Middle-East Journal of Scientific Research 24 (S1): 167-172, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S1.34

Intelligent Transportation Systems Utilizing Self Organizing MAC Protocol

[1]M.K. Arul Jothy and [2]Mr. D. Murugesan

[1]PG Scholar, Valliammai Engineering College, Kattankulathur, India
[2]Assistant Professor, Valliammai Engineering College, Kattankulathur, India

Abstract: This paper presents a STDMA access technique with real-time global path-planning algorithm for autonomous systems in order to avoid the vehicles from congestion. The main advantage of this algorithm is to enhance the system autonomy as well as the behavior with increase of efficiency of transportation systems. In addition, it supports the variations in spectrum occupancy such as vehicles joining or leaving the company. Hence it can be adapted to any application. The network spatial utilization and vehicle travel cost are considered by this algorithm to balance the network smoothness and the drivers' preferences. More importantly, the timeliness of data collection and dissemination are enhanced by RSUs in VANETs, which makes it possible to perform coordinated path planning for a group of vehicles. Generally it presents a generic, self-organized and scheduled medium access control mechanism. The traffic signal controller reduces the traffic congestion and also detects the position forging attacks occurring on VANET thereby providing security to passengers. We will randomly changes secret key of each vehicles while entering from one network to other network based on fast randomized algorithm. Server assigns the master key of the emergency vehicle, it gives high priority to emergency vehicles in network to network movement base on checking the master key.

Key words: STDMA · RSU · Secrete Key · VANET

INTRODUCTION

The emerging field of cognitive radio (CR) networks is to alleviate the problem of spectrum shortage by transmitting on other vacant portions of the spectrum. The emerging technology of ITS has more attentions in cooperating safety systems for vehicles In order to avoid the road side accidents the self scheduled access control in VANET is preferred by access technique STDMA which enables various users to make safer and smarter. The recent interest in Intelligent Transportation System (ITS) has lead to rapid increase in the number of vehicular applications such as Traffic safety application, Variable speed limits, Collision avoidance systems, Dynamic traffic light sequence etc [1]. Accordingly, the FCC has allocated 75 MHz of spectrum in the 5.9 GHz band for WAVE. The IEEE 802.11p spectrum band is divided into seven 1 MHz channels as, consists of one control channel (CCH) which is assigned for safety and control message and six service channels (SCHs) for both safety and non-safety usage. The participating device should monitor the CCH where the high priority control and safety messages are transmitted. In vehicular ad-hoc networks (VANETs), devices typically travel along different paths at different speeds. As the result, the propagation channel changes rapidly due to the relative motion between transmitter and receiver. it is proved that the channel condition in vehicular communication is highly dynamic.

The need of the media access control (MAC) is to improve the probability of successful transmission by resolving contention among all users and to estimate the dynamic channel condition [4]. Duration between the time when SCH is selected and when SCH is used for communication is too long compared with the short channel coherence time in vehicular environments. Hence the channel information used for selecting the SCH may be stale at the time for actual data transmission. In this paper, we present Cognitive MAC for VANET with access technique such as STDMA. Cognitive MAC for VANET splits the spectrum access at both long-term and short-term time scales. In long-term spectrum access, the MAC capacity is enhanced via concurrent transmission using cognitive radio technology.

Corresponding Author: M.K. Arul Jothy, PG Scholar,
Valliammai Engineering College, Kattankulathur, India.

Meanwhile in short-term spectrum access, the multi-user diversity is employed by wideband spectrum pooling method.

First, we employ cognitive radio and MAC protocol with STDMA access technique to fit the self-organization with wireless environments. It achieves both goals of avoiding the vehicles from congestion in an urban environment and to enhance the timeliness of data collection and dissemination. Second, we present details of the traffic signal controller which reduces the traffic congestion and also detects the position forging attacks thereby providing security to passengers [2]. We will randomly changes secret key of each vehicles while entering from one network to other network based on fast randomized algorithm. and evaluate through analysis and simulations.

