Preliminary Results for Secure Traffic Regulation

Assia Belbachir[1,3], Sorore Benabid[1,3], Marcia Pasin[2] and Amal El Fallah Seghrouchni[3]
[1]*Institut Polytechnique des Sciences Avancées, IPSA, Ivry-sur-Seine, France*
[2]*Universidade Federal de Santa Maria, Santa Maria, Brazil*
[3]*Sorbonne Université, Paris, France*

Keywords: Secure Traffic Regulation, SUMO, Central Communication Coordinator (CCC).

Abstract: In this paper, we propose a solution for traffic regulation in Intelligent Transportation Systems (ITS). Due to the heterogeneity and dynamic nature of transportation networks, the big challenge is to be able to take the correct decisions to smooth the traffic flow. This decision is at the same time centralized within a Central Communication Coordinator (CCC) which is in charge of controlling the traffic lights and also distributed among the vehicles that are in the nearby of cross section. The decision should be made upon a permanent exchange of information between the vehicles and the CCC's. Thus, an important issue is to ensure a robust and secure communication between the different components able to resist to hypothetic hacker's attacks. The aim of this paper is to setup an intelligent system to regulate traffic flow taking into account different types of attacks. We show in this paper our simulated results using the client MATLAB together with the server SUMO (Simulation of Urban Mobility) so that client can access and modify the simulation environment. We simulated one intersection using an algorithm to regulate the traffic and explain our obtained results.

1 INTRODUCTION

Traffic congestion is a major constraint nowadays. In many big cities, traffic jams are daily reported, and chaotic transit in the main avenues during rush hours is usual. The situation is even worse in the beginning and the end of holidays. During such traffic jams, which can exceed hundreds of kilometers, people lost many hours in their journey just waiting in their cars.

There is a lot of cause for traffic jam, one of them is caused by traffic lights (TLs). The latter can generates traffic deadlock in an intersection and can affect other intersections. Therefore, TLs can be removed to improve traffic[1]. Drivers waste time waiting at the red light.

However, TLs can also be used to regulate traffic and to reduce traffic jams at road intersections. Recently TLs were installed to reduce traffic jams in an intersection in Nantes, France[2]. Basically, in this case, the TL regulates the traffic when a collector road reaches the motorway. TLs were also introduced with the same objective in Grenoble, France[3]. Moreover, one third of the accidents in France are caused by the fact that the drivers ignore the red signal.

In a near future, with the fully implementation of the Vehicular Ad hoc NETworks (VANETs) technology, vehicles will exchange messages and collaborate to achieve more efficient strategies to deal with intersection control and route planning, and to possibly collaborate to reduce time travels and traffic jams. VANETs pose new challenges to transportation networks (Eze and Liu, 2014). For instance, maintaining a huge set of cars communicating with each other is not a trivial task. Due to the heterogeneity of Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication devices and the complexity of the exchanged information, it is difficult to formalize, to model and to design solutions to achieve the required needs.

Therefore, the need for standardized solutions to deal with this heterogeneity is an issue, since these devices will provide information consumed by other VANETs services.

On the other hand, several potential threats to ve-

[1] https://www.aol.co.uk/2017/02/14/paris-removes-traffic-lights-to-fix-congestion-and-improve-safety/

[2] https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/circulation-les-feux-anti-bouchon-s-allument-ce-lundi-nantes-4917955

[3] https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/feux-regulation-limiter-bouchons-rocade-sud-grenoble-1082649.html

Belbachir, A., Benabid, S., Pasin, M. and Seghrouchni, A.
Preliminary Results for Secure Traffic Regulation.
DOI: 10.5220/0006904504190424
In *Proceedings of the 15th International Conference on Informatics in Control, Automation and Robotics (ICINCO 2018) - Volume 2*, pages 419-424
ISBN: 978-989-758-321-6

hicular communication network exist, ranging from fraudulent messages capable of disrupting traffic, or even causing danger to driver or to its environment. Traffic infrastructure and involved vehicles must be resilient against intruders that potentially generate disruption, degrade safety, or gain an unfair advantage (Ghena et al., 2014).

