Secure Enforcement in Cognitive Internet of Vehicles

Yongfeng Qian, Min Chen, *Senior Member, IEEE*, Jing Chen,
M. Shamim Hossain, *Senior Member, IEEE*, and Atif Alamri

***Abstract*—As for deployment of security strategy, corresponding forwarding rules for switches can be given in allusion to different traffic conditions. However, due to lack of global cognitive control for security strategy deployment in traditional Internet of Vehicles (IoV), it is quite difficult to realize global and optimized security strategy deployment scheme so as to meet security requirements in different traffic conditions. On basis of traditional IoV, cognitive engine is added in cognitive IoV (CIoV) to enhance the intelligence of traditional IoV. In allusion to CIoV, and in consideration of restrictions on transmission delay, the security strategy deployment for switches on core network is formulated in this paper, thus not only the safe transmission rules are met, but the transmission delay can also be the lowest. To be specific, the path selection of switches is modeled as 0-1 programming problem in this paper, and that optimization problem is proved to be a nonconvex optimization problem. Then we convert that problem into a convex optimization problem by log-det heuristic algorithm, thus to give path selection scheme to meet security requirements with the lowest delay on the whole. Experiment proves that cognitive engine-based security strategy deployment put forth in this paper is much better than other schemes.**

***Index Terms*—Cognitive engine, delay sensitive, Internet of Vehicles (IoV), security enforcement, traffic analysis.**

I. Introduction

As PER the Gartner report, there would be a quarter billion vehicles with access to Internet of Vehicles (IoV) in 2020, to guarantee in-vehicle services and functions such as automatic driving. As an integrated application of IoT [1], [2] and artificial intelligence, IoV is the basis for realization of intelligent transportation in future [3]. With popularization of IoV [4], however, security problem needs to be first consideration in actual deployment of IoV [5]–[7]. Intrusion Detection System (IDS) based on traffic monitoring, for instance, can detect abnormal traffic and send alarm [8]. In addition, Privacy preserving is an indispensable measure for IoV [9]. Generally, IoV would provide different services such as Location-Based Services (LBSs) to user, which requires user to provide accurate location information [10]. However, this kind of information is sensitive and private for users, though users wants to obtain LBSs, they may be worried about leaking their real location [11]–[13]. If no appropriate privacy preserving measures were designed, malicious user may acquire sensitive information of legal users, and privacy of legal users may be revealed [14]. Therefore, in order to solve those problems on IoV, fine-grained security strategy deployment scheme should be designed. Liu *et al.* [15] shows that traffic forwarding rules can illustrate security strategy. Thus, in this paper, we convert security strategy deployment into discover corresponding forwarding strategy in allusion to different traffic categories.

However, for traditional IoV, there are mainly two challenges for deployment of security strategy.

1) Due to lack of global control, the global optimized deployment can not be achieved during deployment of security strategy. Though software defined network (SDN) is put forth as a new network model [16] to realize flexible design [17], it is still difficult for SDN to further optimal enforcement due to restrictions of SDN controllers [18]. For example, Ding *et al.* [19] utilized SDN to put forth security enhancement policy for wireless mobile network. But due to the unintelligent controllers, it is not easy to realize global optimized deployment actually.
2) During security strategy deployment, time delay should be taken into consideration [20]. Commonly, security strategy deployment only considers the allocation scheme corresponding to current traffic condition, but the time delay for path selection is seldom taken into consideration. However, time delay would influence users' quality of service (QoS), and high transmission delay would lower user experience [21]. Therefore, time delay is a critical factor, which should be considered carefully, in the process of security strategy deployment.

For cognitive IoV (CIoV), security strategy deployment can be realized due to global perception function of cognitive engine [22]. Furthermore, optimal traffic transmission strategy can represent security enforcement. Therefore, with the help of cognitive engine, the transmission rules in all

Manuscript received November 20, 2017; revised January 14, 2018; accepted January 22, 2018. Date of publication February 5, 2018; date of current version April 10, 2018. *(Corresponding authors: Min Chen; M. Shamim Hossain.)*

Y. Qian and M. Chen are with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: yongfeng@hust.edu.cn; minchen2012@hust.edu.cn).

J. Chen is with the Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Computer School, Wuhan University, Wuhan 430072, China, and also with the Science and Technology on Communication Security Laboratory, Chengdu, China (e-mail: chenjing@whu.edu.cn).

M. S. Hossain and A. Alamri are with the Research Chair of Pervasive and Mobile Computing, King Saud University, Riyadh 11543, Saudi Arabia, and also with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2018.2800035

switches can be formulated, and the optimal path selection can be given.

This paper discusses security strategy deployment problem for CIoV. To be specific, in order to deploy traffic transmission rules in OpenFlow-enabled switches [23], cognitive engine is first adopted to perceive category of different traffic conditions. Considering limited capacity of switches, we describe an optimal path selection scheme with lowest time delay under restriction of safe transmission for different traffic. The main contributions of this paper are as follows.

1) To the best of our knowledge, this is the first time to consider security strategy deployment problem in allusion to CIoV. This paper develops an secure and delay-sensitive transmission scheme, with the help of cognitive engine. The security strategy deployment problem is modeled as 0-1 programming problem, which is proven to be a nonconvex problem. Then, this nonconvex optimization problem is converted into a convex optimization problem by log-det heuristic algorithm. Finally, the global optimal solution is given, i.e., the path selection scheme with the lowest delay is given on premise of meeting safe transmission rules.
2) It has proved in simulation experiment that the security strategy deployment scheme on CIoV is better than that on traditional IoV.

The organization structure of this paper is as follows. Section II introduces related work. Section III illustrates security strategy. Section IV evaluates the performance of cognitive engine-based CIoV. Section V discusses open issues, and Section VI summarizes this whole paper.

II. Related Work

This section mainly introduces related work, and it is divided into two parts: 1) security strategy deployment on traditional IoV and 2) cognitive engine.

A. Security Strategy Deployment on Traditional IoV

In aspect of security strategy deployment, traditional intrusion detection method is more focused on conditions in allusion to stable network traffic. For example, the unsupervised learning-based intrusion detection system put forth by Bostani and Sheikhan [24] enhances false alarm rate and execution time when compared with traditional methods. A new feature expression method is put forth by Lin *et al*. where two kinds of distance (distance between each data point and cluster center, and distance between each data point and its nearest neighbor) are calculated. On this basis, a new distance is given to express each data point, then intrusion detection is conducted, and higher detection rate is acquired [25].