System Module

STDMA: IEEE802.11p is the standard which provides the protocol to support the safety application for the VANET communication. It includes the improvement to the Physical layer (PHY) and Medium Access Control (MAC) for the support of ITS. Thi includes communication links between vehicles and with a roadside infrastructure [3]. The current MAC method uses randomized algorithm and It is known that delays limits the value of safety-related services. The most effective effort is to design a MAC protocol that suits vehicular traffic and safety-related service constraints. Self-Organizing Time Division Multiple Access (STDMA) is a suitable alternative, this structured channel access, predictable delay and self-organizing character [10]. This design were acquired during a real-world experiment in the 5.9 GHz band.

Security: Security plays an essential role in VANET for assessing information assurance, improving defense accountability and predicting protection effectiveness. The main purpose is to explore secure data transmission option that are available to help meet regulatory and legal requirements. This architecture which includes the adhoc network for the intelligent transportation communication which includes the Road Terminal Unit, Road Side Unit and the On Board Equipment. The RTU is the microprocessor device that interfaces object to distributed control system by sending the telemetry messages to master to master system to objects [4]. RSU is the common node used to provide safety warning. A RSE communicates with vehicles' On-Board Equipments (sporadically in ad-hoc mode. OBEs communicate among themselves also in ad-hoc mode. An OBE contains OBD a set of sensors to measure the vehicle's own status such as its brake, GPS to identify its location, Radar to detect other vehicles nearby and Transceiver (TRX) to communicate RSEs and other OBEs. These components feed information to Co-DriverÔ, a special-purpose computer, which monitors road safety and processes travel services. This paper presents the secured communication by detecting the position forging attacks occurring on VANET thereby providing security to passengers. We will randomly changes secret key of each vehicles while entering from one network to other network based on fast randomized algorithm [5]. Server assigns the master key of the emergency vehicle, it gives high priority to emergency vehicles in network to network movement base on checking the master key.

Flow Chart: The flowchart which represents the architecture of the secured Transportation system which includes the RSU as the organizer in the detection of the forgery attackers in the intelligent transportation systems.RSU which distributes the master key to the Registered vehicle. At first the vehicles are registered with particular ID and then it receives the master key based on the randomized algorithm. These master keys are not same as for all networks. It will change automatically for every entrance of the new networks to travel through. if the attacker abuse the car they will be identified by their mismatched key. The RSU identify and show that it is a mismatched key if the verification show that it is matched key then it allows the user to proceed further the travel. To know the master key the owner have the own registered ID. Finally the forgery attack is detected. These proposed algorithm is used by the access techniques STDMA to provide the improved system.

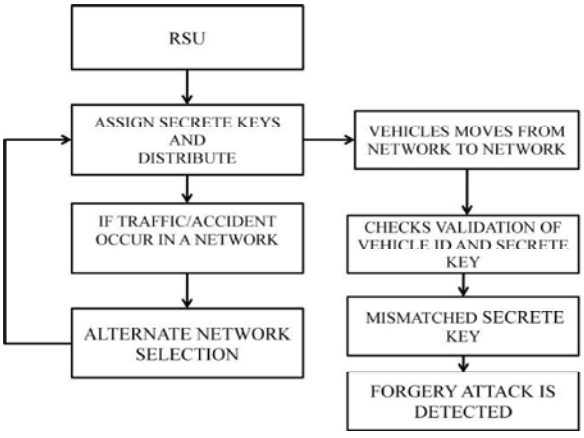

Fig. 1: The architecture of the secured Transportation system

Performance Evolution

Performance Measures: This section derives the performance measures as throughput, delay, packet delivered ratio, period, channel access delay and efficiency.

Throughput: Throughput is the number of useful bits per unit of time forwarded by the network from source address to destination, excluding protocol overhead and excluding retransmitted data packets.

Throughput = (No of packets received)/(simulation time)

Delay: It is defined as the average time taken by the packet to reach the server node from the client node.

Delay = (No of packets send)/(simulation time)

Packet Delivery Ratio: Packet Delivery Ratio is defined as the average ratio of the number of data packets received by each receiver over the number of data packets sent by the source.