In this direction, this paper proposes a novel solution for secure traffic regulation. We define the concept of a Central Communication Coordinator (CCC), a trust unite which is responsible to regulate the traffic in one intersection (see Figure 1). A CCC can be implemented in the infrastructure and will get information from the cars and other infrastructures which are in the vicinity of a given intersection (e.g. traffic light). The problem here is that a CCC regulates the traffic for only one intersection. Due to its decision it can generate other traffic jams for other intersections. Thus, the CCCs need to communicate with each other. However, such exchange of information may cause some overhead due the need of communication and processing. Thus, CCCs need to decide whether to communicate all other CCCs or with a restricted number of CCCs. In this paper, we are investigating only one intersection. The focus is on the communication protocol among cars and a given CCC.

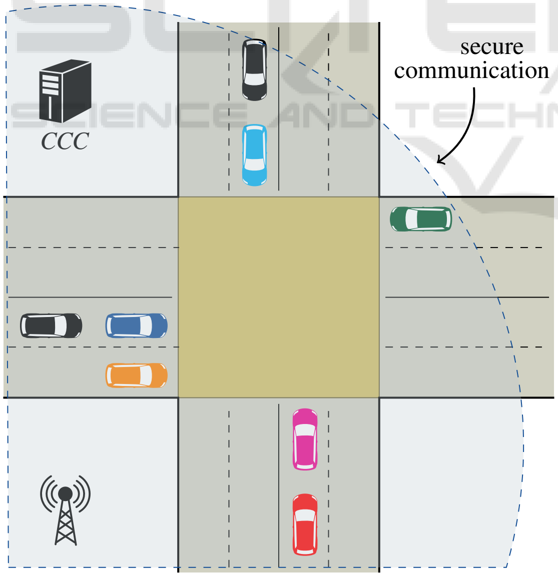

Figure 1: The Central Communication Coordinator (CCC) and vehicles with communication support in a one intersection scenario.

Additionally, cars should be able to organize themselves and exchange information in a secure way. In this sense, our paper defines a different secure way to exchange information between cars, CCCs and vice-versa. Then, we propose a solution to avoid deadlock for traffic jam with regard to one intersection.

We evaluate our proposal through simulation. For our simulations we used SUMO (Simulation of Urban Mobility) (Behrisch et al., 2011). SUMO is an open source road traffic simulation package designed to model the flow of vehicle traffic by treating different realistic cases associated with MATLAB. SUMO can handle large environments, with complex structures using 10.000 streets, and it can import many network formats such as XML for example.

The paper is divided into five sections. Section two, state the actual work on traffic regulation. The third part explain the contribution of our work using one intersection and a secure way of data exchange. The fourth part explain our evaluation and simulated results. Finally, we conclude our work.

2 STATE OF THE ART

Previous researches have suggested VANETs as a way to enable V2V communications and to allow information exchange and other types of information among vehicles (Rawat et al., 2014) (Chembe et al., 2017). Several communication protocols have been proposed for V2V and V2I communication such as Wireless Access in Vehicular Environments (WAVE) and Dedicated Short Range Communications (DSRC). WAVE and DSRC standards are defined in IEEE 1609.1-4 and 802.11p respectively. The U.S. Federal Communication Commission (FCC) has allocated, in 1999, dedicated 75 MHz frequency spectrum in the range 5.85 GHz to 5.925 GHz to be used exclusively for V2V and V2I communication. The DSRC spectrum is divided into seven channels with a 10 MHz bandwidth allocated to each one. Six out of these channels are service channels (SCH) and the center one is the control channel (CCH).

However, security aspects need to be taken into account for traffic regulation and VANETs. A survey by (Karagiannis et al., 2011) introduced the basic characteristics of VANETs, and provided an overview of applications and their requirements, along with challenges and proposed solutions. The authors highlight vehicle communication security capabilities such as mechanisms to maintain privacy and anonymity, integrity and confidentiality, resistance to external attacks, authenticity of received data, data and system integrity.

