Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure intelligent traffic light control using fog computing

Jian Liu [a,b], Jiangtao Li [a], Lei Zhang [a,b,*], Feifei Dai [a], Yuanfei Zhang [a], Xinyu Meng [a], Jian Shen [b]

[a] Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering, East China Normal University, China

[b] School of Computer and Software, Nanjing University of Information Science and Technology, China

HIGHLIGHTS

- Our schemes may resist the attacks from malicious vehicles.
- Our schemes can avoid the problem of single-point failure.
- Our improved scheme is fog device friendly.

ARTICLE INFO

Article history:
Received 31 May 2016
Received in revised form
30 December 2016
Accepted 8 February 2017
Available online xxxx

Keywords:
Intelligent transportation system
VANET
Traffic light control
Puzzle

ABSTRACT

As the number of vehicles grows, traffic efficiency is becoming a worldwide problem. Intelligent transportation system aims to improve the traffic efficiency, where intelligent traffic light control is an important component. Existing intelligent traffic light control systems face some challenges, e.g., avoiding heavy roadside sensors, resisting malicious vehicles and avoiding single-point failure. To cope with those challenges, we propose two secure intelligent traffic light control schemes using fog computing whose security are based on the hardness of the computational Diffie–Hellman puzzle and the hash collision puzzle respectively. The two schemes assume the traffic lights are fog devices. The first scheme is a simple extension of a recent scheme for defending denial-of-service attacks. We show this simple extension is not efficient when the vehicle density is high. The second scheme is much more efficient and is fog device friendly. Even the vehicle density is high, the traffic light may verify the validity of the vehicles efficiently.

1. Introduction

As the number of vehicles is increasing throughout the world, particularly in large urban areas, traffic efficiency is becoming a worldwide problem. Traffic lights (or traffic signals) [1,2] are signaling devices which are used to optimize traffic efficiency by alternating the signal phase for traffic flow control at road intersections, pedestrian crossings, and other places. Traditional traffic lights usually have fixed-cycles, i.e., the lights change at regular intervals. This is inefficient, since traffic situation is constantly changing. Intelligent transportation system (ITS) has been designed to control the traffic flow adaptively according to the real-time traffic situation, in which traffic lights also become intelligent. An intelligent traffic light may alternate the signal phase with an efficient traffic schedule algorithm (such as fuzzy logic, evolutionary algorithms and reinforcement learning) to minimize the waiting times of road users based on the position, speed and direction of the road users.

1.1. Related work

Existing methods for intelligent traffic light control use two strategies: fixed-time one and traffic-responsive one. In fixed-time strategy, several signal plans corresponding to different divisions of time (e.g., 7:00 am to 9:00 am) are predetermined based on the historical traffic flow data. A traffic light is periodically changed according to the predetermined signal plans. For instances, the urban traffic control system [3] and TRANSYT [4] etc., are the intelligent traffic light control systems in this catalog. We note that such systems are not real time and only applicable when the demand is fairly stable within each division of time. They are inefficient to respond to sudden changes in traffic flow caused by accidents or emergency cases. Traffic-responsive strategy overcomes above limitation by making use of current traffic

* Corresponding author at: Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering, East China Normal University, China.
E-mail address: leizhang@sei.ecnu.edu.cn (L. Zhang).

http://dx.doi.org/10.1016/j.future.2017.02.017
0167-739X/

information to optimize the settings of the traffic lights. The key problem of this strategy is how to forecast the incoming vehicles. Generally, we have following methods.

The first one is to use pavement loop detectors. The systems in this category include Sydney coordinated adaptive traffic system (SCATS) [5] and split, cycle, and offset optimization techniques (SCOOT) [6]. In such systems, the loop detectors are able to detect the vehicles when they pass through the loop detectors. Then the loop detectors may send the traffic situation detected to the traffic signal controller through wired links. The traffic signal controller then adjusts the traffic light based on the data received. Such systems are able to adjust the traffic light according to the real time traffic situation. However, pavement loop detectors are usually heavy to use. A road needs to be torn up during installation. Hence, the traffic is usually disrupted during installation. Inductive loop is also prone to breakage as a result of other construction. Therefore, it is inconvenient for large scale deployment.

The second one is to employ video-based traffic detection systems. For example, Reno, NV, USA is a city which is using video-based traffic detection systems. In such system, human operators sitting in a control room collect traffic data through video cameras, and adjust the duration of red lights based on current traffic flow. But this system requires a high degree of human intervention. To deal with this problem, automated vision-based approaches [7,8] were proposed. In such systems, video image processing technique is used to detect the traffic conditions. The controller then adjusts the light based on the traffic conditions detected. Compared with the loop detectors, the video cameras can provide more information of the vehicles. However, video image recognition is still a challenging task. Moreover, some environmental factors (such as shadow and reflection of light) may also influence the detection accuracy.

