Hindawi
Journal of Advanced Transportation
Volume 2018, Article ID 4251701, 10 pages
https://doi.org/10.1155/2018/4251701

Research Article

Context-Aware Intelligent Traffic Light Control through Secure Messaging

Mükremin Özkul,[1] **Ilir Capuni**,[2] **and Elton Domnori**[1]

[1]*Department of Computer Engineering, Epoka University, Tirana 1039, Albania*
[2]*Advanced Computing Research Center, University of New York Tirana, Tirana 1000, Albania*

Correspondence should be addressed to Mükremin Özkul; mozkul@epoka.edu.al

Received 29 May 2018; Revised 28 September 2018; Accepted 22 October 2018; Published 5 November 2018

Guest Editor: Jackeline Rios-Torres

In this paper, we propose STCM, a context-aware secure traffic control model to manage competing traffic flows at a given intersection by using secure messages with real-time traffic information. The vehicle is modeled as a virtual sensor which reports the traffic state, such as its speed and location, to a traffic light controller through a secure and computationally lightweight protocol. During the reporting process, a vehicle's identity and location are kept anonymous to any other vehicle in the system. At an intersection, the traffic light controller receives the messages with traffic information, verifies the identities of the vehicles, and dynamically implements and optimizes the traffic light phases in real-time. Moreover, the system is able to detect the presence of emergency vehicles (such as ambulances and fire fighting trucks) in the communication range and prioritize the intersection crossing of such vehicles to in order to minimize their waiting times. The simulation results demonstrate that the system significantly reduces the waiting time of the vehicles in both light and heavy traffic flows compared to the pretimed signal control and the adaptive Webster's method. Simulation results also yield effective robustness against impersonating attacks from malicious vehicles.

1. Introduction

With the increase in the number of vehicles on roads, traffic congestion is becoming a serious problem in urban areas as it increases travel times and fuel consumption [1]. Traffic light control systems manage incompatible traffic flows by restricting the free flow of the traffic using distinct time intervals or phases at road intersections and at pedestrian crossings. Besides ensuring the safe crossing of traffic, traffic signal control systems try to reduce the waiting times of vehicles at an intersection by appropriately adjusting the timing of the light sequences.

Traditional traffic light control systems use fixed-cycles that are computed as an approximation of the traffic flow based on the historical traffic flow data at an intersection. Such a pattern is followed regardless of the real-time traffic state throughout the day. On the other hand, an adaptive light control system uses the real-time traffic data coming from fixed roadside sensors, such as loop detectors or video cameras, and adopts traffic light timings continuously based on real-time traffic information.

Recently, vehicular mobile wireless ad hoc networks (VANETs) have been a primary focus of study to develop applications that would increase the road safety and the efficiency of traffic flows. In this context, significant research of VANETs has been carried out where vehicles are used as sensor nodes to create intelligent traffic light systems (ITL).

An ITL dynamically changes the traffic light timings based on the traffic information gathered from the vehicles in the VANETs. The traffic along routes with higher vehicle density are prioritized with longer green light timing compared to other routes.

In this collaborative system, the correctness of claimed identity (i.e., the characteristics of the vehicle) and location information is an important issue since it affects the functionality of the scheduling algorithm.

In the literature, existing ITL control systems ignore security control mechanisms assuming that data coming from the vehicles (such as identity, location, and other reported information) are authentic and reliable. However, a vehicle can try to cheat or deceive the control system by broadcasting false traffic information or pretending to be

multiple vehicles in order to increase the apparent number of vehicles observed by the ITL. In this way, the vehicle receives an increased portion of the green light timing. A further weakness in ITL control systems is that private data may be exposed by each vehicle's identity and made publicly available during information dissemination.

Our goal is to design an ITL control system which reduces the time required to cross an intersection and is able to prioritize the movement of emergency vehicles at given intersections without compromising the privacy of the participants.

To achieve this goal, we are aiming to achieve the following properties.

(1) **Security:** the system must be robust against attacks from malicious participants; i.e., a vehicle should not be able to manipulate the decisions of the traffic controller on the light timings and sequences or to claim multiple identities.

(2) **Privacy:** the anonymity of a vehicle should be preserved at all times. The identity of the vehicle v and its related information such as location and speed should be known only to a trusted authority.

(3) **Veracity:** the authenticity and integrity of the messages sent by a vehicle should easily be verified by a trusted authority with a computationally efficient and lightweight protocol.

(4) **Efficiency:** the system adapts promptly to real-time changes in the state of the traffic and minimizes the waiting time that vehicles spend at an intersection.

(5) **Scalability:** the system should scale regardless of the increase in the number of vehicles at an intersection.

2. Related Work

In a fixed-timing traffic light control system, a precalculated pattern is periodically repeated based on the historical traffic data. These systems do not operate in real-time and are only efficient when the traffic flow is stable and regular at the intersection during the day. However, there are several circumstances that may alter the traffic state such as accidents or maintenance work on specific roads. As a result, a prefixed control system is not able to respond to the traffic demand in real-time.

Traffic light control systems have been widely studied in the literature and adopted in practice. One approach is to use physical sensors and devices (e.g., loop detectors, video cameras with content-analysis capabilities, and wireless sensors) to detect the presence of and to classify the vehicles [2] in order to forecast vehicle density at an intersection. Using this approach [3, 4], the traffic light controller optimizes the phase timings based on the real-time inputs coming from the loop detectors installed in the proximity of or immediately before the stop line for the intersection. Loop detectors detect the presence of and count the number of vehicles that pass over them. Data collected in real-time are sent to the light controller which adjusts the traffic cycles based on the vehicle density at an intersection.