(Hasrouny et al., 2017) focus on VANET security characteristics and challenges as well as existing solutions. They present a classification of the different attacks a VANETs may suffer such as authentication, availability by resisting to DoS (Denial of Service) attacks, confidentiality, non-repudiation, integrity, privacy, data verification, access control, traceability and revocability, error detection, liability identification, flexibility and efficiency despite of timing constraints. Moreover, VANETs need to be resilient against a series of attacks including: DoS, malwares, spam, man in the middle attack, injection of erroneous messages, cheating with position information, etc.

In fact, cars with selfish behavior and malicious attacks may impact on the expected traffic performance. For instance, a malicious node can steal frames transmitted from cars or from the infrastructure. A malicious node can also propagate a malicious message to disturb traffic behavior. Selfish cars can take benefit of cheating aiming to arrive first. Fortunately, due to the special characteristics of VANETs and their dynamic nature, cheating cars cannot choose which cars they will interact. Thus, spread lies might become irrelevant as more participating cars receive recent information (Lin et al., 2007). However, it is not yet clear how malicious nodes will influence in intersection control protocols.

(Lin and Li, 2013) proposed a cooperative authentication scheme for VANETs using a reward approach implemented by a Trusted Authority (TA). The TA receives the messages from vehicles when vehicles pass by the Road Side Units (RSUs), and it sends back new messages to the vehicles based on their past rewards. The vehicles obtain a reward as they make contribution to the network.

A more recent work (Lim and Manivannan, 2016) presents a protocol for fast dissemination of authenticated messages to propagating phenomena in VANETs. Phenomena messages are used to propagate accidents, road conditions, etc. RSUs disseminate authenticated messages about the observed phenomena by vehicles in RSU transmission range. RSUs are TAs and can verify the authenticity of the sender and the message integrity before message dissemination. Messages sent by vehicles do not require authentication and verification by other vehicles. The aim of the protocol is to ensure the anonymity of the senders and also to allow a mechanism to trace the messages, when required, for law enforcement agencies, for instance.

Centralized system represents single point of failures (SPOF) and, therefore, worthwhile targets for attackers. Alternatively, decentralized solutions based on new technologies can be proposed.

In this direction, blockchain is a promising distributed architecture to build reliable solutions to Intelligent Transportation Systems (ITS). In Block-VN (Sharma et al., 2017), participating entities have different behaviors. Controller nodes provide necessary services on a large scale communication, miner nodes deal with communication issues, and other nodes are just ordinary nodes (vehicles, for instance). Ordinary nodes send a service request message to other vehicles or for the controller nodes. Using this communication hierarchy in a distributed way, scalability and high availability are expected to be achieved. Block-VN also aims to improve security using trusted intermediary services and by providing distributed, secure, and shared records of all system actions.

(Leiding et al., 2016) also suggests the application of blockchain to deal with ITS challenges. Traffic regulations algorithms can be implemented with the support of Ethereum high-level languages. Based on information about cars and traffic conditions, it is possible to identify and punish misbehaving cars. This might include high speeding, ignoring traffic lights, causing an accident, etc. Each car will be identified by its unique public key. Thus, a punishment can be imposed to the car (or driver) with such corresponding Ethereum account.

However, the blockchain theory is not yet mature. Scalability is still a criterion to be more investigated further. Another important issue is that VANETs are subject to intense churn (nodes are coming in and out all the time) and it is not yet known if this behavior will be efficiently handled by the blockchain technology.

3 SECURE TRAFFIC REGULATION STRATEGY

In this section, we explain the main contribution of our work using one intersection and a secure way of data exchange.

3.1 Traffic Regulation Algorithm

The CCC is a TA and communicates with vehicles and the infrastructure. The used infrastructure is the TL. The CCC controls the TLs state duration and transition according to the ratio (*rap*) between flows. Algorithm 1 represents the used function to regulate the TL for one intersection. The number of vehicles on the entrance (E) and the exit (S) of a road for each direction (North, South, East and West) is given in the following variables: EN, ES, EE, EO, ..., etc. *rap* is computed using the ratio between the vehicle's number which is entering to the intersection in a vertical lane (EN, ES) and the horizontal lane (EE, EO) (see Figure 3).

