International Journal of Advances in Engineering, 2015, 1(1), 7-12
ISSN: 2394-9260 (printed version); ISSN: 2394-9279 (online version)
url:http://www.venuspublications.com/ijae.html

RESEARCH ARTICLE

Secured and Prioritized Traffic Signal Control on Vehicular Adhoc Network

L. KARTHIKEYAN
Dept. of Computer Science and Engineering, Valliammai Engineering College, India
vec_karthi@yahoo.in

Received 09 December 2014 / Accepted 09 January 2015

Abstract*—The intelligent adaptive traffic signal controller includes road side sensors to detect the limitation of vehicles which is present or absent in the network coverage area. So it identifies the position of the Vehicles during moving situation only. The Vehicular Ad Hoc Network (VANET) applications work on the principle of periodic exchange of messages between each vehicle. However, a malicious vehicle can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions by creating multiple virtual identities using different forged positions. Now the intelligent adaptive traffic control system is proposed in such a way that a traffic signal controller with wireless sensor receives the information from OBU vehicles such as position and speed. By using this information, it optimizes the traffic signal scheduling at the intersection. Now, the traffic signal controller is designed to reduce the waiting time of the vehicle from the RSU and also it detects the position forging attacks occurring on VANET thereby providing security to passengers by using secret key which changes randomly while travelling from one network to other network. In order to find the alternate path due to traffic jam, the RSU can get the best path by sending request to specific network and will get the required response from that network.

Keywords*—Conflict graphs; online job scheduling; traffic signal control; vehicular ad hoc network (VANET) simulation; Webster's algorithm; Position Forging; Identity Forging; Attack.

I. INTRODUCTION

The current methods of the intelligent and real time adaptive traffic signal control includes roadside sensors, such as loop detectors. The Loop detectors which is physically equipped with the traffic signal controller, can only detect the presence or absence of vehicles [15], [16], which is a serious limitation. This connection is used for the communication between loop detectors and the traffic signal control. The traffic signal controller then uses the data to schedule traffic through the intersection by cycling through preset phases and assigning appropriate amounts of GREEN time or skipping phases altogether. In this paper we analyze the intelligent adaptive traffic signal controller, which receives information from OBU of vehicles, such as the position of vehicle and speed, and uses this information to optimize the traffic signal scheduling at the intersection. This approach is enabled by onboard sensors in vehicles and standard wireless communication protocols specifically for vehicular applications. We also discuss in detail about the position forging attacks in VANET and the attacker behavior that pose high risks to the system. Because the main objective of Vehicular Ad Hoc Networks (VANETs) is to improve vehicle passenger safety by means of inter vehicle communication. For example, in case of a traffic, VANET communication can be used to warn other vehicles approaching the site. Sometimes, a malicious node creates multiple virtual identities and associates forged positions with them. It can disseminate false traffic information in order to force other vehicles and vehicular authorities to take incorrect decisions. For example, a malicious node can misuse safety related applications to clear the path for an aggressive driver to its destination by convincing other vehicles to slow down or speed up on the road. The malicious vehicle forges its identity (sometimes creates multiple virtual identities) and position information to escape its detection.

II. SYSTEM MODEL

In this section, we present a brief description of the VANET and associated communication model.

a) VANET model

VANET consists of two basic components: (1) Road Side Unit (RSU) and (2) On Board Unit (OBU). RSU is a fixed unit while OBUs are installed in vehicles and are moving. Each node in VANET consists of an EDR (Event Data Recorder), GPS (Global Positioning System) receiver, computing platform and a radar. A hierarchy of central authorities (CA) is responsible for managing of vehicles identities registered in its respective geographic region. At the data link layer, dedicated short range communication (DSRC) protocol [18], currently being standardized as IEEE 802.11p is used. It provides transmission range between 250 to 1000m, with data rates in the 6-27Mbps range.

b) Communication Model

In VANETs, both RSUs and vehicles participate in communication. VANET offers three types of communication: (1) In-Vehicle (IV) (2) Vehicle to Vehicle (V2V) and (3) Vehicle to Road side unit (V2R). In-vehicle communication facilitates information to exchange between different components of a vehicle. V2V allows communication between vehicles. It is used for disseminating safety and warning messages in the network. V2V can be categorized into two types depending upon the relative position of sender and receiver: single-hop and multi-hop. Safety messages are sent by local broadcast of vehicles i.e. using single-hop V2V communication. Multihop V2V communication is usually exploited for sending non-safety messages. V2R allows communication between the vehicles and RSUs. It is used to provide facilities e.g Internet access and special service request.

c) Traffic Light Scheduling With Job Scheduling (OJF Algorithm)

Here, we propose a method to reduce traffic signal control problem to the problem of scheduling jobs on processors, and we propose an online job scheduling algorithm called the OJF algorithm. This is phase two of the OAF two-phase traffic signal control algorithm. Fig. 1 shows a typical four-leg intersection with eight traffic movements numbered 1–8.