However, on IoV, due to diversity in type of IoV services, such as location-based services, entertainment information, path recommendation and etc., and difference in terminal devices, the generated traffic would appear great difference when IoV is under different attacks. If traffic monitoring and analysis is conducted based on above-mentioned method, the accuracy rate would necessarily decrease, and users' experience would be reduced. As Electronic Control Units (ECUs) on IoV tend to be compromised, anonymity-based intrusion detection system is put forth in [26], to detect any abnormal behavior.

B. Cognitive Engine

Mitola and Maguire [27] proposed that interaction and awareness between cognitive radio and wireless communication network environment can be conducted based on cognitive cycle, thus to realize adaptivity to corresponding wireless environment. Various parameters can be changed through self-organization, and corresponding autonomic cognitive process can be established at last. Software defined cellular network is put forth by Zhou *et al.* [28], in allusion to ever-increasing amount of data, to realize unified intelligent management, which endows cognitive engine with intelligent functions.

Cognitive engine can be established based on cloud platform, so it has massive storage and computing capacity. In the meantime, different branches of cognitive engine can be deployed according to business requirements, to meet requirements of users.

III. Security Policy Enforcement in CIoV

The architecture of CIoV will be first introduced, and then security strategy deployment scheme on CIoV will be introduced.

A. CIoV

Fig. 1 describes key component of CIoV. It can be seen from Fig. 1 that the whole CIoV is divided into three layers: 1) physical layer; 2) core network layer; and 3) cognitive engine layer. To be specific,

1) Physical layer is composed of Road Side Unit (RSU) and vehicles. During driving process, the communication between a vehicle and RSU can be conducted, and the communication between a vehicle and another vehicle can also be conducted. The former communication mode is called vehicle to RSU (V2R) and the latter is called vehicle to vehicle (V2V). In this paper, IEEE 802.11p is adopted as the communication mode. The physical layer of CIoV can realize data perception and implement local data preprocessing, etc. CIoV is more focused on user experience and quality of services provided. Therefore, in physical layer of CIoV, in addition to collecting data such as images, videos and voice requried by traditional IoV, the data collected also include physical signs, such as expressions and heart beats for comprehensive emotion detection for drivers, according to different requirements of diverse applications. However, as the smart brain for IoV (it will be introduced in details later), cognitive engine can guide physical layer in type of data to be collected. The data on CIoV are multidimensional temporal and spatial data, and high users' experience will be provided through cognitive engine.
2) The middle layer is core network layer. This layer is mainly composed of fronthaul network (communication

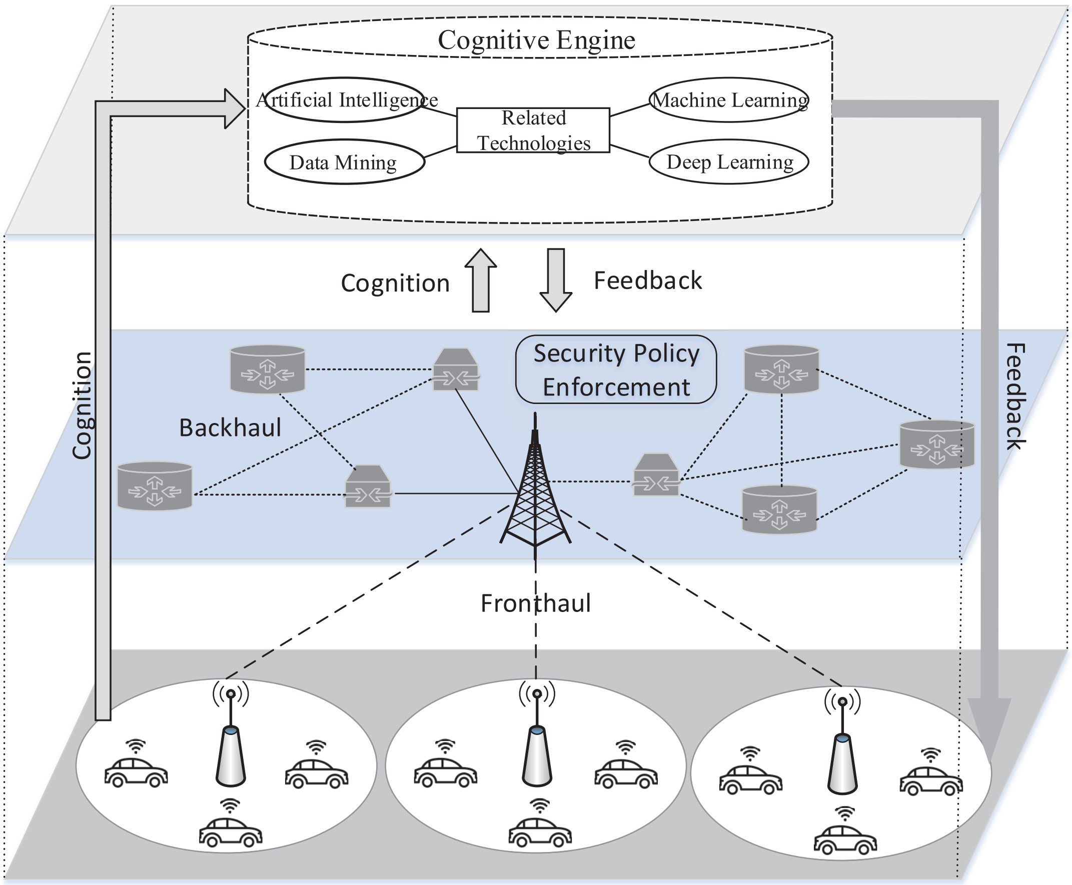


Fig. 1. Illustration of cognitive Internet of Vehicles.

from RSU to base station) and backhaul network (connection between base station and gateway, between router and switches). When we discuss security strategy deployment in this paper, the switches in backhaul network are OpenFlow-enabled switches by default. Thus, forwarding strategy in switches can be defined. While our proposed security policy exactly makes use of such feature of OpenFlow-enabled switches, security enforcement policy can be deployed directly on switches. Then, the optimization algorithm can make switches forward traffic according to requirements. These advantages are what traditional switches do not have. In fact, OpenFlow-enabled switches utilized the idea of software defined network (SDN). Similarly, Salahuddin *et al.* [29] discussed how to utilize SDN to build RSU Cloud and adding OpenFlow switches in IoV.