The counter shows how long the TL has not changed its state. GreeenLight (NSALL) and Green-

Light (EOALL) represent respectively the green light state for the two TLs in the vertical lane (EN, ES) and the horizontal lane (EE, EO). We predefined a minimum and a maximum TL state to green color as follow: MIN and MAX u.t (unit of time). The procedure is changing the traffic light color according to the ratio (*rap*) and the counter (*C*) duration. When the traffic is dense at *EN* and *ES* compared to *EE* and *EO* the green light state is activated. Otherwise, and according to *rap* value the green light state of *EN* and *ES* is activated.

Algorithm 1: Traffic light regulation algorithm.

```
C: represents a counter
S: represents a state
procedure TRAFFIC REGULATION ($C,S,EN,ES,EE,EO,SN,SS,SE,SO$)
    if (EE + EO) $\neq 0$ then
        $rap \leftarrow (EN+ES)/(EE+EO)$
    else
        $rap \leftarrow 100$
    if ($C < MAX$ and $rap > 1.5$) or $C < MIN$ then
        $C \leftarrow C+1$
        GreenLight(NSAll)
        if S $\neq$ NSAll then
            $C \leftarrow 0$
            $S \leftarrow NSAll$
    else if ($C < MAX$ and $rap < 0.66$) or $C < MIN$ then
        $C \leftarrow C+1$
        GreenLight(EOAll)
        if S $\neq$ EOAll then
            $C \leftarrow 0$
            $S \leftarrow EOAll$
    else if $C = MAX$ or $C = MIN$ then
        $C \leftarrow 0$
        if S = NSAll then
            GreenLight(EOAll)
            $S \leftarrow EOAll$
        else if S = EOAll then
            GreenLight(NSAll)
            $S \leftarrow NSAll$
```

3.2 Hacking Scenario's

Denial of Service (DoS) consists in making different resources and services for users in the network unavailable; it is usually caused by other attacks on bandwidth or energy resources of other vehicles. It is necessary to supervise and detect DoS in order to avoid an incident. DoS attacks can lead to abnormal conditions, preventing, intercepting or blocking communication between vehicles in a VANET. In our case, we consider the CCC as an important unit which is able to attribute services to all vehicles for one intersection.

Figure 2 depicts a service demand by a malicious vehicle *m*. The *m* asks several services to the CCC which makes the CCC busy. When a vehicle *v* asks for one service, the CCC denies the requested service. To resolve this problem, we delimited a number of requested services. Each vehicle can ask one service at a time.

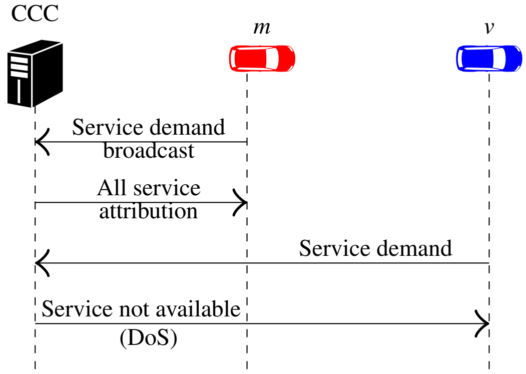

Figure 2: Denial of Service using our scenario.

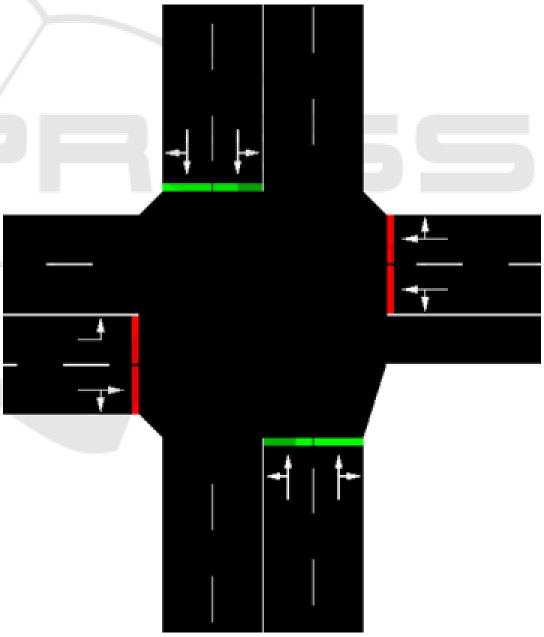

Figure 3: Two double-handed lanes and an intersection.