Even though an adaptive system reduces the waiting time of vehicles compared to a fixed time control, the infrastructure used in the systems entails high installation, maintenance, and operational costs and needs frequent human intervention. Moreover, loop detectors are not reliable under adverse weather conditions (e.g., the performance of the video cameras is reduced in rainy or foggy conditions or at night since visual contact with vehicles is restricted), they are ineffective in oversaturated traffic conditions (e.g., whenever the vehicle queue grows beyond the installed infrastructure), and they are not able to detect the passage of emergency vehicles approaching an intersection.

Due to the drawbacks in using road sensors, recently, vehicle actuated systems have been introduced to develop intelligent traffic lights using wireless communications. In such systems, vehicles play a crucial role in the decision-making process as they become the source of information. Through vehicular ad hoc networks (VANET), vehicles share traffic information with each other or with roadside units (RSUs) within their transmission range using Dedicated Short-Range Communications (DSRC). A vehicle, acting as a virtual sensor, is equipped with an on-board unit and periodically sends messages including the vehicle's ID, current speed, and location. Such information can be sent exclusively to the roadside unit through a vehicle-to-infrastructure (V2I) communication as in [5] or such messages may be shared with other vehicles through a vehicle-to-vehicle (V2V) communication, as proposed in [6], before they reach the roadside unit.

The roadside unit continuously collects the data and by using dynamic programming, an optimal light phase sequence is determined to reduce the total queue length at the intersection. To optimize the computation several approaches have been proposed. In [7], the authors proposed a model in which speed and position data are gathered from the vehicles' broadcast messages and used to divide the traffic into vehicle *platoons*; each platoon is then treated separately to optimize the traffic flow. Recently, in [8], a virtual *wait area* in front of the road intersection is defined for each traffic flow and the vehicles inside this area are considered ready to cross the intersection. Each vehicle uses multihop communications and advertises itself within the transmission range by broadcasting a message. The size of the vehicle queue in each wait area is computed using the broadcast data of the vehicles.

Roadside units might not be available at every intersection, especially in rural areas, raising the need for a self-coordination process among vehicles. The issue has been discussed for the first time in [9], proposing an adaptive traffic signal system based on car-to-car communication and the creation a virtual traffic light (VTL) controller. The advantage of the VTLs on the other intelligent systems is that they do not require the installation and maintenance costs of permanent infrastructure. The vehicles autonomously elect a leader vehicle which coordinates the traffic lights at the intersection. The coordinator election in a VTL has been discussed in [10] and an optimized distributed algorithm has been proposed in [11].

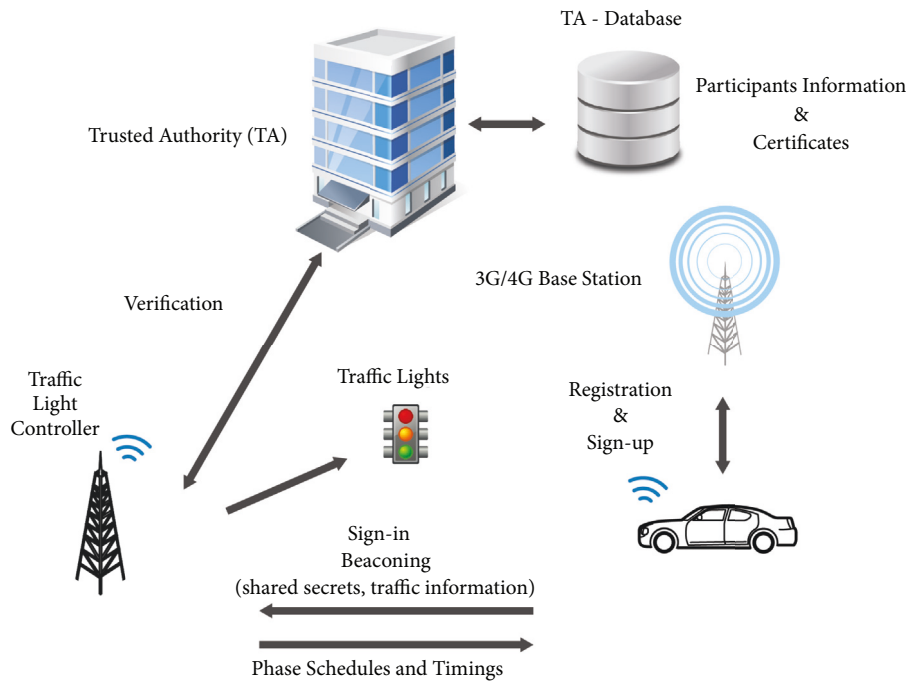

Figure 1: The system architecture with communication protocol.

The use of VTL becomes problematic once the number of vehicles increases over a certain threshold. The system approaches a lack of scalability by facing two issues: (a) the election process for the coordinator could be problematic in VTLs showing poor performances (as discussed in [12]) and (b) the coordinator should afford all the computation required to collect the data, take a decision, and forward it to the other vehicles in the network.

The involvement of vehicles in the decision process, beside computation, has raised another issue: that of the reliability of the data they share. Adversary vehicles can collude to get a higher priority and time to cross through an intersection. Although the proposed intelligent controls in [7, 9–11] are more efficient in terms of reducing vehicle delay times and increasing traffic flow than the prefixed controls and actuated systems, the security issues of the models are not addressed at all. The aforementioned intelligent traffic systems operate under the assumption that data from participating vehicles is fully accurate; i.e., that all identity and location reports from the vehicles are veracious. However, a malicious vehicle can try to cheat a traffic light control by simply broadcasting a bogus identity, e.g., impersonating an emergency vehicle or pretending to be multiple vehicles by replaying the messages of other vehicles to increase the green time allotted to the cheating vehicle's road section. Therefore, an accurate and reliable method of real-time information verification is a key aspect in implementing an efficient and intelligent traffic light controller.