Packet Delivery Ratio = No of packets collected by the receiver / Total No of packets send

Efficiency: Forwarding efficiency is the total number of data packets transmitted by any node in the network, divided by the total number of packets received by all the receivers.

Efficiency=100*(No of packets Received) /(No of packets send)

Period: The period is defined by the following expression

TP =1/F uprate of the position message. The transmitter will receive the channel access request for every TP seconds by the MAC layer.

RESULTS AND DISCUSSION

Scenario 1: This Figure represents the broadcasting of the vehicles to show their presence to the network.

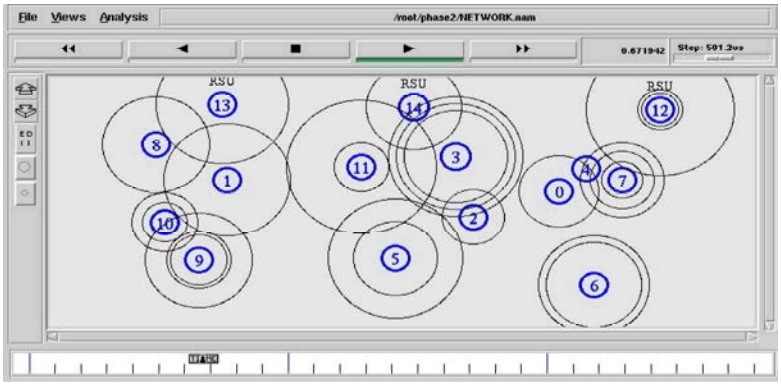

Fig. 2: Broadcasting of the vehicles

Scenario 2: This Fig shows the distribution of the master key to the user with their registered ID.

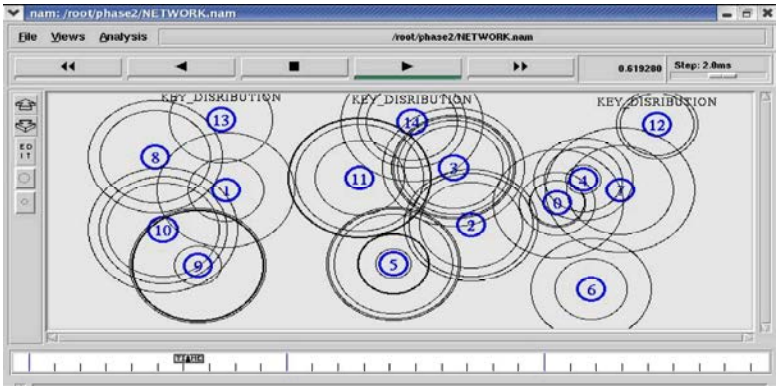

Fig. 3: Distribution of the Master key

Scenario 3: This Fig shows the distributed key to the corresponding users based on the travelling network. The master key is changed for every new entry of the network. If the entered key is wrong then the RSU display this car is forgery by someone by Mismatched Key.