3) The highest layer is cognitive engine layer. Cognitive engine is smart brain on CIoV, and it can realize personalized services for users. However, the technologies that support cognitive engine are artificial intelligence, data mining, machine learning, deep learning, reinforcement learning, etc. With strong learning ability, cognitive engine can give comprehensive analysis in allusion to multidimensional data perceived in physical layer. Specifically, cognitive engine is smarter controller compared with traditional SDN controller. Cognitive engine can perceive the change of intermediate layer traffic, such as the delay sensitivity of traffic, the real time load of switches, etc. These data will be the labeled data for these learning algorithms. Therefore, cognitive engine utilizes these labeled data to conduct artificial intelligence and machine learning algorithm to dynamically deal with the deployment of secure policy. For example, cognitive engine can use the support vector machine (SVM) to classify new traffic and conduct corresponding processing if the new traffic belongs to some similar categories. Otherwise, cognitive engine will deal with the new traffic further according to user's needs, such as adding it to original data set. Furthermore, cognitive engine also conducts feedback to physical layer and core network layer, thus to enable physical layer to timely update perceived data. As for core network layer, with the help of cognitive engine, security strategy deployment can be updated corresponding to updated traffic.

B. Optimization Algorithm

On CIoV, cognitive engine can perceive deployment requirements of different security strategies, conduct optimized deployment for security policy in switches, and realize minimum transmission delay for whole network, in combination

TABLE I
NOTATION

Parameters	**Definition**
n	Number of switches
$S_i, i = 1, 2, \cdots, n$	Switches
$G(V, E)$	graph model, wherein $\lvert V \rvert = n$
$e(S_i, S_j), i, j \in \{1, 2, \cdots, n\}$	Connection between S_i and S_j
$B(e)$	Available bandwidth for $e(S_i, S_j)$
$C_i, i \in \{1, 2, \cdots, n\}$	Capacity of S_i
m	Number of different traffic type
$T_i, i \in \{1, 2, \cdots, m\}$	i-th traffic
$V_i, i \in \{1, 2, \cdots, m\}$	All T_i
$\theta_i, i \in \{1, 2, \cdots, m\}$	Security sensitivity of T_i
$\widetilde{\omega}_{i,j}$	Proportion of T_i allocated to S_j
$\omega_{i,j}$	Standardization of $\widetilde{\omega}_{i,j}$
$P_{i,j}$, $i \in \{1, 2, \cdots, m\}$, $j \in \{1, 2, \cdots, l_i\}$	Possible forwarding path of T_i
$r_{i,j}$, $i \in \{1, 2, \cdots, m\}$, $j \in \{1, 2, \cdots, l_i\}$	Rate allocated to$P_{i,j}$
$Path_i, i \in \{1, 2, \cdots, m\}$	All forwarding path of T_i
$\phi(x)$	Identify function

with traffic information in switches in bottom layer. To be specific, this paper mainly concerns path selection of switches on core network to guarantee minimum network delay and safe transmission, with the restricted resources of switches and global view of cognitive engine. For this purpose, the path selection of switches is modeled as a 0-1 programming problem, and the problem is converted into convex optimization problem by Log-det heuristic algorithm. The path selection scheme that meets safe requirements with minimum delay is given on the whole. Table I shows the symbols used in this paper.

C. Problem Formulation

Assume switches involved on CIoV are all Open Flow-enabled switches. For the sake of simplicity, "switch" below stands for OpenFlow-enabled switch. Define the number of switches on CIoV as n. Set $S = \{S_1, S_2, \ldots$ and $S_n\}$ stand for all switches. Core network can be expressed by graph model $G(V, E)$, thereinto, V stands for node, i.e., switches, $|V| = n$. E stands for edge between switches. The edge between S_i and S_j can be expressed by $e(S_i, S_j)$, whose value is

$$e\big(S_i, S_j\big) = \begin{cases} 1, & \text{Connected directly between } S_i \text{ and } S_j \\ 0, & \text{Otherwise.} \end{cases} \tag{1}$$

Note B as the available bandwidth of E, that is $B = \{B(e(S_i, S_j))\}$, wherein $B(e(S_i, S_j))$ stands for the available bandwidth of $e(S_i, S_j)$. C_i, where in $i = 1, 2, \ldots, n$, denotes capacity of switch S_i. $T_1, \ldots, T_m$ stand for all categories of switches. The total number of each T_i is $V_i, i = 1, 2, \ldots, m$. As data represented by traffic are different, the security sensitivity is different. For example, on CIoV, a user generates traffic containing sensitive data, then this kind of traffic should be transmitted preferentially. In other words, the security sensitivity for this kind of traffic is high, and the transmission delay should be controlled in a smaller scale. In addition, in allusion to normal traffic, cognitive engine would perceive it and give corresponding security sensitivity. For example, the security sensitivity generally endowed with data flow that requires normal passing or forwarding would be lower, and higher security sensitivity would be endowed with data flow that requires dropping. In order to quantify these weights, note the weight of each kind of traffic as θ_i, and its value stands for sensitivity of traffic on security. If the value of θ_i is higher, the requirements of T_i on security are higher, so T_i needs preferential consideration. On the contrary, the requirements of T_i on security are lower. On CIoV, the sensitivity of different traffic conditions on security is perceived through cognitive engine; the value of $\theta_i, i = 1, 2, \ldots, m$ can be given after comprehensively weighing degree of importance and security requirements of traffic. $\widetilde{\omega}_{i,j}$ stands for the proportion of task load assigned by traffic T_i to switch S_j, and its value is between 0 and 1. As the quantity of switches needed by each kind of traffic T_i is limited, in other words, only several switches are needed to forward T_i, these several switches can be recorded as $\{S_{i_1}, S_{i_2}, \ldots, S_{i_{d_i}}\}$. However, some other switches S_k (thereinto, $\{S_k | k \in \{1, 2, \ldots, n\} - \{i_1, i_2, \ldots, i_{d_i}\}\}$) would not process T_i. For the sake of unification, all switches are taken into consideration, i.e., standardization is conducted to $\widetilde{\omega}_{i,j}$. Record $\omega_{i,j}$ as

$$\omega_{i,j} = \begin{cases} \widetilde{\omega}_{i,j}, & S_j \text{ can handle } T_i \\ 0, & \text{Otherwise.} \end{cases} \tag{2}$$