Recently, several secure message delivery protocols for VANETs have been proposed. In [13], the authors propose a privacy-preserving framework for continuous tracking and verification of the vehicles using a computationally lightweight cryptography. In the model, each vehicle announces its location periodically through anonymous beacons to the nearby vehicles, which collect and report the received beacons to a location authority. The location authority processes the reported beacons to verify and infer the positions of the vehicles. In our system, information about location is not saved by the transportation authority. In the VANETs, anonymous authentication schemes to verify the authenticity of vehicles as presented in [14, 15] are a well-adapted method that avoids revealing real identities by using multiple certificates and pseudo identities.

To address these problems, we propose a traffic light control system using secure messages of vehicles in VANET. A vehicle only sends anonymous messages to announce its presence to a traffic controller in a way that the movements of a vehicle are not tractable and the real identity is hidden from the vehicles. The reliable messages obtained from the vehicles provide the basis of efficient light timing for a traffic controller.

3. System Layout

In this section we outline the system and the notation that will be employed during the analysis and implementation.

The system architecture and the communication protocol are represented as seen in Figure 1. The system consists of a trusted authority (TA) which maintains a database of registered vehicles and communicates with the vehicles via a 3G/4G network and Traffic Light Controllers (TLC) installed at road intersections. Once a vehicle starts, it needs to go through a sign-up process with the TA. Once this phase is completed, the vehicles mostly communicate with the TLCs.

TLCs do not communicate with each other; hence they do not share information (except with the TA). This

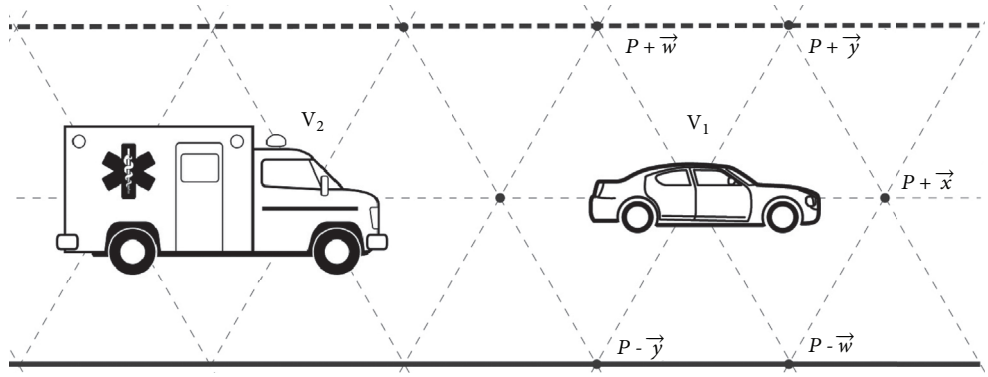

Figure 2: The grid system. V_1 shows a standard vehicle located in a single site P and V_2 shows a longer vehicle, an ambulance, modeled by using two adjacent sites.

communication strategy preserves the private information of each participant, both their true identity and location at each instant of time.

We will use a two-dimensional triangular grid with a fixed coordinate system as shown in Figure 2. This model is introduced in [16]. Each point $\overrightarrow{p} = (x, y)$ of this system is called a *site* and may contain at most one object. A vehicle is an object of specific kind; it is an automaton which is self-propelled. As an automaton, its state information includes data such as the unique ID given by the trusted authority, current location, speed obtained by the on-board units, time, its vehicle category, etc. Each vehicle is equipped with a wireless communication unit (such as Dedicated Short-Range Communications (DSRC) and a temper proof Global Positioning System receiver (GPS)) and has 3G/4G capability. The vehicles can move to one of the six neighboring sites and can change and update their state by applying a rule from the rule set. The *movable set* M_v of a vehicle v contains the set of neighboring empty sites in the direction of the traffic flow where a vehicle can go in the next update. An empty movable set M_v of a vehicle v means that v cannot apply movement rules.

A list of consecutive sites between grid boundaries with the same movement direction is called a *lane*, and a set of neighboring lanes (facing independent directions) is called a *road*.

A road *intersection* I is a set of sites which connects the lanes with different traffic directions. The set of inbound lanes in an intersection I define the incoming traffic flow, and the set of outbound lanes define the outgoing traffic flow.

The traffic controller manages the traffic flow into and through the intersection by updating the rules to each traffic flow using time intervals. The sets of these rules are called *phases*. These rules define the movable sets which were mentioned above. In a *red phase*, a vehicle has an empty M_v, whereas a *green phase* results in a nonempty M_v.

Phases allow at most two flows to proceed simultaneously into and through the intersection without conflicting with each other. The resulting decisions made by TLC are displayed by the classical traffic lights.

Let P_{ij} be a pair of unconflicting flows i and j, where $i, j \in \{1, 2, \ldots, 8\}$, as seen in Figure 3(a). During an active phase, flows are allowed to cross the intersection transition to the next phase in the sequence. From this time the controller restarts the phase sequence, which is called a *traffic light cycle* configuration $C_t = \{P_{15}, P_{26}, P_{37}, P_{48}\}$, at time t, as follows:

$$\mathscr{P}_{15} \longrightarrow \mathscr{P}_{26} \longrightarrow \mathscr{P}_{37} \longrightarrow \mathscr{P}_{48}. \quad (1)$$

Note that a light cycle is flexible in the sense that there are no constraints on the phase sequences and timings or the time intervals between the phases. The controller can reorder the current phase C_t at an emergency event or use a different phase sequence on the next cycle C_{t+1}.