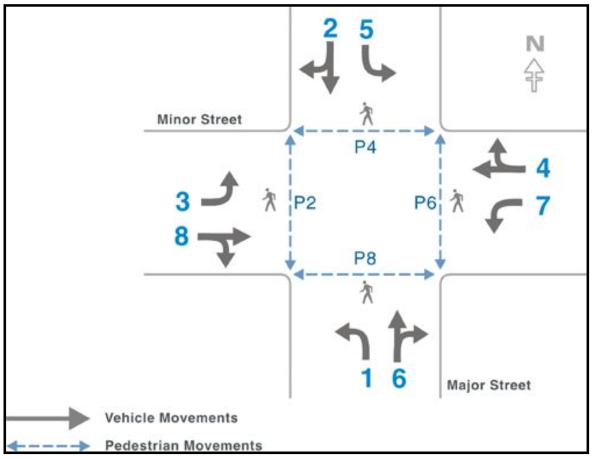

Figure. 1 The four-leg intersection showing the different movements

This type of intersection is the most common and well-studied type [7], [8]. There are conflicts among some of these movements. For example, traffic movements 1 and 2 cannot simultaneously occur. We can reduce the problem of traffic signal control to the scheduling of jobs on a processor, where a job is a platoon of one or more vehicles. We classify jobs as follows. A job is of type *i* if and only if the platoon of vehicles that it represents is part of traffic movement *i*. A pair of jobs of type *i* and *j* are said to be in conflict if the traffic movements *i* and *j* are in conflict; hence, jobs of type *i* and *j* cannot be scheduled to be simultaneously processed. For the intersection in Fig. 1, we can build a conflict graph *G*(*V*,*E*), where *V* is a set of vertices, and *E* is a set of arcs. There is a vertex for each job type. If jobs of type *i*, *j* are in conflict (and cannot be scheduled simultaneously), then there exists an arc (*i, j*) in *E*. *E* does not contain any other arc, and *V* does not contain any other vertex. The conflict graph for the four-leg intersection in Fig. 1 is shown in Fig. 2. Figure. 2 Conflict graph for the intersection in Fig.1

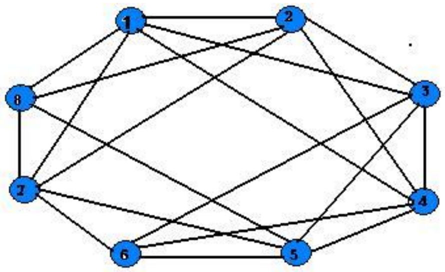

Figure. 2 Conflict graph for the intersection in Fig.1

Conflict graphs have been studied by traffic engineers to build safe traffic signal control plans. In [9], methods of developing safe signal control plans are shown for more complicated traffic intersections.We will assume that jobs, are of equal size, and each job i of type j has an arrival time, which would correspond to the instance of time when the first vehicle of platoon i arrives at the stop line in movement j. We will assume that time is divided into slots, and since all jobs are equal, without loss of generality, we can assume that all jobs need 1 unit of time to complete. Thus, if a job is scheduled at time t, it will complete at time $t + 1$. The ability to divide the oncoming traffic into platoons that require approximately equal amount of GREEN time (the green time represents the amount of processing time required) is achieved using a VANET. At the beginning of time unit t, jobs of any type j can arrive, and we can think of them as arriving at vertex j in G. A group of vertices is chosen that do not conflict, and a job from each of these is scheduled in time t. Now, our objective would be to minimize the maximum latency over all jobs. Therefore, the objective is simply to minimize the maximum latency. In the context of vehicular traffic, minimizing maximum latency is equivalent to minimizing the maximum time that any vehicle spends at rest at an intersection waiting for green light. Consequently, any algorithm that schedules jobs in this setting cannot make any assumptions on the arrival times of jobs and can only schedule jobs that have already arrived at the vertices. Such a type of algorithm is called an online algorithm. In contrast, if an algorithm has prior knowledge of arrival times of all jobs, it might use this information to compute a better schedule. This type of algorithm is called an offline algorithm.