In this way, as for T_i, $\omega_{i,j} = 1$ shows that switch S_j is required to forward T_i, then, switch S_j needs to meet forwarding rules of traffic volume T_i. Therefore, we can say S_j meets safe forwarding requirements of T_i. It is because the forwarding of this T_i can be directly dropped or reported to cognitive engine if there is no forwarding rules for T_i in S_j. This forwarding rules shall be cached in S_j temporarily, then too high delay may be caused until T_i is under processing, thus the quality of service of user may be influenced. $\omega_{i,j} = 0$ shows that switch S_j need not to forward T_i. Then, forwarding rules for T_j should not be deployed in advance in S_j, or unnecessary waste will be caused. It is because the resources in each switch are limited, only rational utilization of switch resources can guarantee effective deployment of forwarding rules. In fact, it is put forth by Liu *et al.* [15] that each security strategy can be converted into specific flow entries in switch, therefore, the deployment of security can be converted into formulation of forwarding rules for traffic volume in switches.

As for traffic T_i, all possible forwarding paths are expressed as $P_{i,1}, P_{i,2}, \ldots, P_{i,l_i}$. Note Path$_i$ as all paths for T_i. Assume $D_{i,j}$ is delay for path $P_{i,j}$, and $r_{i,j}$ stands for the rate of allocation to $P_{i,j}$, thereinto, $j \in \{1, 2, \ldots, l_i\}$. Assume the specific rate allocated to each T_i is R_i.

D. Model Formation

Our aim is to establish a forwarding path that meets security requirements with minimum delay. Actually, the delay that considered in this paper is mainly the transmission time between switches. Thus, the path delay t_{Path_j} can be defined as follows:

$$t_{\text{Path}_j} = \sum_{k=1}^{l_j} \theta_j D_{j,k} \Phi\left(r_{j,k}\right) \tag{3}$$

wherein $\phi(\cdot)$ is identify function as follows:

$$\phi(x) = \begin{cases} 1, & x > 0 \\ 0, & x = 0. \end{cases} \tag{4}$$

When $r_{i,j} > 0$, it means rate is allocated to path $P_{i,j}$, i.e., this forwarding path is adopted, then $\phi(r_{i,j}) = 1$. When $r_{i,j} = 0$, it means path $P_{i,j}$ is not adopted. When forwarding path is selected, switches involved in the path should meet security requirements, i.e., when $r_{i,j} > 0$, $\omega_{i,j} = 1$ should be met. In other words, when the possibility where path $p_{i,j}$ is allocated for traffic T_i is $r_{i,j}$, then forwarding rules for T_i must be deployed in switches involved in the path, i.e., $\omega_{i,j} = 1$, which meets security requirements of traffic T_i.

Hence, global optimization problem can be obtained under global control of cognitive engine, thus to guarantee minimum delay on premise of meeting security requirements. The optimal problem can be formulated as

$$\underset{\mathbf{r_{i,j}}}{\text{minimize}} \quad f\left(r_{i,j}\right) = \sum_{i=1}^{m} t_{\text{Path}_i} + \eta \sum_{i,j} \phi\left(r_{i,j}\right) \tag{5a}$$

$$\text{subject to} \quad \sum_{j=1}^{l_i} r_{i,j} \le R_i, i \in 1, 2, \ldots, m \tag{5b}$$

$$\sum_{(i,j):e \in \text{Path}_i} r_{i,j} \le B(e) \tag{5c}$$

$$\sum_{i=1}^{m} \omega_{i,j} V_i \le C_j, j \in 1, 2, \ldots, n \tag{5d}$$

$$r_{i,j} \ge 0 \tag{5e}$$

$$\omega_{i,j} = 1, \quad \text{when} \quad r_{i,j} > 0. \tag{5f}$$

Objective function (5a) denotes the minimum delay on the whole, and the first item stands for the time generated during transmission of all kinds of traffic. On CIoV, cognitive engine provides global optimization, thus to realize minimum travel time for all kinds of traffic. In the meanwhile, according to (3), we can get when the weight item θ_i is added, minimum restrictions can make lower delay for traffic with large weight in security requirements. The second item is regular term added additionally, aiming to minimize quantity of paths with requirements of deployment, i.e., quantity of value 0 of $\phi(r_{i,j})$ should be as many as possible. In consideration of hardware restrictions in switches, as for each kind of traffic, the quantity of forwarding strategies that should be deployed in switches should be reduced as far as possible, i.e., the forwarding paths for each kind of traffic should be as few as possible in general. The decrease in paths would necessarily reduce time delay for that kind of traffic, which is in line with minimum time delay of objective function. In condition (5b), the rate consumed by all forwarding paths for each kind of traffic T_i cannot exceed preset restriction R_i. It whould guarantee all resources can be rationally allocated as per preset conditions, and avoid the situation where some truly urgent and important kind of traffic cannot be forwarded in time because some kind of unimportant traffic consumes too many resources. Condition (5c) guarantees that the bandwidth of path through side of graph model cannot exceed the maximum bandwidth of that side, thus to avoid network congestion, and to avoid waiting time needed by traffic transmission. Condition (5d) guarantees that the amount of tasks allocated to switch for processing cannot exceed its capacity, thus to avoid queuing time at switches, and to avoid overload operation of switches. Condition (5f) guarantees that traffic forwarded meets safe forwarding rules.

E. Problem Conversion

As for optimization problem given in the previous section, the following lemma can be obtained.

Lemma 1: This optimization problem is a nonconvex optimization problem.