3.1. Encoded Data. Initially, a vehicle is registered to the trusted authority (TA), which manages the sign-in process, distributes digital certificates and a set of pseudo IDs to the vehicles, keeps the identity information of the vehicles in its database, and is totally trusted by all the vehicles.

When a vehicle starts, it initiates communication using traffic controllers or through the cellular network and establishes a symmetric key with the TA. First, a vehicle v sends a registration request at time t^0 to the TA which verifies the identity, id of v, and returns the triplet $(K_v; r_v; o_v)$ to the vehicle, where K_v is a short-term symmetric key, and r_v and o_v are two random integers. Both parties initialize a counter n to the value r_v and increment it by o_v at every message sent by v. A time dependent secret $s_v(t)$ serves for the TA to verify the identity of the vehicle v and the integrity of the messages it sends. The secret is computed and encrypted as follows.

First,

$$s_v(t) = E_{K_v}\{r_v + no_v\}. \quad (2)$$

Then at every τ_b seconds, the vehicle periodically broadcasts a beacon in which it sends location and speed to TLCs in the communication range through the wireless IEEE 802.11p standard. The beacon message is calculated as follows:

$$\mathscr{B} = \left\langle E_{K_v}\{(l \parallel s) \oplus s_v(t)\}, t_{stamp}, \sigma \right\rangle \quad (3)$$

where l is the location of the vehicle on the grid system, s is the vehicle speed which is appended to the location information, and both l and s are XOR'ed with the encoded data $s_v(t)$, t_{stamp} is used to prevent a message replay attack, and the σ is the beacon digest obtained by using a hash function, e.g., SHA-1.

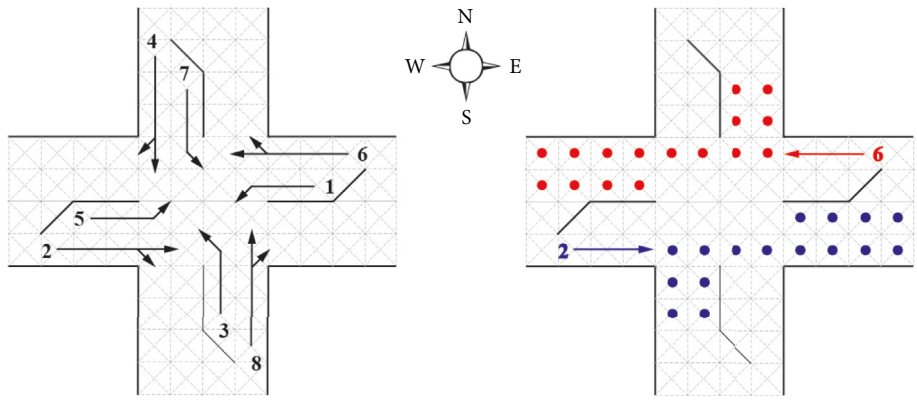

FIGURE 3: (a) Traffic flows at the intersection. (b) The sites with dots show the movable set for the phase sequence P_{26}.

4. Traffic Light Controller

In the system, the vehicles act like virtual sensors and perform the task of reporting the traffic information to a traffic controller in the communication range.

The traffic controller is physically centered at the intersection and has access to the TA database. It receives beacons from the vehicles to detect their presence, determine their location and speed, and monitor the traffic state in real-time. Whenever a beacon is received, it must be verified for veracity. For each message b received, the traffic controller determines the vehicle v which the message belongs to as follows:

(1) Define t_{beacon} the time the beacon b is received.

(2) For each $w \in \mathcal{S}$, where $\mathcal{S}$ is the set of vehicles to be verified, compute

$$i = \left\lfloor \frac{t_{beacon} - t_w^0}{\tau_b} \right\rfloor, \tag{4}$$

where i represents the index of the precomputed encoded data value and t_w^0 represents the time when TA has received the sign-up request from the vehicle w.

(3) It retrieves the secret value x_w^i that matches x_v^i.

If there is a match, the traffic controller identifies v to be the vehicle that has sent the beacon and includes the vehicle in the set of authenticated vehicles $\mathcal{V}$ which are in the vehicle queue to cross the intersection.

4.1. Phase Scheduling. The traffic controller dynamically executes the phase sequence according to assigned priority to each direction or skips a green phase as necessary, e.g., in the case of prioritizing the passage of emergency vehicles. Valid beacons allow the traffic controller to define the traffic state at a time t, such that the traffic controller has the exact number of waiting vehicles, the length of vehicle queues, the types of vehicles, and the vehicular density in a traffic flow on each road section.

When all phases of a current cycle are executed, the traffic controller computes the new phase timings to each flow as follows:

$$T_{phase} = n_l + \frac{c \cdot t_c}{s} \tag{5}$$

where n_l is a time constant used to compensate vehicle stop-and-go movements caused by the phase changes, c is the number of sites occupied with vehicles, t_c is the time per vehicle to enter the intersection, and s is the mean speed on the road.

The phase timings are granted to each traffic flow based on of the number of vehicles at the road intersection, therefore assigning more phase timing to traffic flow with a higher density. To prevent vehicles waiting very long in traffic flow with low density an upper time limit t_{max} is set for each phase timing.

A phase to traffic flow can be skipped in the next cycle if there is no vehicle within the communication distance. Priority of the traffic flows is also defined at this stage. Whenever an emergency vehicle is detected, the respective traffic flow is given highest priority to cross independent of the present traffic state at the intersection.

Then, the traffic controller periodically broadcasts the phase timing information (every 1 second), which also includes information about the time remaining for the current phase, the phase sequence, and times through beacons at the intersection.