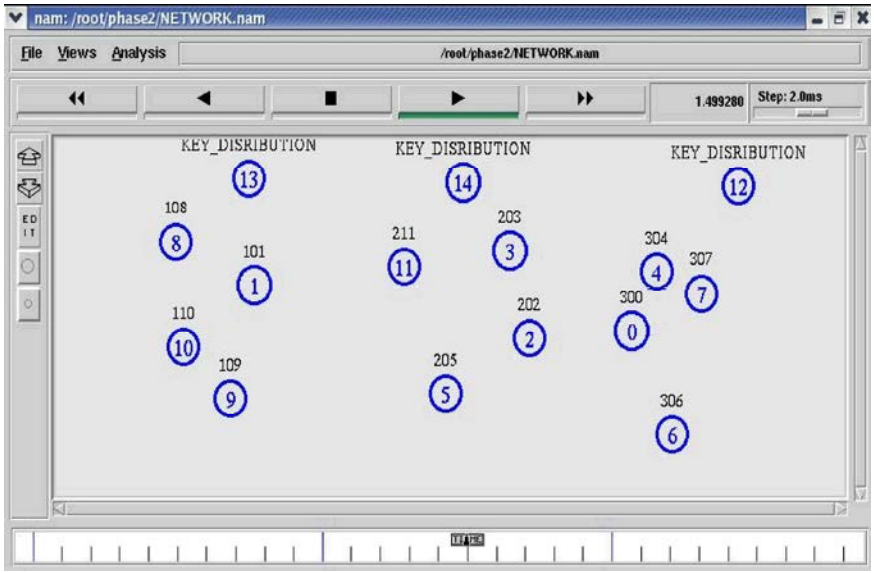

Fig. 4: Distributed key

Scenario 4: This Fig shows the identified forgery attacker with mismatched key and also it finds the matched key by the user.

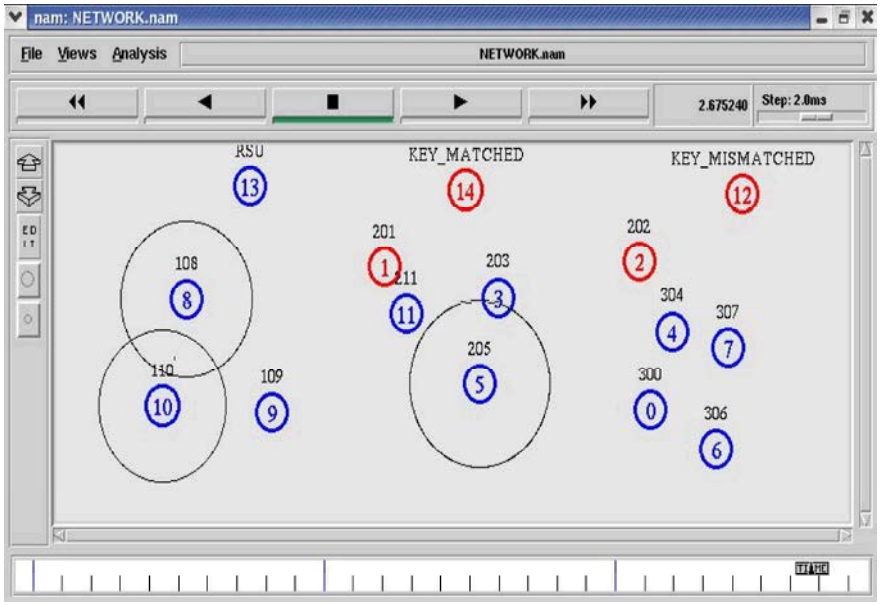

Fig 5. Identification of attacker

Simulated Graph: The simulation results which includes the prametres as the Throughput, Delay and Packet Delivered Ratio. The first graph shows the throughput increases consistently till the packet transmission take place and then it maintain linearly.

Fig. 6: Throughput

This graph shows that the number of data packets received by each receiver over the number of data packets sent by the source is increased and the delay. This shows that the system is efficient.

