop count, power and congestion. Greedy forwarding can lead to a dead end, where no neighbor is closer to the destination. In such cases, a recovery strategy such as face routing is used to find a path to another node, from which greedy forwarding can be resumed. In face routing a message is routed along the interior of the faces in the communication graph. The face changes at edges crossing the imaginary line connecting the source and destination. A recovery strategy such as face routing is necessary to assure that a message can be delivered to the destination. Figure 1.4 shows an example of face routing with a source node (S) and a destination node (D). The face edges are highlighted in red and are not used for routing the route between S and D is highlighted in blue.

D. Objective

The main objective of this project is to improve the scalability parameters of the Vehicular Adhoc Networks. To achieve a better route and at the same time, and improve the scalable property for large area network communication. So, VANET-based secure and privacy-preserving navigation scheme are proposed in this paper.

IV. REQUIREMENTS ANALYSIS

A. Hardware Specification

Processor : IntelPentium IV
Processor Speed: 1.4 GHz
Memory (RAM): Default
Hard disk : Default
Monitor : Default
Input Device : Keyboard (104)

B. Software Specification

Operating System: Ubuntu 10.04
Simulator Tool : NS 2.34
Language : TCL
Protocol Design : C++
Platform : Independent

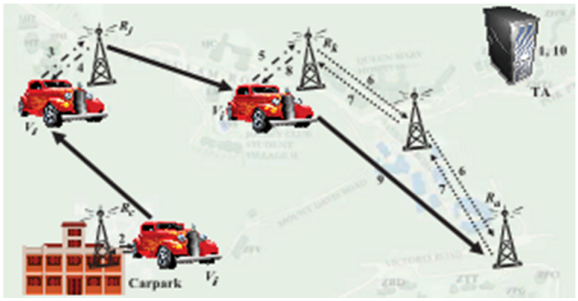
V. RESULT AND DISCUSSIONS

This section presents a comparative analysis of the performance metrics generated with the employment of the use of Network Simulator 2.34. Performance metrics that have been proposed for the performance evaluation of an ad-hoc network protocol. The following metrics are applied to comparing the protocol performance. Some of these metrics are

suggested by the VANET working group for routing protocol evaluation.

A. Simulation Parameters

Tested Protocol	:	AODV
Propagation Model	:	Drop Tail
Type of Antenna	:	Omni directional
Power Threshold	:	-95dBm
Time	:	100seconds
Area (m x m)	:	500*500
Number of Nodes	:	50
Number of Packets:		30
Travel Type	:	TCP/IP
Pause Time	:	50 seconds
Clock speed	:	11Mbps