4.2. Emergency and Public Transport. Emergency vehicles need to reach their destination as quickly as possible. Therefore, they need to be given higher priority at an intersection. Such vehicles warn and announce their presence to the others with visual and sound alarms in the neighborhood, so that a nonemergency vehicle is to yield and allow the emergency vehicle to pass through the intersection.

Even though vehicles should always respond in a timely way to the alarms and give the right of way to emergency vehicles, sometimes careless drivers may miss or ignore the alarm, hence causing delays to response times of emergency vehicles. In our model, an emergency vehicle approaching the

intersection is identified by the beacons it broadcasts, after which the active phase is interrupted if necessary or the phase time is extended to provide the safe passage of the emergency vehicle without any significant delay.

First, a priority index k = (0-highest, 1-high, 2-normal, 3-low, 4-lowest) is set in the traffic rule set to detect the emergency vehicles approaching the intersection. The emergency vehicles have the highest priority, while a nonemergency vehicle such as a truck has the lowest priority. A further classification of the vehicles can be defined into several different categories; e.g., medical, police and security, fire, and rescue, as in the work [17], depending on their importance. If an emergency vehicle is detected in the traffic flow served by the current green phase, the controller simply extends the phase time until the vehicle passes through the intersection in a way that creates a green wave effect for the quick passage of the vehicle to its destination. For the cases in which the vehicle is present in a flow other than the served green phase, the current phase is interrupted and the green phase is granted to the flow where the vehicle is approaching. Finally, the phase sequence is restored to its initial configuration before the emergency event.

The traffic controller virtually extends the phase time for vehicles such as buses or taxis used in the public transportation structure. Here, depending on the size of the vehicle and the time of the day, the traffic controller doubles or triples the time assigned per vehicle.

5. Security and Privacy Analysis

In this section, we analyze the security aspect of the traffic light control system. We pay particular attention to message alteration, replay attacks, and identity impersonation of a vehicle.

5.1. Message Alteration. In the system, a vehicle cannot claim to be another vehicle, since at the initial sign-up the TA requires a valid digital certificate. Therefore, a vehicle cannot deny having sent a beacon because a verifiable signature guarantees the beacon's integrity. Furthermore, the identity of a vehicle and its report is verified with the encoded, s_v, data upon receiving the reports.

In a message alteration attack, an adversary tries to change or modify the information in a beacon of its neighbors. However, a beacon at time t always includes the encoded data to TA, and the identity of a vehicle is verified with the encoded data s_v upon receiving the beacon by the traffic controller. Since only the vehicle v can create the valid encoded data s_v at the time t, a trusted authority can verify the validity and integrity of the information in the beacon.

5.2. Replay Attacks. In this attack, an adversary vehicle uses and replays the beacons which are sent by its neighbors at an earlier time. It then tries to increase the number of vehicles in the traffic flow or impersonates an emergency vehicle to have priority crossing.

However, the traffic controller first determines the time the encoded data is generated and compares with the t_{stamp} of the received beacon.

If the time is outside the allowable time interval of τ_b, an adversary replays a beacon it recorded at an earlier time, validation of the t_{stamp} will fail, and the beacon will be treated as old and and then simply discarded.

In a case for which a beacon is successfully replayed in the window of τ_b, only the first valid beacon is processed and the others are dropped without processing. Moreover, each beacon has a different time dependent secret of s_v for two consecutive time instants t and $t + 1$. If the same encoded data were detected, the time registered would not match. Therefore, the code contained in the beacon along with the t_{stamp} guarantees the freshness of the beacon. Thus, the system is secure against any replay attack.

5.3. Sybil Attacks. In Sybil [18] attacks, an adversary vehicle claims multiple identities and impersonates another. Recall that the decision of the traffic light controller is based on the numbers and the types of vehicles gained, from the broadcast beacons of the vehicles. Therefore, a dishonest vehicle may present multiple identities with the intent of increasing the number of vehicles at an intersection. At the sign-in, each vehicle receives a set of pseudo IDs and a symmetric key by trusted authority using a valid digital certificate. For this type of attack to succeed, a vehicle must obtain a number of valid certificates of other vehicles or fabricate a valid certificate which is virtually impossible with the use of digital signature certificates. This attack only is effective when the security of the TA is compromised.

A vehicle must obtain a number valid of certificates of other vehicles as fabricating a valid certificate or a pseudonym is not possible with public-key-based digital signatures. An adversary vehicle is not able to use multiple identities at once.

5.4. Privacy. Pseudonym changing techniques are the main solution adopted to provide privacy and anonymity in VANETs. In the system, each vehicle is assigned multiple certificates with pseudo identities by the TA. At the initial sign-in phase a vehicle's certificate is verified, and then a symmetric key is established with the TA and the vehicle. Then, instead of using one fixed certificate, each message is signed using pseudonym certificates by the vehicle.

6. Simulation

In this section, the performance of our proposed system is evaluated against the prefixed time and actuated Webster's traffic control in terms of average vehicle waiting times. Then, the system security is tested under the influence of adversary vehicles which broadcast bogus beacons or impersonate truthful vehicles by simply replaying their beacons.

6.1. Simulation Settings. Our proposal is evaluated through OMNET++ wireless simulator, a discrete-event network simulator based on C++ [19], and Simulation of Urban Mobility (SUMO) [20], a realistic open source traffic simulator for vehicular traffic. SUMO generates the vehicular traffic and is used to obtain the traffic information, including speed and location, from the vehicles. OMNET++ implements a framework for simulating wireless communications and uses

Table 1: The simulation parameters for waiting times.

Parameter	Value
Number of vehicles per two-lane road	500 - 1800 per hour
Beacon transmission rate	1 x per second
Transmission range	$\cong 200m.$
Road length	100 sites at each approach
Simulation duration	70 min.

the IEEE 802.11p protocol stack at both the physical and Media Access Control (MAC) protocol layers. VEINS [21] is a framework for vehicular network simulations, which through TraCI [22] serves as an interface between SUMO and OMNET++ and maps the vehicles as a mobile network node in OMNET++.

The prefixed time control is set to have 45 seconds of green time and 3 seconds offset for the phase changes. Webster's equation is used to compute the optimal cycle time C_o which minimizes vehicle delays at an intersection for the adaptive traffic lights control and is defined as follows:

$$C_o = \frac{1.5L + 5}{1 - \sum Y_i} \tag{6}$$

where Y_i is the ratio of an upstream flow rate to the saturation flow at the same approach for the phase i and L is unusable offset times per cycle including all-red periods. Here, the green phase is given time in proportion to the degree of the saturation on its approach.

The main simulation parameters are summarized in Table 1.

The simulation map is based on a four-leg road intersection. At the intersection, a roadside unit is positioned, receives the traffic information from the vehicles, and broadcasts the cycle information to the vehicles. All the roads have two lanes in the same traffic direction and have a total length of 1 km upstream and downstream of the intersection.

At each road, the maximum speed limit is set to 40 km/h. A random distribution of the speed is specified for the vehicles between the range 25 km/h to 40 km/h. The typical passenger car length is equal to 5 m., and intervehicle distance at full stop is set to 2.5 m. The vehicles periodically broadcast beacons at intervals of 1 second whereas a RSU is set to broadcast at an interval of 1 second for dissemination of phase timings at the intersection.

6.2. System Performance. In the simulation, several vehicle densities are used to evaluate the effects of density over the vehicle waiting times at the intersection. First, the traffic flow is set to a constant 600 vehicles/hour for the north-south flow, defined as the $\mathscr{P}_{48}$, while east-west traffic flow density is varied from light to high density levels several times during the simulation. The east-west flow has four different vehicle density rates, 500, 800, 1000, and 1400 v/h (vehicles/hour), defined as the $\mathscr{P}_{26}$, which is considered to be light and medium vehicle density levels. The simulation starts with the 500 v/h east-west vehicle density and then is switched to the next level at 10 min. intervals, and then from the peak density level it reverts to the initial light density

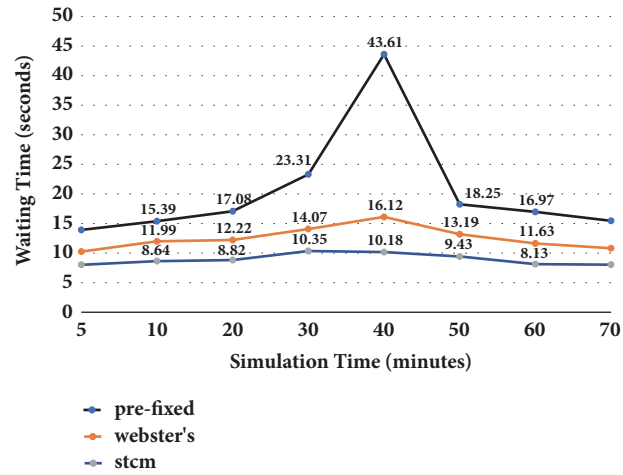

Figure 4: The comparison of the light control systems under light and medium traffic flows.

level. Second, the model is tested under heavy vehicle density levels where the east-west traffic flow density is set to 1400, 1800, and then back 1400 v/h. The simulation is run in a period of 70 minutes where the initial 5 minutes is defined as the warm up period after which the measurements are recorded. The average vehicle waiting time is expressed in seconds and represent the time a vehicle takes to cross the last 250 meters of an intersection (this is the average distance of wireless communication), and the results are plotted at 5 min. intervals in all the traffic light control systems.

Figure 4 shows the performance evaluation of the model in light and medium traffic flows compared to the prefixed time method and adaptive Webster's method, in terms of average vehicle waiting times.

From the results, it can be observed that as the vehicle density increases the average vehicle waiting times also increase in all methods. However, our model exhibits a linear increase compared to the fixed time and Webster's control systems. This is due to the vehicles need to wait more than one green phase at the intersection, resulting in an exponential increase of the vehicle delay times. Moreover, as seen in Figure 5, the model recovers faster in heavy vehicle densities than in the other two systems since the density drops toward a medium level over time.

The magnitude of the waiting times reduction obtained using our model varies in the range of 35% in the light vehicle densities and 25% in heavy densities with the other methods considered here.

6.3. System Security. In this section, the effect of adversary vehicles on the average waiting times is tested in the system. Recall that a green phase timing depends proportionally on the number of vehicles (vehicles that truthfully participate in the system by periodically broadcasting the encoded data, penetration level) in the respective road section.

Figure 6 shows the results of the vehicle waiting times under several rates of adversary vehicles in the traffic flows. Here, the north-south bound vehicles always broadcast correct information; whereas in the east-west flow the number

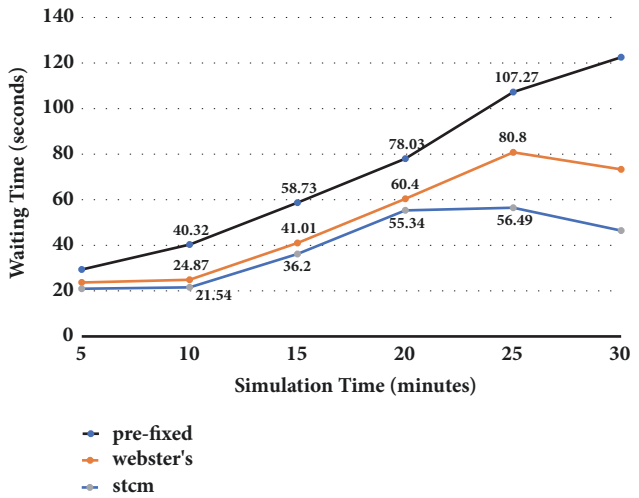

Figure 5: The comparison of the light control systems under heavy traffic flow.