Procedure: Job Scheduling Algorithm

Step-1: Let A1, A2, A3 and A4 be the arrival time of the vehicles.

Step-2: Find the arrival time on each of the vertices of the graph G.

Step-3: If the job is waiting, then find the earliest arrival time among them.

Step-4: S be side of graph. For each vertex v on the side S in G, Schedule the job with the earliest arrival time.

d) Traffic Intersection Control on Vehicular Adhoc Network

Here, we show how we implemented the platooning phase (phase one) of the OAF algorithm and how we implemented the other traffic light control schemes, such as the vehicle actuated logic and Webster's method using VANETs. We first explain some of the terms used in describing our adaptive traffic control algorithms that may differ slightly from their conventional definitions.

III. SYSTEM DESCRIPTION

In this paper, we only study an isolated intersection. Fig. 1 shows the single traffic intersection under consideration. It is a typical four-leg intersection with eight traffic movement groups represented by the arrows. Each of the legs of the intersection is L meters long, and each of the left turning bays is B meters long. The numbered arrows show the directions of the various traffic movements. For this type of traffic intersection, we now describe the system architecture of the VANET-based traffic signal controller. The traffic signal controller is connected to a wireless receiver that is placed at the intersection. The wireless receiver listens to information being broadcast from the vehicles. The broadcast medium is the 5.9–5.95-GHz radio spectrum, and the communication standards are defined in the IEEE 802.11p standards [19]. This system architecture is shown in Fig. 3. The information consists of speed and position data collected from vehicles. Speed data can be gathered from the vehicle speedometers, and position data can be gathered using GPS receivers fitted to the vehicles. In our implementation, the following data are gathered and encapsulated in data packets that are broadcast over the wireless medium. This is what we call the data dissemination phase.

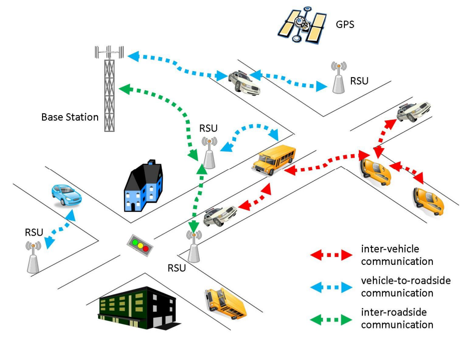
GPS
RSU
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig.3 VANET-based traffic signal control architecture.

- Vehicle ID: Every vehicle is uniquely identified by its Vehicle ID#.
- Speed: Speed of a vehicle is a floating point quantity expressed in meters per second and is obtained from the in-vehicle speedometer sensor.
- Current Time: The time at which the packet was created. The format is (hh:mm:ss). Because of the nature of the traffic control application, there is no need for a finer grain time.

a) Platooning Algorithm

The lower bounds were achieved by an online algorithm that had no knowledge of future inputs. We can estimate the time for a platoon to pass through the intersection as

$$1.5 + h1 + \cdots + hn$$

where the hi values are the headways of the $1 \leq i \leq n$ vehicles in the platoons, and 1.5 is a constant that accounts for the startup delay of the very first vehicle in the platoon. The platooning algorithm is an exhaustive search over all the platoon configurations to determine the platoon combination that minimizes the difference between the maximum and minimum GREEN times.