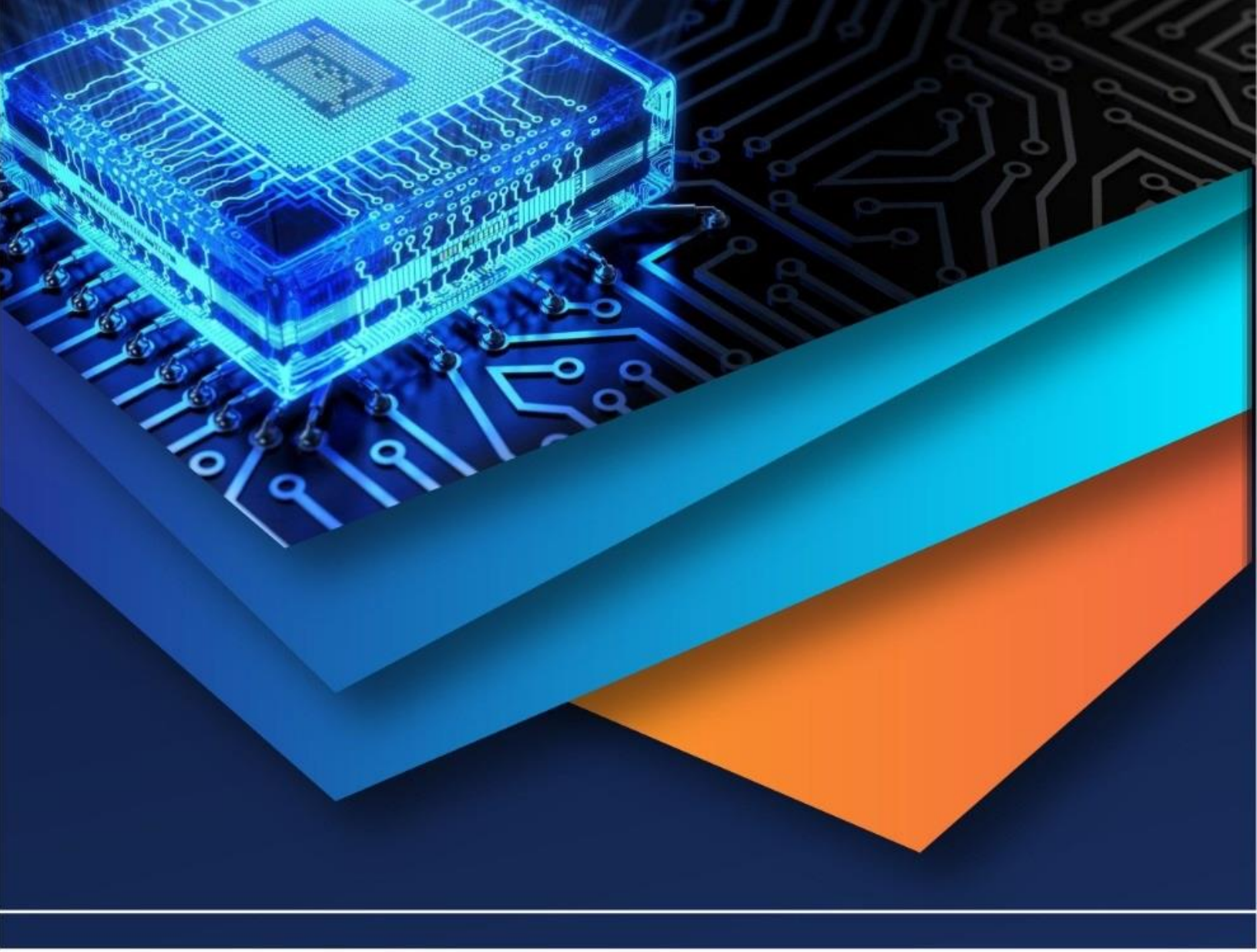


VI. CONCLUSION

A vehicular ad hoc network (VANET) uses cars as Vehicular nodes in a MANET to create a Vehicular network.It is an important element of the Intelligent Transportation Systems (ITSs).In a typical VANET, each vehicle is assumed to have an onboard unit (OBU) and there are road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the backend. A VANET can also be interpreted as a sensor network because the traffic control center or some other central servers can collect lots of useful information about road conditions from vehicles. It is natural to investigate how to utilize the collected real-time road conditions to provide useful applications. A new application—VANET based secure and privacy-preserving navigation (VSPN),which makes use of the collected data to provide navigation service to drivers.We utilized speed data and road conditions collected by RSUs to guide vehicles to desired destinations in a distributed manner.The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. However, such a centralized approach is not scalable, especially for large cities. VSPN scheme on a test bed to further verify its performance is implemented.

REFERENCES

[1] F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing,vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.
[2] H. Oh, C. Yae, D. Ahn, and H. Cho, "5.8 GHz DSRC Packet Communication System for ITS Services,"Proc. IEEE VTS 50th Vehicular Technology Conf. (VTC '99),pp. 2223-2227, Sept. 1999.
[3] I. Leontiadis, P. Costa, and C. Mascolo, "Extending Access Point Connectivity through Opportunistic Routing in Vehicular Networks,"Proc. IEEE INFOCOM '10,Mar. 2010.
[4] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks,"Proc. IEEE INFOCOM '08,pp. 816-824, Apr. 2008.
[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots,"Proc. IEEE INFOCOM '09,pp. 1413-1421, Apr. 2009.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY