International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1		**VOL**	02
Website	icssccet.org		**eMail**	icssccet@asdf.res.in
Received	25 – February – 2016		**Accepted**	10 - March – 2016
Article ID	ICSSCCET133		**eAID**	ICSSCCET.2016.133

Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET

H Indrapriyadarsini[1], T G RamaBharathi[2]
Assistant Professor, [1,2]Karpagam Institute of Technology, Coimbatore.

Abstract: *Vehicular Ad Hoc Networks (VANETs) are classified as a subset of Mobile Ad Hoc Networks (MANETs). VANETs have the potential of improving road safety and providing travelers comfort. This network rehearses moving cars as nodes in a network to create a mobile network. Intelligent Transportation System (ITS) enables coordinated traffic management, like advanced traveler information services, Vehicle tracking and Autonomous vehicle safety audits etc. In VANET vehicles are used as nodes which transmit and receive messages by using the wireless VANET based applications on the intelligent transportation system. In ITS vehicles are equipped with on board unit (OBU), application unit (AU), advanced mobile devices such as iPhone and other types of sensors.*

I. INTRODUCTION

VANET turns every participating car as network router. VANET provides wireless communication between moving vehicles using a dedicated short range communication (DSRC)

Wireless access in vehicular environments (WAVE) referred by the IEEE to standardize the whole communication now. VANET also integrates different technologies such as WAVE IEEE 1609, WiMAX.

The number of vehicles owned by people is rapidly growing with the development of economy and society. The safety problem in transportation is increasingly outstanding. It brings a serious threat to humans' life and property. As we all known, safe-driving is always one of the most important topics in vehicle engineering. In order to reduce traffic accidents, the intelligent vehicle emerges as the times require. It is a combination of multiple academic subjects and latest technologies, representing the developing tendency of future automobile technology. Therefore, it attracts more and more attention. With the fast development in ad hoc wireless communications and vehicular technology, it is foreseeable. A distributed network of vehicles such as a vehicular ad hoc network (VANET) can easily turn into an infrastructure-less self-organizing traffic information system, where any vehicle can participate in collecting and reporting useful traffic information.

II. Related Works

S. Palaniswamy, A. Rajaraman, A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks (IJCSIS) International Journal of Computer Science and Information Security. Blum J, Eskandarian A, Hoffman L. Challenges of intervehicle ad hoc networks. C.C. Communication Consortium. Car 2 car communication consortium manifesto. Jakubiak J, Koucheryavy Y.: State of the art and research challenges for vanets. Luo J, Hubaux J-P.: A survey of inter-vehicle communication. Adi Shamir, of RSA notoriety, introduced the concept of identity-based cryptography. Its primary innovation was its use of user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification Farhan Aadil, Vehicular

Cite this article as: H Indrapriyadarsini, T G RamaBharathi. "Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 660-664. Print.

Ad Hoc Networks (VANETs) are classified as a subset of Mobile Ad Hoc Networks (MANETs). VANETs have the potential of improving road safety and providing travelers comfort.

Shahzad Rizwan, Intelligent Transportation System (ITS) enables coordinated traffic management, like advanced traveler information services, Vehicle tracking and Autonomous vehicle safety audits etc. In this research paper we tried to pre-sent a thorough survey of VANETs

III. Existing Works

The main idea of this class of routing, which we call road-based using vehicular traffic (RBVT) routing. The RBVT class of routing presents two main advantages:

1) Adaptability to network conditions by incorporating realtime vehicular traffic information and
2) Route stability through road-based routes and geographical forwarding. We present two RBVT protocols:
   2.1. A reactive protocol RBVT-R and
   2.2. A proactive protocol RBVT-P.

RBVT-R discovers routes on demand and reports them back to the source, which includes them in the packet headers (i.e., source routing). RBVT-P generates periodical connectivity packets (CPs) 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. Our initial NS-2 simulations with an IEEE 802.11 VANET showed that, when the wireless medium becomes congested, the overhead introduced by the periodic "hello" packets for maintaining the list of neighbors in geographical forwarding significantly degraded the end-to-end data transfer performance. To reduce this overhead, we propose a beaconless distributed receiver-based election of next hop, considering non-uniform radio propagation. This method uses a light modification of the request-to-send/clear-to-send (RTS/CTS) mechanism in the IEEE 802.11 standard. A multicriterion prioritization function is introduced to select the best next hop by using the distance between the next hop and the destination, the received power level (which could be affected by noise and channel fading), and the distance to the transmitter as parameters. We evaluate the performance of the proposed protocols using two scenarios: 1) an urban environment with obstacles using periodic "hello" messages and the standard 802.11 medium access control (MAC) protocol (node movements are generated using the open-source microscopic traffic generator simulation of urban mobility (SUMO), which has been validated against real vehicular traces) and 2) an urban environment without obstacles, using the proposed forwarding optimization for the RBVT protocols. This scenario tests the protocols in high-contention environments. In these tests, we used a vehicular traffic generator that we developed based on the car following model proposed by Gipps. This model enables vehicles to move at the maximum safest speed while avoiding collisions. The simulation results show that the RBVT protocols outperform existing protocols in both studied scenarios. In terms of successful data delivery, RBVT-R performed best, with an increase of as much as 40% compared with AODV and 30% compared with GSR using the IEEE 802.11 standard. In terms of the average delay, RBVT- P performed best, with delays of as much as 85% lower than existing solutions. The proposed forwarding optimization provided noticeable improvements in the high-contention scenario. The scenario with obstacles yielded better performance, even without using the optimization. This case was the result of lower contention in the network and the fact that RBVT protocols forward data along the roads and not across the roads.

4. Proposed Works

A. On Board Unit (OBU)

An OBU is a wave device usually mounted on-board a vehicle used for ex-changing information with RSUs or with other OBUs. It consists of a Resource Command Processor (RCP), and resources include a read/write memory used to store and retrieve information, a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology. It may additionally include another network device for non-safety applications based on other radio technologies such as IEEE 802.11a/b/g/n. These devices connected through wireless link based on the IEEE 802.11p radio frequency channel. The main functions of the OBU are wireless radio access, ad hoc and geo-graphical routing, network congestion control, reliable message transfer, data security and IP mobility.

A. Application Unit (AU)

The AU is the device equipped within the vehicle that uses the applications provided by the provider using the communication capabilities of the OBU. The AU can be a dedicated device for safety applications or a normal device such as a personal digital assistant (PDA) to run the Internet, the AU can be connected to the OBU through a wired or wireless connection and may re-side with the OBU in a single physical unit; the distinction between the AU and the OBU is logical. The AU communicates with the network solely via the OBU which takes responsibility for all mobility and networking functions.

Cite this article as: H Indrapriyadarsini, T G RamaBharathi. "Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 660-664. Print.

A. Wireless Access Technology in VANET

Wireless technology that used in VANET provide radio interface, some of these technologies rely on a centralized infrastructure to coordinate the communications between nodes. In contrast, other technologies operate in ad hoc mode (distributed coordination).

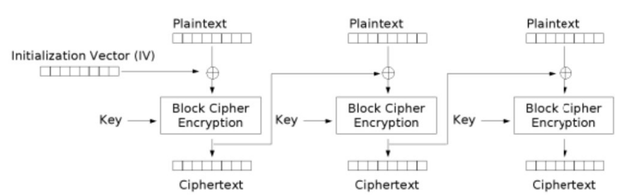
WLAN/Wi-Fi: Wireless local area network (WLAN) or wireless fidelity (Wi-Fi) can provide wireless access to enable V2V communication or V2I communication. IEEE 802.11 standard can be applied to provide wireless connectivity. IEEE 802.11a works at 5 GHz and provides a data rate of 54 Mbps with a communication range of at least 38 m indoor and a 140 m range for outdoor use.

B. Proposed Authentication Protocol

We propose a Trust based packet forwarding scheme in VANETs without using any centralized infrastructure. It uses trust values to favour packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. Each intermediate node marks the packets by adding its hash value and forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, otherwise it is decremented. If the trust counter value falls below a trust threshold, the corresponding the intermediate node is marked as malicious. This scheme presents a solution to node selfishness without requiring any pre-deployed infrastructure. It is independent of any underlying routing protocol. We focus on the CBC-X mode Encryption/Decryption algorithm to satisfy the necessity of minimum computational and communication overhead. This algorithm supports encryption/decryption and authentication of packets on a one pass operation. The upper layers of the protocol stack are provided with security services obviously.

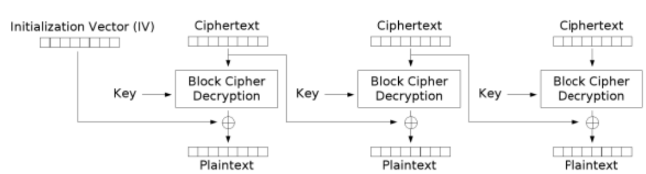
A CBC-X mode symmetric key mechanism is devised to employ our link layer security system. Encryption/Decryption and authentication operations are included into a single step which reduces the computational overhead to half, instead of calculating them individually. The padding technique states that this method has no cipher text expansion for the transmitted data payload. Thus the communication overhead is reduced significantly.

CBC-X Mode Operations



Cipher Block Chaining (CBC) mode encryption

Encryption



Cipher Block Chaining (CBC) mode decryption

Decryption

The basic steps involved in the encryption and decryption operations are illustrated in figure 3.2 and figure 3.3 , respectively. If the first block has index 1, the formula for CBC encryption is

Ci EK Pi Ci C IV = Å = (−1), 0
while the formula for CBC decryption is
Pi DK Ci Ci C IV = Å = ( ) −1), 0

Cite this article as: H Indrapriyadarsini, T G RamaBharathi. "Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 660-664. Print.

The working of the present CBC mode is described below:

One cipher text block will be returned for each plaintext block, if a part of the plaintext is encrypted. In encryption of the last block of the plaintext, one or two cipher text blocks can be returned. On the other hand, decryption works in the reverse order. Apart from the decryption of the last block, a one plaintext block will be returned for each cipher text block. After the decryption of the last plaintext block, its padding is calculated and cut off, returning a valid plaintext.

Challenges and requirements in VANET

- Signal fading
- Bandwidth limitations
- Connectivity
- Privacy issue
- Routing protocol

C. Protocols used

It is a critical challenge to design an efficient protocol that can deliver a packet in minimum period of time. However many researchers have concentrated on designing routing protocol suitable for dense environment that have a high density of vehicle with close distance between them .

4.1.1 Dynamic Source Routing Protocol

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets.

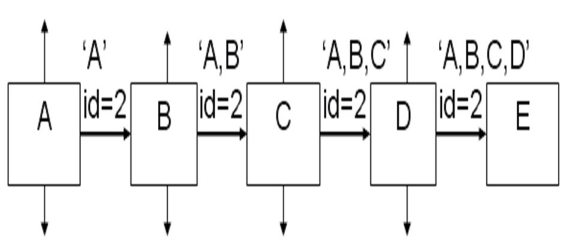
Compared to other reactive routing protocols like ABR or SSA, DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence.

DSR was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only move around at a moderate speed.

DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding.

DSR contains 2 phases

- Route Discovery (find a path)
- Route Maintenance (maintain a path)
- Route Discovery



If node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started:

Cite this article as: H Indrapriyadarsini, T G RamaBharathi. "Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 660-664. Print.

1) Node A (initiator) sends a Route Request packet by flooding the network
2) If node B has recently seen another Route Request from the same target or if the address of node B is already listed in the Route Record, Then node B discards the request!
3) If node B is the target of the Route Discovery, it returns a Route Reply to the initiator. The Route Reply contains a list of the "best" path from the initiator to the target..
4) Otherwise node B isn't the target and it forwards the Route Request to his neighbours (except to the initiator).

IV. Conclusion

In this project, we have presented an in-depth study of Vehicle Tracking Mechanism in a Vehicular AdHoc environment. We have integrated authentication to the vehicles using Trust Based packet forwarding scheme. Geographical forwarding was used to find forwarding nodes along the road segments that form these paths. To improve the end-to-end performance under high contention, we have also proposed a distributed next-hop self-election mechanism for geographical forwarding. For this project to be completely successful, the entire participating vehicles must be equipped with this technology.

V. Future Work

The future of automobile technology is the Unmanned Cars whose development is under process. Integration of GPS to this project can contribute so much to those unmanned vehicles.

A vehicle which is not equipped with this technology can be detected with the use of sensors around the vehicle. Thus the drivers would be aware of the vehicles and objects around them and ensures safe driving.

VI. Reference

1. Blum J, Eskandarian A, Hoffman L. Challenges of intervehicle ad hoc networks. IEEE Transactions on Intelligent Transportation Systems;5(4):347–51 (2004)
2. C.C. Communication Consortium. Car 2 car communication consortium manifesto. ⟨http://car-to-car.org/ index. php?id=31⟩
3. Chen W, Guha R, Kwon T, Lee J, Hsu Y.: A survey and challenges in routing and data dis-semination in vehicular ad hoc networks. Wireless Communications and Mobile Compu-ting;11(7):787–95 (2011)
4. Faezipour M, Nourani M, Saeed A, Addepalli S. Progress and challenges in intelligent vehicle area networks. Communications of the ACM;55(2):90–100 (2012)
5. Global Mobile Information System Simulation glomosim. ⟨http://pcl.cs.ucla.edu/ projects/glomosim/⟩
6. S. Palaniswamy, A. Rajaraman, A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009

Cite this article as: H Indrapriyadarsini, T G RamaBharathi. "Intelligent Transportation System in Vehicle Tracking Mechanism Using VANET". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 660-664. Print.