IV. KINDS OF POSITION FORGING ATTACKS

An attacker may use one or multiple identities (IDs) to launch a position forging attack. An attacker can forge positions using various methods. Positions can be selected or guessed by knowing its own and neighboring nodes' positions. Attacker can spoof the positions of other nodes and uses them at different time intervals. Digital maps provide another method of deriving node positions. If an attacker implements a combination of Position and ID forging attack, multiple virtual identities are used simultaneously for position forging. This makes other vehicles believe that there are more nodes in the network than the actual count. This gives the impression of a state of congestion and may lead to all vehicles slowing down their speed, thereby leading to real congestion.

a) FRPSI (Forging Random Positions using Single ID)

In this position forging attack, an attacker forges its identity for sending any message. The attacker uses this forged identity for sending the same safety message but from random positions. The position forging attack is shown in Figure 4. Numbers 1, 2, ...5 represent time instances at which an attacker node M broadcast messages using forged positions. Node positions connected with solid lines represent the actual path movement at different time intervals. Node positions connected with dotted lines represent the sequence of forged positions used by forged identity of an attacker. This notation is applicable for all forms of position forging attacks. The purpose of this type of attack is to simply broadcast same event information from different positions.

b) FRPMI (Forging Random Positions using Multiple IDs)

An attacker broadcasts fake messages using multiple fake identities from random positions at the same time. To create an illusion of some warning or safety event, an attacker spoofs the identities of other nodes or fabricates identities and uses them simultaneously in the network. The attacker associates random positions with each fabricated node at each time interval. In this attack, the major concern is to choose the appropriate IDs and node positions. The attacker has to consider that no two fabricated nodes broadcast same position at same time. Attacker's effort is proportional to the number of identities used by the attacker.

c) FPSI (Forging Path using Single ID)

In a path-forging attack, the attacker forges its identity to broadcast fake messages using a forged consistent sequence of positions. This attack is intelligent and difficult to detect. The motive of the attacker is to create an illusion that the node is moving normally on a pre-defined path. This attack is successful when the traffic situation does not change. Inconsistent movement paths may be detected based on changes in traffic pattern.

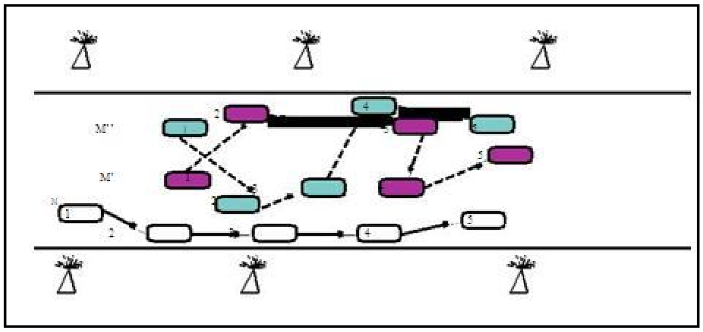

Figure. 4 Attacker M broadcast messages by using random sequence of positions

d) FPMI (Forging Path using Multiple IDs)

In this attack, an attacker creates multiple virtual identities that participate simultaneously in the network with a sequence of positions on the pre-defined path. Simultaneous multiple path forging attacks are carried out in this case. The attacker takes care that same positions are not used by more than one node at the same time. The attacker may forge the whole traffic situation by simulating a majority of vehicles i.e. their positions as well as movement. This type of attacker possesses the highest possibility of passing position and speed consistency checks as it is more careful about the construction of forged paths.

V. CONCLUSION AND FUTURE WORK

In this paper, we have shown how a VANET can be used to aid in traffic signal control, including a new job-scheduling based online algorithm, i.e., the OAF algorithm. We implemented several adaptive traffic signal control algorithms that use the fine grain information broadcasts by the vehicles. We implemented and compared these algorithms under various traffic conditions. Our experimental results show that the OAF algorithm reduces the delays experienced by the vehicles as they pass through the intersection, as compared with the other three methods under light and medium vehicular traffic loads. Under heavy vehicular traffic load, the performance of the OAF algorithm degenerates to that of the vehicle-actuated traffic method but still produces lower delays, compared with Webster's method and the pre timed signal control method. This is because, under lighter traffic, the OAF algorithm can dynamically skip through phases and minimize the delay of vehicles whenever there is a gap in the traffic. This ensures that under rush-hour congestions or after a traffic accident, most important messages will not be missed by the Verifier. Security analysis and performance evaluation justify our authentication and verification approach to WAVE-enabled vehicular communications.

REFERENCES

[1] The City of Reno Public Works Department. [Online]. Available: http://www.reno.gov/index.aspx?page=658

[2] America Revealed: Nation On The Move. PBS documentary

[3] The vehicular traffic simulator. [Online]. Available: http://sumo.sourceforge.net/

[4] The wireless simulation framework. [Online]. Available: http://www.omnetpp.org/

[5] The German Aerospace Research Laboratory. [Online]. Available: www.dlr.de/en/

[6]The TRACI interface can be found. [Online]. Available: http://sourceforge.net/apps/mediawiki/sumo/?title=TraCI

[7] G. F. Newell, Theory of Highway Traffic Signals, 6th ed. Berkeley, CA,USA: Univ. California, 1989.

[8] D. C. Gazis, Traffic Science, 1st ed. New York, NY, USA: Wiley, 1989.

[9] Optimal Traffic Control: Urban Intersections, 1st ed. Boca Raton, FL,USA: CRC, 2008, pp. 400–401.

[10] C. N. Chuah, D. Ghosal, A. Chen, B. Khorashadi, and M. Zhang,“Smoothing vehicular traffic flow using vehicular_based ad hocnetworking amp; computing grid (VGrid),” in Proc. IEEE ITSC, Sep. 2006, pp. 349–354.

[11] K. LaCurts, S. Madden, H. Balakrishnan, S. Toledo, A. Thiagarajan, L. Ravindranath, and J. Eriksson, “Vtrack: Accurate, energy-aware road traffic delay estimation using mobile phones,” in Proc. 7th ACM Conf. Embedded Netw. SenSys, New York, NY, USA, 2009, pp. 85–98.

[12] D. Ghosal, C. N. Chuah, B. Liu, B. Khorashadi, and M. Zhang, “Assessing the VANET’s local information storage capability under different traffic mobility,” in Proc. INFOCOM, 2010, pp. 1–5.

[13] A. Borodin and R. El-Yaniv, Online Computation and Competitive Analysis. New York, NY, USA: Cambridge Univ. Press, 1998.

[14] K. L. Mirchandani, D. Head, and P. B. Sheppard, “Hierarchical framework for real-time traffic control,” Transp. Res. Rec., Traffic Operations, vol. 16, no. 1360, pp. 1420–1433, Dec. 2008.

[15] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, “Adaptive traffic lights using car-to-car communication,” in Proc. IEEE 65th VTC-Spring, Apr. 2007, pp. 21–25.

[16] N. Hounsell, J. Landles, R. D. Bretherton, and K. Gardener, “Intelligent systems for priority at traffic signals in London: The INCOME project,” in Proc. 9th Int. Conf. Road Transp. Inf. Control, Number 454, 1998, pp. 90–94.

[17] S. Irani and V. Leung, “Scheduling with conflicts,” in Proc. 7th Annu. ACM-SIAM SODA, Soc. Ind. Appl. Math, Philadelphia, PA, USA, 1996, pp. 85–94.

[18] B. Hull, R. Newton, S. Madden, J. Eriksson, L. Girod, and H. Balakrishnan, “The pothole patrol: Using a mobile sensor network for road surface monitoring,” in Proc. 6th Int. Conf. MobiSys, NewYork, NY, USA, 2008, pp. 29–39.

[19] D. Jiang and L. Delgrossi, “IEEE 802.11p: Towards an international standard for wireless access in vehicular environments,” in Proc. IEEE VTC Spring, May 2008, pp. 2036–2040.

[20] R. M. Karp, “Reducibility Among Combinatorial Problems,” in Complexity of Computer Computations, R. E. Miller and J. W. Thatcher, Eds. New York, NY, USA: Plenum, 1972, pp. 85–103.

[21] B. Khorashadi, F. Liu, D. Ghosal, M. Zhang, and C. N. Chuah, “Distributed automated incident detection with VGRID,” IEEE Wireless Commun., vol. 18, no. 1, pp. 64–73, Feb. 2011.

[22] S. Krauss, P.Wagner, and C. Gawron, “Metastable states in a microscopic model of traffic flow,” Phys. Rev. E, vol. 55, no. 5, pp. 5597–5602, May 1997.

[23] C. Lund and M. Yannakakis, “On the hardness of approximating minimization problems,” in Proc. 25th Annu. ACM STOC, New York, NY, USA, 1993, pp. 286–293.

[24] W. R. McShane, R. P. Roess, and E. S. Prassas, Traffic Engineering. Englewood Cliffs, NJ, USA: Prentice-Hall, 1998.

[25] C. Priemer and B. Friedrich, “A decentralized adaptive traffic signal control using v2I communication data,” in Proc. 12th Int. IEEE ITSC, Oct. 2009, pp. 1–6.d