Proof: Bring expression (3) for t_{Path_i} in objective function $f(r_{i,j})$ of optimization problem, we can get

$$f\left(r_{i,j}\right) = \sum_{i=1}^{m} \sum_{j=1}^{l_i} \theta_i D_{i,j} \phi\left(r_{i,j}\right) + \eta \sum_{i,j} \phi\left(r_{i,j}\right). \tag{6}$$

Next, prove function $\phi(x)$ is a nonconvex function, with proof by contradiction. If $\phi(x)$ is a convex function, two conditions should be verified as per definition of convex function.

1) *Condition 1:* Verify domain of definition Ω is convex set or not.
2) *Condition 2:* Verify for arbitrary $0 \le \xi \le 1$, and $x, y \in \Omega$, satisfy

$$\phi(\xi x + (1 - \xi)y) \le \xi\phi(x) + (1 - \xi)\phi(y). \tag{7}$$

Both of the two conditions are indispensable. Next, verification will be conducted one by one. First, the domain of definition Ω for $\phi(x)$ is $x \ge 0$, and it is quite clear that Ω is convex set. Assume $\phi(x)$ is convex function, then inequation (7) would apply for any $0 \le \xi \le 1$ and any $x \ge 0, y \ge 0$. Assign special value $\bar{x} > 0, \bar{y} = 0, 0 < \bar{\xi} < 1$, then $\bar{x}, \bar{y} \in \Omega$ and $\bar{\xi} \in (0, 1) \subseteq [0, 1]$ apply, which meets precondition. Bring it in left side of inequation (7). As $\bar{\xi}\bar{x} > 0$, we can get

$$\phi\left(\bar{\xi}\bar{x} + \left(1 - \bar{\xi}\right)\bar{y}\right) = \bar{\phi}\left(\bar{\xi}\bar{x}\right) = 1. \tag{8}$$

Bring it to the right of (7), we can get

$$\bar{\xi}\phi(\bar{x}) + \left(1 - \bar{\xi}\right)\phi(\bar{y}) = \bar{\xi}. \tag{9}$$

Because special $\bar{\xi} < 1$ that meets precondition is assigned, so the inequation does not apply, which is contradictory to assumption where function $\phi(x)$ is convex function. Then, we can get hypothesis is not established. Thus $\phi(x)$ is proved to be nonconvex function.

It can be seen from formula (6) that function $f(r_{i,j})$ is linear combination of $\phi(r_{i,j})$. Because $\phi(x)$ is nonconvex function, $f(r_{i,j})$ is also nonconvex function. Then this optimization problem is a nonconvex optimization problem. ■

In order to better solve above mentioned nonconvex optimization problem, we will convert it into convex optimization problem [30]. According to the definition of function $\phi(x)$, we can get that $\phi(r_{i,j}) \in \{0, 1\}$, then this optimization problem can be viewed as 0-1 integer programming. Above mentioned optimization problem then can be converted into convex optimization problem with Log-det heuristic algorithm.

In consideration of numerical iterative process that changes with iterative times k, adopt $r^k_{i,j}$ to denote result of k-th iteration. Then a restrictive condition for termination of iteration can be given. For example, randomly give a small constant $\zeta > 0$, and when

$$|r^{k+1}_{i,j} - r^k_{i,j}| \le \zeta \tag{10}$$

applies, iteration is terminated, and $r^{k+1}_{i,j}$ is outputed, and $r^{k+1}_{i,j}$ will be made as the final approximate value. When iterative time changes from k into $k+1$, $r_{i,j}$ changes from $r^k_{i,j}$ into $r^{k+1}_{i,j}$. Based on theoretical thought of Log-det heuristic, substitute $\phi(r^{k+1}_{i,j})$ for $\phi(r_{i,j})$, and the expression is as

$$\tilde{\phi}(r^{k+1}_{i,j}) = \frac{r^{k+1}_{i,j}}{r^k_{i,j} + \tau}. \tag{11}$$

Then, set up initial value, i.e., value of $r_{i,j}$ at first time of iteration ($k = 0$). Note it as $r^0_{i,j}$, and use it for numerical iterative process.

As $\tilde{\phi}(x)$ is convex function, it is clear that the restricted condition for that optimization problem is convex function. Therefore, the nonconvex optimization problem is converted into a convex optimization problem. Next, the rationality in substituting $\tilde{\phi}(x)$ for $\phi(x)$ will be analyzed. When τ is small enough, $|r^{k+1}_{i,j} - r^k_{i,j}| \le \zeta$ can be established through iteration

$$\tilde{\phi}(r^{k+1}_{i,j}) = \frac{r^{k+1}_{i,j}}{r^k_{i,j} + \tau} \approx \begin{cases} 1, & \text{If } r^{k+1}_{i,j} > 0 \\ 0, & \text{If } r^{k+1}_{i,j} = 0. \end{cases} \tag{12}$$

It shows $\tilde{\phi}(x) \approx \phi(x)$, and it also shows rationality in such substituting. Therefore, original 0-1 nonconvex optimization problem is converted into the following iteration process, and each iteration is a convex optimization problem, i.e.,

$$\underset{\mathbf{r^{k+1}_{i,j}}}{\text{minimize}} \quad \sum_{i=1}^{m}\sum_{j=1}^{l_i} \theta_i D_{i,j} \frac{r^{k+1}_{i,j}}{r^k_{i,j} + \tau} + \eta \sum_{i,j} \frac{r^{k+1}_{i,j}}{r^k_{i,j} + \tau} \tag{13a}$$

$$\text{subject to} \quad \sum_{j=1}^{l_i} r^{k+1}_{i,j} \le R_i, i \in 1, 2, \ldots, m \tag{13b}$$

$$\sum_{(i,j):e\in \text{Path}_i} r^{k+1}_{i,j} \le B(e) \tag{13c}$$

$$\sum_{i=1}^{m} \omega_{i,j} V_i \le C_j, j \in 1, 2, \ldots, n \tag{13d}$$

$$r^{k+1}_{i,j} \ge 0, k \ge 0 \tag{13e}$$

$$\text{When} \quad r^{k+1}_{i,j} > 0, \quad \omega_{i,j} = 1. \tag{13f}$$

TABLE II
NOTATION

Parameters	Definition
n	6
$B(e)$	Uniform distribution, mean value is 5
m	80
$\theta_i, i \in \{1, 2, \cdots, m\}$	Exponential distribution, mean value is 55
$\omega_{i,j}$	Standard normal distribution

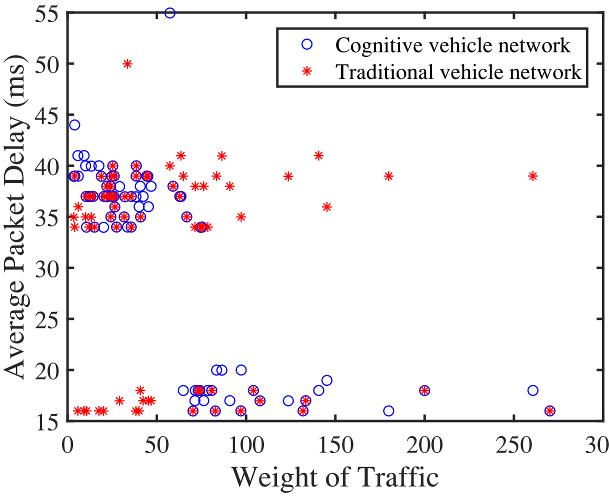


Fig. 2. Illustration of comparison cognitive vehicle network with traditional vehicle network.

IV. Simulation Experiment

In this section, we utilize simulation experiment to evaluate cognitive vehicle network. In this experiment, we assume that there are 6 switches and 80 traffic with different security sensitivities in the network. For every traffic, we set up its security sensitivity θ, which is derived from the exponential distribution with mean value is 55. The required bandwidth R is from the uniform distribution with mean value is 5. Table II shows the values of parameters used in this experiment.

In this paper, we compare the time delay between the traditional vehicle network and cognitive vehicle network. Considering cognitive vehicle network, there is a cognitive engine, then the security sensitivity of traffic can be obtained by cognitive engine. As for traditional vehicle network, it has no way to perceive its security sensitivity coefficient θ. Therefore, for the traditional vehicle network, we set up the traffic forward always through the shortest path. For the evaluation of delay, we use the metrics are the average packet delay and the cumulative distribution function (CDF).

As shown in Fig. 2, when security sensitivity of traffic $\theta < 50$, traditional vehicle network is better than our cognitive vehicle network. This is because our algorithm first guarantees the delay of sensitive traffic, which may lead to delay the unsensitive traffic. When $\theta >= 50$, we can see from this figure, the cognitive vehicle network is better than traditional vehicle network. This is because the cognitive vehicle network can ensure the delay of sensitive traffic, and with the increase of θ, cognitive vehicle network can guarantee more secure than traditional vehicle network.

As shown in Fig. 3(a), we give experiment results, when maximum 40 security sensitivity ω_i are selected. From the figure we can conclude that, in this situation, the performance of cognitive vehicle network is better than traditional vehicle network. This is because, cognitive engine can analysis security sensitivity of traffic, and forward the optimal routing, thus to reduce the delay and improve security. In Fig. 3(b), we have shown the results, when minimum 40 ω_i are chosen. From this figure, we can draw a conclusion that when end-to-end delay is less than 2 and greater than 35, the performance of cognitive vehicle network is not very different from traditional vehicle network. This is because, when the security sensitivity is low, for cognitive vehicle network, there will be some traffic with low sensitivity will be transmitted late, which will lead to delay. As for Fig. 3(c), we give 80 traffic delays. From this figure, we can get that the cognitive vehicle network we proposed in this article is better than traditional vehicle network.

V. Open Issues

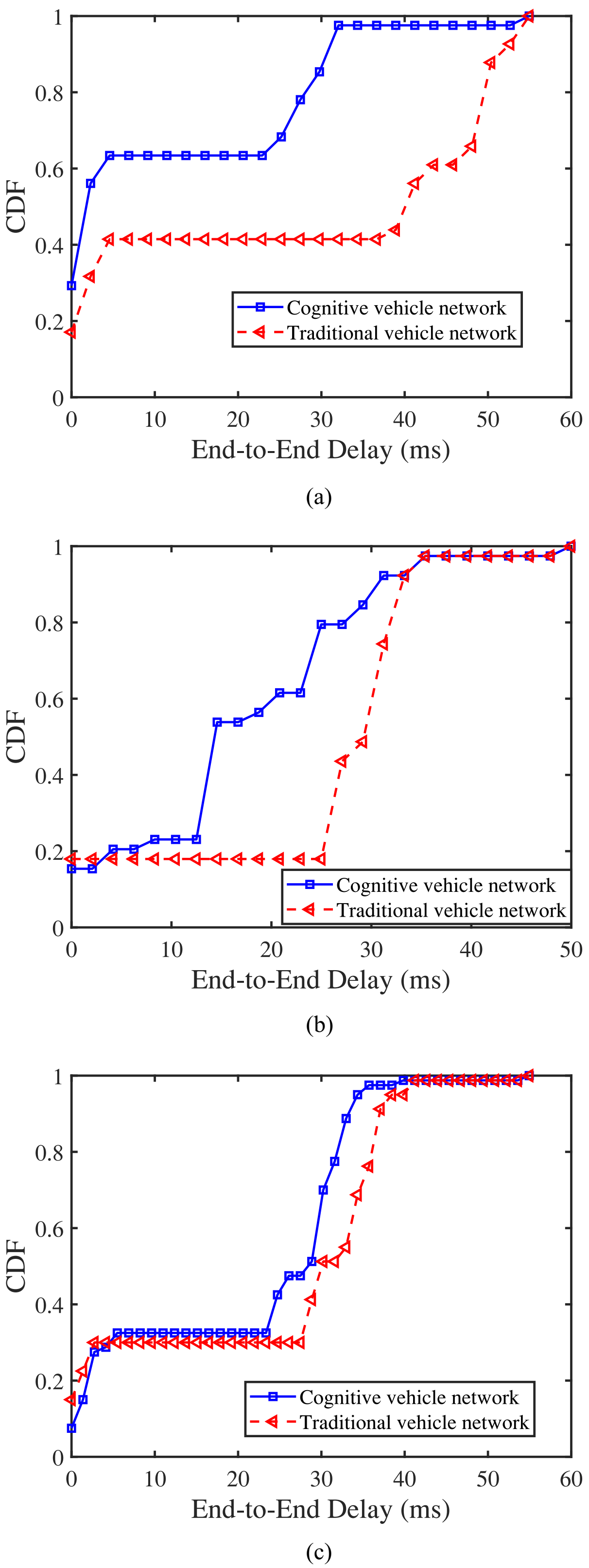
There are the following open issues in addition to security strategy deployment on CIoV.