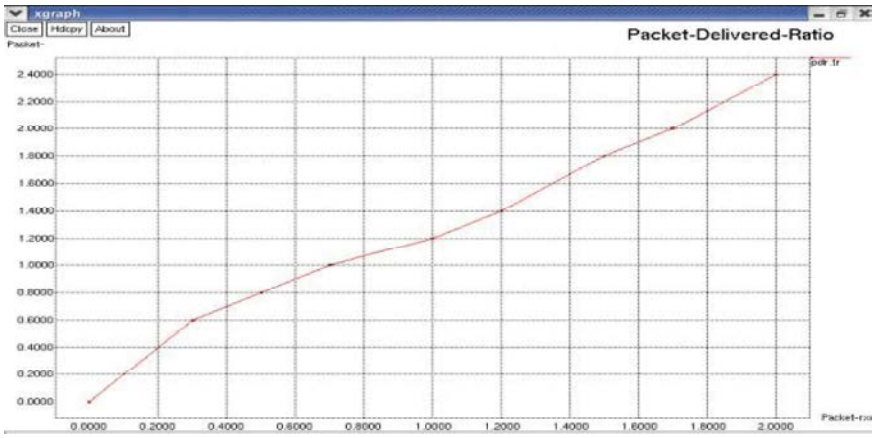

Fig. 7: Packet Delivered Ratio

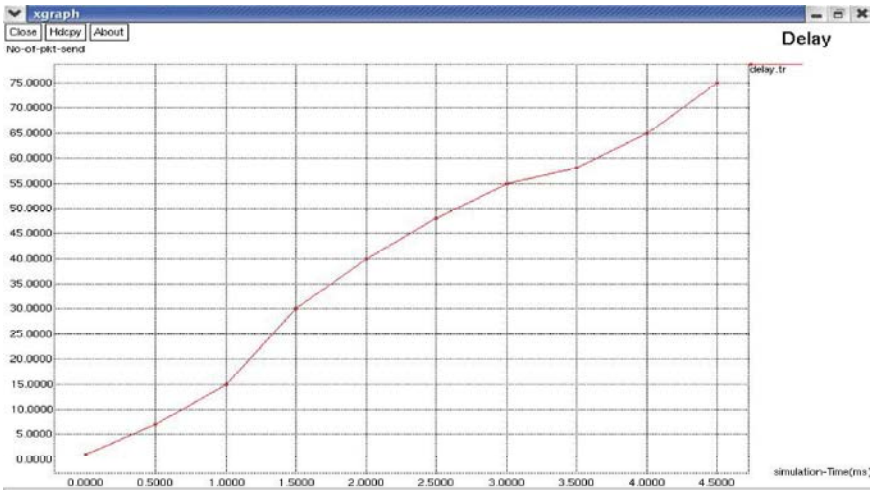

Fig. 8: Delay

CONCLUSION

The proposed system utilized the STDMA access technique with the combination of MAC protocol CR techniques to fulfill the requirements of intelligent transportation systems. The purpose of cognitive radio (CR) networks is to alleviate the problem of spectrum shortage by transmitting on vacant portions of the spectrum in CR platform. By having the analysis and simulation result, it is concluded that this mechanism fulfill the requirements of real time communication with improved throughput and less channel access delay because of the self-organizing nature of the STDMA. The main advantage of this algorithm is to avoid vehicles from congestion in an urban environment and to enhance the timeliness of data collection and dissemination by combining the STDMA with MAC and CR platform with increase of efficiency of transportation systems. As well it supports the variations in spectrum occupancy such as vehicles joining or leaving the company. Hence it can be adapted to any application. Effectively it presents self-organized intelligent medium access control mechanism. Since STDMA does not require slot synchronization and position information to function.

REFERENCES

1. Onieva, E., J. Alonso, J. P ´erez, V. Milan ´es and T. de Pedro, 2009. Autonomous car fuzzy control modeled by iterative genetic algorithms, ? in Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE ’09), pp: 1615- 1620, Jeju Island, Republic of Korea, August 2009.
2. Morgan, Y.L., 2010. Notes on DSRC and WAVE standards suite: its architecture, design and characteristics,? IEEE Communications Surveys and Tutorials, 12(4): 504-518.
3. Mohammad, S.A., A. Rasheed and A. Qayyum, 2011. VANET architectures and protocols stacks: a survey,? in Communication Technologies for Vehicles, vol. 6596 of Lecture Notes in Computer Science, pp: 95-105, Springer, 2011.
4. Manzano, M., F. Espinosa, A.M. Bravo-Santos, E. Santiso, I. Bravo and D. Garcia, 2013. Dynamic cognitive self-organized TDMA for medium access control in real time vehicle to vehicle communications,? Mathematical Problems in Engineering, 2013, Article ID 574528, pp: 13.
5. IEEE802. 11p. Standard for Information technology- Telecommunications and information exchange between systems-Local and metropolitan area networks-Speciic requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speciications. Amendment 6: Wireless Access in Vehicular Environment?.