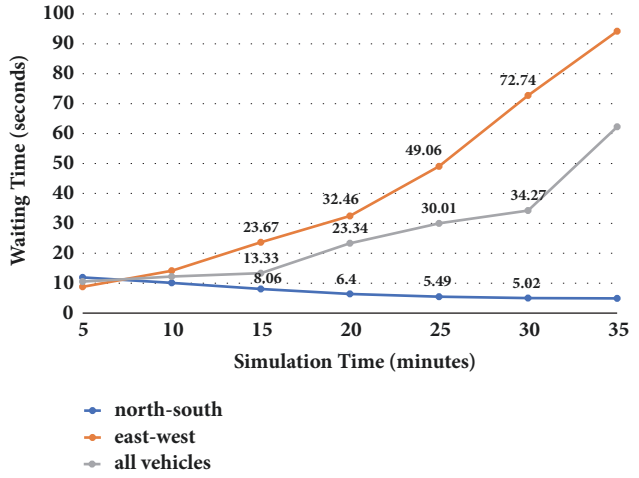

Figure 6: The system performance under adversary vehicles.

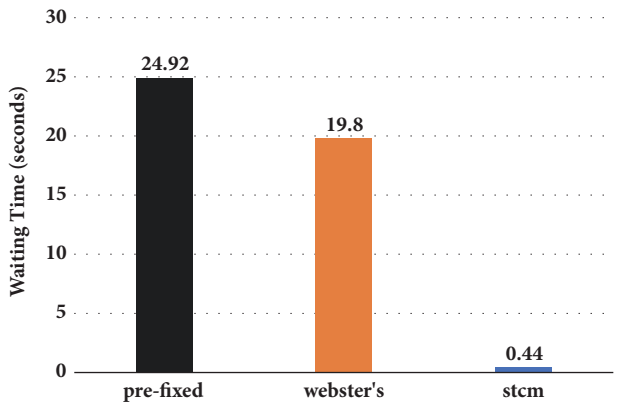

Figure 7: Emergency vehicles waiting times.

of the truthful vehicles is decreased over time during the simulation. The waiting times for all vehicles between the 70% and 90% penetration levels are similar to those for the 100% levels. There is, however, an increase in average waiting times under the penetration levels of 50% and lower.

Specifically, the waiting times of east-west flow dramatically increase as the levels of truthful vehicles goes below 50%. Therefore, the result indicates that the system is not affected by the bogus messages since the adversary vehicles are not considered in determining the signal timing, which causes an increase of the waiting times. Note that the north-south waiting times improve over time since the number of the vehicles increases proportionally relative to the east-west flow.

6.4. Emergency and Public Transport. Figure 7 shows the average waiting times of the emergency vehicle which cross the intersection. The emergency vehicles make up 1.5% of all vehicles and are entered into the simulation with Poisson arrival rate. A vehicle usually experiences some peak waiting times whenever it is caught up at a red phase in the prefixed and Websters' control methods, whereas our system consistently exhibits minimum waiting times throughout the simulation. However, the average waiting times per vehicle increase, up to 30% in some cases as compared with the results in which no emergency vehicle exists due to extended and interrupted phases to the flows to prioritize the emergency vehicles. This can be considered an acceptable trade-off given the benefits of near elimination of the waiting times of the emergency vehicles.

Note that the simulation scenario assumes the vehicle queue at the road section on which an emergency vehicle is present is within the boundaries of the communication distance.

In the next simulation, the size of the public vehicles, buses, is virtually increased at every 12 minutes from 1 site to 9 sites in a simulation of one hour. The east-west flow has a density of 800 v./h and contains additional traffic of 60 buses per hour, whereas north-south flow is set to 600 v./h with no public vehicles present. Figure 8 shows the effect of virtual resizing on wait times of vehicles. The results show the decrease in wait times in east-west flow as the size of the buses increases. Naturally, north-south flow wait times are affected inversely with a trade-off that favors public transport vehicles.

7. Conclusions

In this paper, we presented a traffic light control system which operates on the exchange of messages between the vehicles and a traffic light controller. The system maintains the anonymity of the vehicles at all times and uses a computationally lightweight encryption protocol. At the same time the system allows a trusted authority to identify the vehicles including those that are used in cases emergency and public transportation.

The simulation results show that the system is efficient in optimizing the waiting times of the vehicles and significantly reduces the waiting time of emergency vehicles. Furthermore, the system is robust against network attacks from adversary vehicles, and the vehicles that try to cheat the system with bogus messages to gain some advantage over the intersection

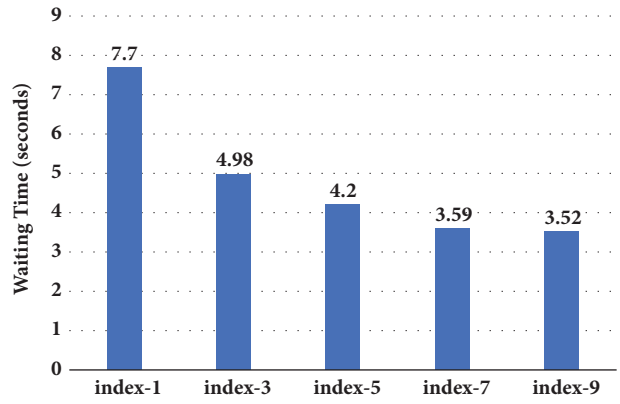

FIGURE 8: Public transport vehicle; bus; wait times with different site values.

crossing end up with a disadvantage in terms of longer waiting times.