A. *Vulnerability Scanning for IoV*

As there are numerous devices carried on IoV, there is a wide range of corresponding vulnerabilities, and there is great platform difference. For this purpose, a kind of vulnerability scanning method should be designed, thus to realize cross-platform vulnerability scanning that does not rely on device. IoV requires that vulnerability can be rapidly repaired after detection of a vulnerability, which often requires investment of large amount of human and material resources. How to guarantee patching development efficiency with less resources consumption is a key problem to be solved. In the meantime, the vulnerability repair in environment of IoV is different from situation for traditional devices. A slight negligence may cause car crash. Therefore, how to repair vulnerabilities without influencing driving security is one of key problems to be solved.

B. *Safe Communication on Interior Network of IoV*

CAN bus sends messages in the form of broadcast, and once a message is sent to CAN bus, other nodes on CAN bus can receive that message, so ECU that receives this message could not confirm which node this message is from. In addition, in order to save cost and to enhance communication efficiency, few manufacturers conducted encryption for CAN communication data, and this design defect could naturally cause message forgery and spoofing attack. Therefore, designing communication security strategy for interior network with compatible format (including secret key management, lightweight bus encryption algorithm and authentication scheme) is another key problem to be solved.



(a)

(b)

(c)

Fig. 3. End-to-end delay of cognitive vehicle network and traditional vehicle network. (a) Traffic with bigger ω_i. (b) Traffic with smaller ω_i. (c) All 40 traffic.

C. *Security on External Network of IoV*

If the speed of a vehicle exceeds 100 km/h, then the possibility that the link on IoV can maintain for 15 s is less than

57%. Therefore, during access of vehicle into external network, the computing time required by generation of message authentication code should be lowered, and interaction times for completion of authentication should be reduced. It is clear that only low-cost noninteractive authentication scheme can guarantee this condition. For this purpose, this project should solve difficult problems in design of low-cost noninteractive authentication scheme. In the meantime, on IoV, vehicle node may access or quit network at any time, which shows quite strong self-organization. Therefore, low-cost secret key updating mechanism is required to guarantee timeliness for legal identity of vehicles and time limit of conversation.

D. Integrity Protection and Security Upgrade for ECU Firmware

If the integrity protection and security upgrading scheme is to be established for ECU firmware, the critical point lies in how to guarantee integrity of ECU firmware thus to realize rapid and secure booting of ECU. In the meantime, a kind of authentication scheme that is able to verify upgrade package of ECU firmware should be put forth, thus to realize remote secure upgrade of firmware, and to refuse malicious upgrade operation. There are many kinds of ECU firmware from numerous manufacturers, and the security performance in each manufacturer is different, which brings great difficulty in integrity protection of ECU firmware. How to overcome this difficulty is the key problem to be solved in this project.

VI. Conclusion

In this paper, path selection scheme for forwarding rules of delay-sensitive traffic is given in allusion to security deployment problem on CIoV. 0-1 programming problem is given to describe this path selection strategy, and the solution is given through converting the problem into convex optimization problem. It is proved in experiment that by introducing cognitive engine, the performance of CIoV is better than that of IoV in aspect of average packet transmission delay and end-to-end transmission delay.

Acknowledgment

The authors would like to thank the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

References

[1] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.

[2] G. Fortino, R. Gravina, W. Russo, and C. Savaglio, "Modeling and simulating Internet-of-Things systems: A hybrid agent-oriented approach," *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 68–76, 2017.

[3] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[4] X. Hou *et al.*, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, Jun. 2016.

[5] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[6] S. Du, X. Li, J. Du, and H. Zhu, "An attack-and-defence game for security assessment in vehicular ad hoc networks," *Peer Peer Netw. Appl.*, vol. 7, no. 3, pp. 215–228, 2014.

[7] J. Chen *et al.*, "Dominating set and network coding-based routing in wireless mesh networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 423–433, Feb. 2015.

[8] J. Chen *et al.*, "Batch identification game model for invalid signatures in wireless mobile networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 6, pp. 1530–1543, Jun. 2017.

[9] H. Li *et al.*, "Privacy leakage via de-anonymization and aggregation in heterogeneous social networks," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2017.2754249.

[10] H. Zhu *et al.*, "You can jam but you cannot hide: Defending against jamming attacks for geo-location database driven spectrum sharing," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2723–2737, Oct. 2016.

[11] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. 32nd Int. Conference Very Large Data Bases (VLDB Endowment)*, 2006, pp. 763–774.

[12] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: Attacks and defense," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2016.2604383.

[13] L. Zhou, Q. Chen, Z. Luo, H. Zhu, and C. Chen, "Speed-based location tracking in usage-based automotive insurance," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2017, pp. 2252–2257.

[14] J. Chen *et al.*, "Uncovering the face of Android Ransomware: Characterization and real-time detection," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 1286–1300, 2018.

[15] J. Liu *et al.*, "Leveraging software-defined networking for security policy enforcement," *Inf. Sci.*, vol. 327, pp. 288–299, Jan. 2016.

[16] D. Kreutz *et al.*, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[17] S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar, "Dependable demand response management in the smart grid: A Stackelberg game approach," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 120–132, Mar. 2013.

[18] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 623–654, 1st Quart., 2016.

[19] A. Y. Ding, J. Crowcroft, S. Tarkoma, and H. Flinck, "Software defined networking for security enhancement in wireless mobile networks," *Comput. Netw.*, vol. 66, pp. 94–101, Jun. 2014.

[20] K. Wang, Y. Qi, B. Yang, Y. Xue, and J. Li, "LiveSec: Towards effective security management in large-scale production networks," in *Proc. IEEE 32nd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, 2012, pp. 451–460.

[21] M. Chen, Y. Hao, L. Hu, K. Huang, and V. K. N. Lau, "Green and mobility-aware caching in 5G networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 12, pp. 8347–8361, Dec. 2017.