The third one is to use wireless sensor networks (WSNs) [9–12]. In a WSN based traffic light control system [13–15], detecting nodes are distributed on both sides of the road. When vehicles enter the monitored region where the detecting nodes are deployed, the detecting nodes send the status information of the vehicles to the control nodes. Finally, based on the received information, the control nodes control the alternating of the signal phase. But there are some restrictions in this method. One of the problems is due to the fact that large number of detecting nodes may exist in the system which implies high maintenance cost. Further, the security of the WSN system is difficult to guarantee. The detecting nodes can be corrupted, and interfering signals can be generated by attackers to mislead the control nodes.

Recently, vehicular ad hoc network (VANET) [16–19] has attracted more and more attention from both industry and academic community. In VANET, a vehicle can communicate with nearby vehicles and roadside units (RSUs) using the DSRC protocol. Several intelligent traffic light control systems are already designed in VANET environment. In [20–22], VANETs are used to help a traffic light controller to collect traffic data. However, security issues are not studied in existing schemes. In fact, malicious vehicles may exist in VANETs. A malicious vehicle may send fake information to the traffic light controller for its own profit. For instance, a malicious vehicle may pretend to be multiple vehicles, such that the vehicle may get a higher priority to pass through an intersection. Further, these schemes (as well as the schemes using pavement loop detectors, videos or WSNs) assume the traffic lights are maintained by a remote central controller (e.g., a server or a cloud). However, since all the traffic lights have to communicate with the controller frequently for decision, these schemes may result in large latency. In the worst case, if the communication channel between a traffic light and the controller is interrupted, the system fails.

Fog computing [23] is a new technique which was put forward by Cisco. In fog computing, users utilize a collaborative multitude of end-user clients or near-user edge devices to carry out the operation of computation and storage. In traffic light control schemes using fog computing [24], a traffic light may act as a fog device who may interact with neighboring traffic lights and nearby vehicles. Based on the received information, the traffic light may run a traffic schedule algorithm to adjust the traffic light. Since the traffic schedule algorithm is run by the traffic light, compared with the previous methods, this method has the property of low-latency. This paper studies intelligent traffic light control in VANET using fog computing.

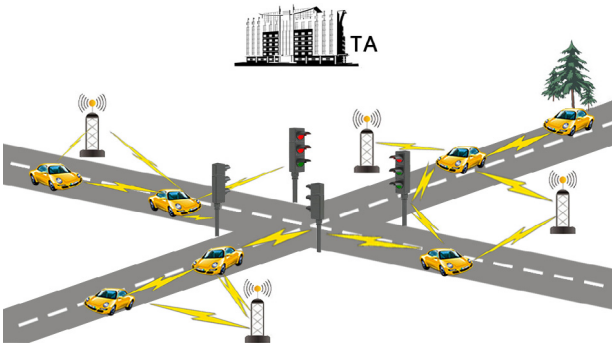

Fig. 1. System architecture. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

1.2. Our work

Existing traffic light control schemes in VANET assume the vehicles are honest, i.e., the vehicles report their status information honestly, and, have the problem of single-point failure. To deal with these problems, we propose two secure traffic light control schemes in VANET using fog computing.

Firstly, we propose a basic scheme for traffic light control in VANET using fog computing. The basic scheme is a simple extension of the scheme in [25] which is initially used to defend denial-of-service (DOS) attacks. Similar to the schemes in [25], the security of our scheme is based on the computational Diffie–Hellman (CDH) puzzle (a type of cryptographic puzzle) which states that, in a cyclic group $\mathbb{G}$ with prime order q, given $g, g^a, g^b \in \mathbb{G}$ for unknown a, b, it is time-consuming to compute g^{ab}. In our scheme, a pool of CDH puzzles with designated hardness are generated by a traffic light. The puzzles are then encrypted using a location based encryption (LBE) scheme (see Section 2.3) and broadcasted to the nearby vehicles. Only the vehicles within the specified area are able to get the puzzles. A vehicle has to solve a puzzle in a negotiated time period. Once the puzzle is solved, a proof is generated and sent back to the traffic light by the vehicle. The traffic light has to verify the validity of the proof. Based on the proofs, the traffic light may run a traffic schedule algorithm to adjust the traffic light plans. Our scheme is secure, privacy preserving and costly sensor free. We note that, in our basic scheme, a traffic light needs to generate and verify one proof for each vehicle in a time slot. Considering that the fog devices are not those with strong computation and storage capabilities, the computation and storage overheads of a traffic light might be too high to afford if the number of vehicles is very large. We then propose an improved scheme.

In our improved scheme, a traffic light only needs to broadcast a single puzzle encrypted using an LBE scheme to nearby vehicles. Further, the traffic light just needs to perform very light computations to verify the validity of the proofs. The improved scheme is based on the hash collision puzzle. That is, given a hash function H, find (x, x') with $x \neq x'$ such that $H(x) = H(x')$. We note that, finding a collision is usually hard for a secure

Please cite this article in press as: J. Liu, et al., Secure intelligent traffic light control using fog computing, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.02.017