Received May 27, 2020, accepted June 8, 2020, date of publication June 19, 2020, date of current version July 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003808

Intelligent Vulnerability Analysis for Connectivity and Critical-Area Integrity in IoV

SHUMEI LIU[1,2], **YAO YU**[1,2], **(Member, IEEE), WENJIAN HU**[2], **YUHUAI PENG**[2], **(Member, IEEE), AND XIAOLONG YANG**[3], **(Member, IEEE)**

[1]Key Laboratory of Intelligent Computing in Medical Image, Ministry of Education, Northeastern University, Shenyang 110819, China
[2]School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
[3]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Corresponding authors: Yao Yu (yuyao@mail.neu.edu.cn) and Yuhuai Peng (pengyuhuai@mail.neu.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1702000, in part by the National Natural Science Foundation of China under Grant 61871107 and Grant 61941113, in part by the Fundamental Research Funds for the Central Universities under Grant N171612014, Grant N170308028, Grant N181613003, and Grant N180708009, and in part by the Visiting Scholar Program of the China Scholarship Council under Grant 201906085031.

ABSTRACT The large-scale connectivity of Internet of Vehicles (IoV) is an important challenge for the Intelligent Transportation Systems (ITS). Intelligence vulnerability analysis is an excellent solution. However, existing methods for analyzing connectivity vulnerability have ignored the existence of critical areas in the system. Due to the heterogeneities of the IoV environments and services, the failure of some specific areas may seriously damage connectivity and system performance. To this end, in this paper we focus on both the dynamic connectivity and the critical-area integrity, and propose an intelligent vulnerability analysis method to effectively identify the critical area of extreme vulnerability. Specifically, we consider an intelligent analysis scenario in which roadside servers continuously learn IoV heterogeneous environment and dynamic topology, and then translate the learning results into a flexible disruption cost problem. Based on this, we utilize the spectral partitioning method to identify the minimum-cost set of topological elements whose failure not only severely damages system connectivity but also disrupts its critical areas. Furthermore, we confirm that the identified set can be used to optimize disruption cost problem, thus intelligently improving vulnerability. Simulation results show that our proposed method can effectively identify vulnerable elements and prevent significant loss in the IoV system connectivity and performance.

INDEX TERMS Intelligent transportation systems (ITS), Internet of Vehicles (IoV), intelligence vulnerability analysis, connectivity, critical area.

I. INTRODUCTION

Dynamic connectivity plays a vital role in evaluating the system performance of future Intelligent Transportation Systems (ITS), and is a fundamental concern in designing and implementing wireless intelligent systems [1]. Particularly in the Internet of Vehicles (IoV), system connectivity and the robustness of connectivity are key factors in determining the quality of service and security level of applications [2]. However, due to the heterogeneity of the IoV environments, there may be some important but easily neglected and weakly protected areas. Disruptions to the weaknesses will lead to the large-scale paralysis of the system due to a wide-range of causes including natural disasters and malicious attacks, thus resulting in dramatic degradation in the system performance [3].

Intelligent vulnerability analysis is an effective solution for solving such security problems. It continuously assesses the risks for a network or system, enabling system managers to make dynamic decisions based on facts and measurements [4]. By combining artificial intelligence (AI) technology, it can be implemented by putting the environments and system state into a AI checker, then verify if undesired states that are related to security properties will occur. Due to the high dynamic of the IoV environment and topology, conducting vulnerability analysis on the IoV dynamic topology and making intelligent security decisions are of great significant [5]. However, although there have been

The associate editor coordinating the review of this manuscript and approving it for publication was Amr Tolba.

many studies analyzing topological vulnerability, existing solutions cannot be directly incorporated into intelligent IoV applications due to several critical limitations.