4 EXPERIMENTAL EVALUATION

Map Definition

The scenario used in the experiments has two roads. Both roads share a single intersection and have four lanes. In each road, two lanes are from South/East to North/West and two are on the opposite flow. This

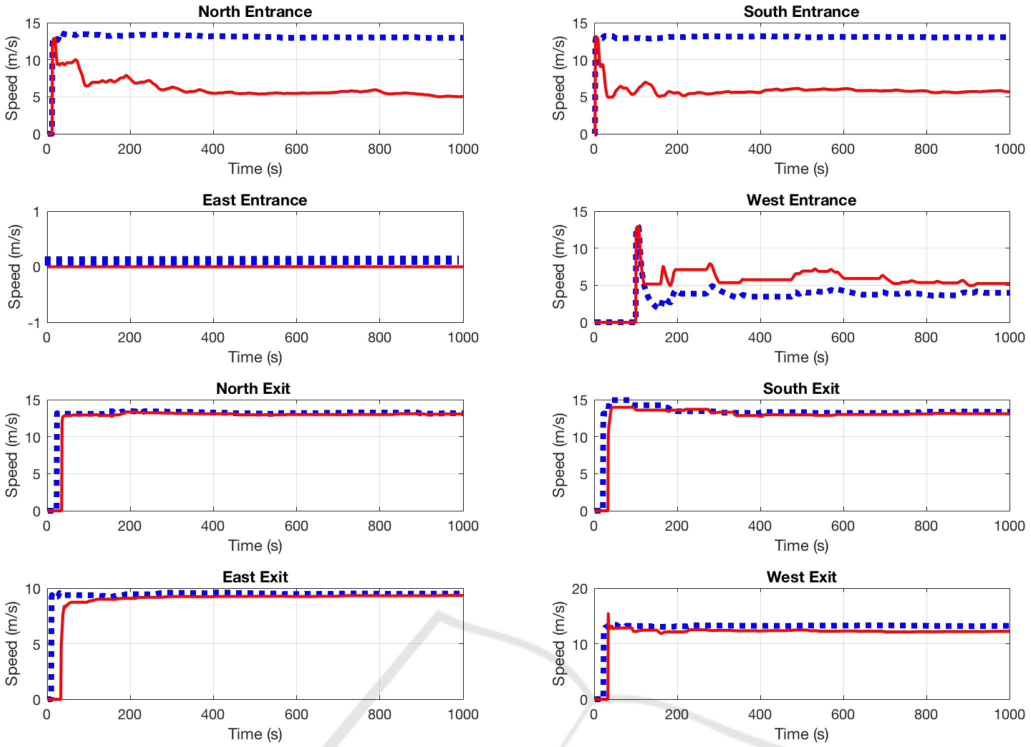

Figure 4: Vehicles average speed for each direction with and without optimal traffic lights control using Matlab based on SUMO simulations.

scheme is shown in Figure 3. To implement these roads, we used SUMO, TraCI4Matlab and Matlab.

Experiments

The system simulations were done in Matlab environment. TraCI4Matlab is built on top of the TCP/IP stack, implemented on Traffic Control Interface (TraCI) application level protocol. It connects the client MATLAB together with the server SUMO so that client can access and modify the simulation environment. TraCI4Matlab allows MATLAB to take control of SUMO objects such as vehicles, traffic lights, etc., providing users a testbed to evaluate traffic lights control protocol or any other related traffic algorithm.

We compare, in Figure 4, the vehicles average speed on their roads for each direction (EN, ES, EE, EO, SN, SS, SE and SO). This comparison is related to two cases of study: traditional and optimal traffic lights control. The first case of study is represented in the continuous line, the second one in discontinuous line. The latter uses the developed algorithm given in section 3.1. We replace the two values MIN and MAX from the algorithm by 15 and 50 u.t (unit of time). The statistical obtained results are shown in Figure 4 where the simulation duration is around 17 min (1000 s). We can notice that the average speed is higher in the optimal case than in the traditional one for most of the directions.