Clearly, in real life application, not all the vehicles are registered within the TA. The system needs a certain number of vehicles to actively participate in order for the system to be beneficial and efficient. As the results depicted in Figure 6 imply, if the participation rate is less than 60% the performance of the system degrades.

Even though not explicitly shown in the paper, the system can easily be deployed at urban intersections where the commuter pedestrian traffic is high. Here, the participants with a mobile unit with wireless capabilities, such as a smartphone or a tablet, can participate by simply using a mobile application or some specific carry on device.

Moreover, the traffic controller is able to dynamically prioritize the traffic flows based on the vehicle types present in traffic in real-time by simply changing the index values set in the system. During rush hours, public transport vehicles like buses and other similar vehicles can be given higher passage priorities to encourage the usage of public transportation and consequently reduce the number of private vehicles in traffic.

For the ease of presentation, we have assumed that vehicles do send the GPS coordinates to the TLC. However, it is easy to see that sending the type of vehicle and its size and proving its location by replaying the messages of the neighboring vehicles is sufficient. Unfortunately, this would impose some cumulative delays and overall loss of efficiency in the system.

Data Availability

No data were used to support this study

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] D. Schrank and T. Lomax, *Urban Mobility Report*, Texas Transportation Institute, 2005.

[2] S. Atev, H. Arumugam, O. Masoud, R. Janardan, and N. P. Papanikolopoulos, "A vision-based approach to collision prediction at traffic intersections," *IEEE Transactions on Intelligent Transportation Systems*, vol. 6, no. 4, pp. 416–423, 2005.

[3] N. Hounsell, J. Landles, R. Bretherton, and K. Gardner, "Intelligent systems for priority at traffic signals in London: the INCOME project," in *Proceedings of the Ninth International Conference on Road Transport Information and Control*, pp. 90–94, London, UK.

[4] R. Akçelik, M. Besley, and E. Chung, *An evaluation of scats master isolated control [Msc. thesis]*, 2001.

[5] C. Priemer and B. Friedrich, "A decentralized adaptive traffic signal control using V2I communication data," in *Proceedings of the 2009 12th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pp. 1–6, St. Louis, October 2009.

[6] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, "Adaptive traffic lights using car-to-car communication," in *Proceedings of the 2007 IEEE 65th Vehicular Technology Conference (VTC '07)*, pp. 21–25, April 2007.

[7] K. Pandit, D. Ghosal, H. M. Zhang, and C.-N. Chuah, "Adaptive traffic signal control with vehicular Ad Hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 4, pp. 1459–1471, 2013.

[8] M. Bani Younes and A. Boukerche, "Intelligent Traffic Light Controlling Algorithms Using Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 5887–5899, 2016.

[9] N. Maslekar, J. Mouzna, M. Boussedjra, and H. Labiod, "CATS: an adaptive traffic signal system based on car-to-car communication," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1308–1315, 2013.

[10] F. Hagenauer, P. Baldemaier, F. Dressler, and C. Sommer, "Advanced leader election for virtual traffic lights," *ZTE Commun*, vol. 12, no. 1, pp. 11–16, 2014.

[11] A. Bazzi, A. Zanella, and B. M. Masini, "A distributed virtual traffic light algorithm exploiting short range V2V communications," *Ad Hoc Networks*, vol. 49, pp. 42–57, 2016.

[12] V. V. Gayah, X. Gao, and A. S. Nagle, "On the impacts of locally adaptive signal control on urban network stability and the macroscopic fundamental diagram," *Transportation Research Part B: Methodological*, vol. 70, pp. 255–268, 2014.

[13] F. Malandrino, C. Borgiattino, C. Casetti, C.-F. Chiasserini, M. Fiore, and R. Sadao, "Verification and inference of positions in vehicular networks throughanonymous beaconing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2415–2428, 2014.

[14] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[15] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6 I, pp. 3442–3456, 2007.

[16] M. Ozkul and I. Capuni, "An autonomous driving framework with self-configurable vehicle clusters," in *Proceedings of the 3rd International Conference on Connected Vehicles and Expo, ICCVE 2014*, pp. 463–468, Austria, November 2014.

[17] M. B. Younes, A. Boukerche, and A. Mammeri, "Context-Aware traffic light self-scheduling algorithm for intelligent transportation systems," in *Proceedings of the 2016 IEEE Wireless*

Communications and Networking Conference, WCNC 2016, Qatar, April 2016.

[18] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, vol. 2429 of *Lecture Notes in Computer Science*, pp. 251–260, Springer, Berlin, Germany, 2002.

[19] A. Varga and R. Hornig, "An overview of the omnet++ simulation environment in," in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications*, pp. 60-10, 2008, http://dl.acm.org/citation.cfm.

[20] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo - simulation of urban mobility: An overview in," in *Proceedings of the in SIMUL, 2011*, pp. 63–68, 2011.

[21] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[22] A. Wegener, M. Piórkowski, M. Raya, H. Hellbrück, S. Fischer, and J. Hubaux, "Traci: An interface for coupling road traffic and network simulators," in *Proceedings of the 11th Communications and Networking Simulation Symposium, CNS '08*, pp. 155–163, ACM, New York, NY, USA, April 2008.