[22] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, "A 5G cognitive system for healthcare," *Big Data Cogn. Comput.*, vol. 1, no. 1, p. 2, 2017.

[23] N. McKeown *et al.*, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.

[24] H. Bostani and M. Sheikhan, "Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept," *Pattern Recognit.*, vol. 62, pp. 56–72, Feb. 2017.

[25] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowl. Based Syst.*, vol. 78, pp. 13–21, Apr. 2015.

[26] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *Proc. USENIX Security Symp.*, Austin, TX, USA, 2016, pp. 911–927.

[27] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[28] M. Chen, Y. Qian, Y. Hao, Y. Li, and J. Song, "Data-driven computing and caching in 5G networks: Architecture and delay analysis," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 2–8, Feb. 2018.

[29] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-defined networking for RSU clouds in support of the Internet of Vehicles," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 133–144, Apr. 2015.

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

Yongfeng Qian received the M.S. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2015, where she is currently pursuing the Ph.D. degree at the Embedded and Pervasive Computing Laboratory, School of Computer Science and Technology, under the supervision of Prof. M. Chen.

Her current research includes the Internet of Things, big data analytics, network security, and data privacy.

Min Chen (SM'09) has been a Full Professor with the School of Computer Science and Technology, Huazhong University of Science and Technology (HUST) since February 2012. He is the Director of the Embedded and Pervasive Computing (EPIC) Lab, HUST. He is Chair of the IEEE Computer Society (CS) Special Technical Communities (STC) on Big Data. He was an Assistant Professor with the School of Computer Science and Engineering, Seoul National University (SNU). He worked as a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of British Columbia (UBC), for three years. Before joining UBC, he was a Post-Doctoral Fellow with SNU for one and half years. His research focuses on Cyber Physical Systems, IoT Sensing, 5G Networks, Mobile Cloud Computing, SDN, Healthcare Big Data, Medica Cloud Privacy and Security, Body Area Networks, Emotion Communications and Robotics, etc.

Prof. Chen was the recipient of the Best Paper Award from QShine 2008, IEEE ICC 2012, ICST IndustrialIoT 2016, and IEEE IWCMC 2016. He serves as Editor or Associate Editor for *Information Sciences*, *Information Fusion*, and IEEE ACCESS, etc. He is a Guest Editor for *IEEE Network*, *IEEE Wireless Communications*, and the IEEE TRANSACTIONS ON SERVICE COMPUTING, etc. He was Co-Chair of the IEEE ICC 2012-Communications Theory Symposium and Co-Chair of IEEE ICC 2013-Wireless Networks Symposium. He was General Co-Chair for IEEE CIT-2012, Tridentcom 2014, Mobimedia 2015, and Tridentcom 2017. He was the Keynote Speaker for CyberC 2012, Mobiquitous 2012, Cloudcomp 2015, IndustrialIoT 2016, and The 7th Brainstorming Workshop on 5G Wireless. He has more than 300 paper publications, including 200+ SCI papers, 80+ IEEE TRANSACTIONS/JOURNALS papers, 18 ISI highly cited papers and 8 hot papers. He has four books: *OPNET IoT Simulation* (2015), *Big Data Inspiration* (2015), *5G Software Defined Networks* (2016) and *Introduction to Cognitive Computing* (2017) with HUST Presss, a book on big data: *Big Data Related Technologies* (2014) and a book on 5G: *Cloud Based 5G Wireless Networks* (2016) with the Springer Series in Computer Science. His latest book (co-authored with Prof. Kai Hwang), *Big Data Analytics for Cloud/IoT and Cognitive Computing* (Wiley, U.K.) was published in 2017. His Google Scholars Citations reached 12,000+ with an h-index of 53. His top paper was cited 1100+ times. He was the recipient of the IEEE Communications Society Fred W. Ellersick Prize in 2017.

Jing Chen received the Ph.D. degree in computer science from the Huazhong University of Science and Technology, Wuhan, China.

He has been an Associate Professor since 2010. He is the Chief Investigator of several projects in network and system security, funded by the National Natural Science Foundation of China. He has published over 60 research papers in many international journals and conferences, such as the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM, the *International Journal of Parallel and Distributed System*, INFOCOM, SECON, TrustCom, and NSS. His current research interests include network security and cloud security in computer science.

Dr. Chen acts as a Reviewer for many journals and conferences, such as the IEEE TRANSACTIONS ON WIRELESS COMMUNICATION, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, *Computer Communications*, and GLOBCOM.

M. Shamim Hossain (S'03–M'07–SM'09) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada.

He is with the Department of Software Engineering, College of Computer and Information Sciences King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor of EECS with the University of Ottawa, Ottawa, ON, Canada. His research interests include cloud networking, social media, IoT, cloud and multimedia for healthcare, smart health, and resource provisioning for big data processing on media clouds. He has authored or coauthored approximately 165 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters.

Dr. Hossain has served as a member of the Organizing and Technical Committees of several international conferences and workshops. Currently, he serves as a Co-Chair of the 1st IEEE ICME Workshop on Multimedia Services and Tools for Smart-health MUST-SH 2018. He was a recipient of a number of awards including the Best Conference Paper Award, the 2016 *ACM Transactions on Multimedia Computing, Communications and Applications* (TOMM) Nicolas D. Georganas Best Paper Award, and the Research in Excellence Award from King Saud University. He is on the Editorial Board of IEEE MULTIMEDIA, IEEE ACCESS, *Computers and Electrical Engineering* (Elsevier), *Games for Health Journal and International Journal of Multimedia Tools and Applications* (Springer). Previously, he served as a Guest Editor for the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (currently JBHI), *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), and *International Journal of Distributed Sensor Networks, and Sensors* (MDPI). Currently, he serves as a Lead Guest Editor of *IEEE Communication Magazine*, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE ACCESS, and *Future Generation Computer Systems* (Elsevier).

Atif Alamri received the Ph.D. degree in computer science from the University of Ottawa, Ottawa, ON, Canada, in 2010.

He is an Associate Professor with the Research Chair of Pervasive and Mobile Computing, King Saud University, Riyadh, Saudi Arabia, where he is also with Department of Software Engineering, College of Computer and Information Sciences. His current research interests include collaborative rehabilitation, haptic enabled applications, service-oriented architecture, and Web-service composition.