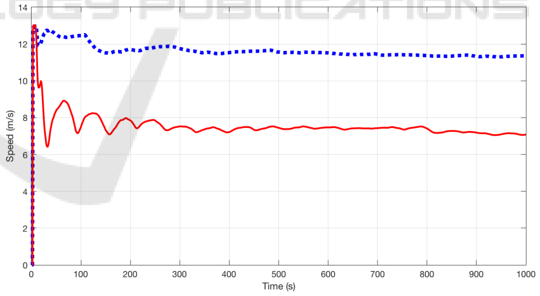

Figure 5: Vehicles average speed simulation for the whole itinerary with and without optimal traffic lights control.

To confirm this result, we performed a simulation for the whole vehicles trajectory. Figure 5 shows the obtained result. As we can see, the average speed in the traditional case is $7m/s$ while in the optimal case is $11m/s$. This result is improving the vehicle average speed by around $4m/s$. In other words, the vehicle's speed is improved by 36% compared to the traditional one. Therefore, the optimal traffic lights control greatly improves the road traffic.

5 CONCLUSIONS

In this paper we presented an algorithm to regulate the traffic for one intersection in ITS. This developed algorithm is at the same time centralized within a CCC which is in charge of controlling the traffic lights and also distributed among the vehicles that are in the intersection. We also introduce one hacking scenario and our proposed resolution. In order to test the proposed algorithm, we implemented it on Matlab and connected with SUMO. TraCI4Matlab is built on top of the TCP/IP stack, implemented on Traffic Control Interface (TraCI) application level protocol. It connects the client MATLAB together with the server SUMO so that client can access and modify the simulation environment. The obtained results shown that our implemented algorithm improves the vehicles speed and regulate the traffic better than the classical regulation traffic algorithm. This result is encouraging and is pushing us to implement the approach on robot cars.

REFERENCES

Behrisch, M., Bieker, L., Erdmann, J., and Krajzewicz, D. (2011). SUMO: simulation of urban mobility (an overview). In *Proceedings of the Third International Conference on Advances in System Simulation (SIMUL 2011)*, pages 63–68.

Chembe, C., Noor, R. M., Ahmedy, I., Oche, M., Kunda, D., and Liu, C. H. (2017). Spectrum sensing in cognitive vehicular network: State-of-art, challenges and open issues. *Computer Communications*, 97:15 – 30.

Eze, S. Z. E. C. and Liu, E. (2014). Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward. In *Proceedings of the 20th International Conference on Automation and Computing*, pages 176–181.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., and Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, San Diego, CA. USENIX Association.

Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A. (2017). Vanet security challenges and solutions: A survey. In *Vehicular Communications, Volume 7*, pages 7–20.

Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., and Weil, T. (2011). Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. In *IEEE Communications Surveys & Tutorials, 13 (4)*, pages 584–616.

Leiding, B., Memarmoshrefi, P., and Hogrefe, D. (2016). Self-managed and blockchain-based vehicular ad-hoc networks. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, UbiComp '16, pages 137–140, New York, NY, USA. ACM.

Lim, K. and Manivannan, D. (2016). An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks. In *Vehicular Communications, vol. 4*, pages 30–37.

Lin, R., Kraus, S., and Shavitt, Y. (2007). On the benefits of cheating by self-interested agents in vehicular networks. In *Proceedings of the 6th International Joint Conference on Autonomous Agents And Multiagent Systems (AAMAS 2007), New York, NY, USA*, pages 327–334.

Lin, X. and Li, S. (2013). Achieving efficient cooperative message authentication in vehicular ad hoc networks. In *IEEE Transactions on Vehicular Technology, 62 (7)*, pages 3339–3348.

Rawat, D. B., Bista, B. B., Yan, G., and Olariu, S. (2014). Vehicle-to-vehicle connectivity and communication framework for vehicular ad-hoc networks. In *2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, pages 44–49.

Sharma, P. K., Moon, S. Y., and Park, J. H. (2017). Block-vn: A distributed blockchain based vehicular network architecture in smart city. In *Journal of Information Processing Systems, vol. 13, no. 1*, pages 184–195.