Most existing works on vulnerability analysis focus on using single analytical measure, which is the insufficient consideration for the heterogeneous IoV environments. Among them, some of the most classic methods are centrality based method, such as degree centrality [6] and betweenness centrality [7]. These methods cannot reveal the connection damage to a system when facing attacks. For the dynamic IoV applications, connectivity is a basic requirement [8]. Some recent studies have used pairwise connectivity as an analysis measure [9]–[11], the methods aim to identify the network elements that pose a significant threat to global connectivity if they are disrupted. However, these previous methods ignore the differences in the importance of different subnetworks in the network and cannot reveal the enormous damage to a network caused by high-priority attacks on a critical area of the network or system.

Particularly in the heterogeneous IoV applications, some area-specific services are confidential but the current communication connections may be vulnerable [12]. The failure of the critical component or area may lead to serious consequences to the IoV system [13]. To this end, AI technology opens up new opportunities for the topological vulnerability analysis considering critical areas [14]. Specifically, it can continuously learn the service environment and communication status of the system, dynamically identifying the critical areas. However, few studies have considered the advantages of AI technology when analyzing topological vulnerability.

In this paper, motivated by the above challenges, we propose an intelligent vulnerability analysis method considering connectivity and critical-area integrity (IVA-CC). In the proposed IVA-CC method, we utilize the advantage of AI technology to dynamically transform the vulnerability of system elements (i.e., nodes and links) into a disruption cost problem. To ensure the high security of the IoV environments, we consider the worst-case scenario that aims to find a minimum-cost and high-vulnerability set of system elements. Removal of this set not only severely damages system connectivity, i.e., breaking the system into two or more unconnected subnetworks, but also simultaneously disrupts the integrity of the critical area. Such a set is of high importance to the system, but may not be adequately protected due to being assigned a low disruption cost. For the heterogeneous IoV systems, the system elements that play a key role in maintaining both critical-area integrity and network connectivity should be continuously identified and protected, which thus motivates our study in this paper. The main contributions of this paper are summarized as follows:

- We consider an intelligent scenario where roadside servers continuously learn IoV heterogeneous environment and dynamic topology, and then translate the learning results into a flexible disruption cost problem.
- To accommodate the high security requirements of the IoV systems, we utilize the spectral partitioning method to identify the minimum-cost and high-vulnerability elements by considering the worst-case scenario.
- We conduct extensive experiments to evaluate our proposed IVA-CC method. Our results show that IVA-CC could efficiently identify vulnerable elements in the critical areas, and then prevent significant loss in the IoV system connectivity and performance.

The rest of this paper is organized as follows. Section II provides an overview of previous work. In Section III, we introduce the network model and some definitions. In Section IV, we formulate the problem and propose a novel intelligent vulnerability analysis method. Since the problem is NP-hard by nature, we transform and solve the problem in Section V. In Section VI, we evaluate the performance of the proposed method through extensive simulation. Conclusions are given in Section VII.

II. RELATED WORK

Intelligent vulnerability analysis can learn the regularity of the environment and predict system vulnerabilities in advance, helping to formulate corresponding security policies [15]. But existing intelligent vulnerability analysis methods focus on software or protocol vulnerabilities, and thus ignore the fundamental importance of topological connectivity [15], [4], [5]. Moreover, many works on analyzing topological vulnerability have focused on the advantages of classic centrality methods, such as degree centrality [6] and betweenness centrality [7], finding the critical elements and areas in a network. Similarly, these centrality-based methods cannot reveal the vulnerability of connectivity.

For the dynamic IoV systems, connectivity is a basic requirement of the systems, and the destruction of the system connectivity would dramatically degrade the performance [16], [17]. To resolve this challenge, some recent studies have used connectivity as a measure in topological vulnerability analysis [9]–[11], [18]–[21], but most of these have considered node vulnerability and link vulnerability separately. In [9], [10], the authors proposed two optimization problems to respectively identify vulnerable links and nodes whose removals maximally destroy the system connectivity. In [18], the authors proposed a distributed algorithm based on suboptimal solutions of two optimization problems for identifying critical nodes in a network. The authors in [19] highlighted the importance of network connectivity and defined a *Critical Node Detection Problem* problem, then [19] reviewed and discussed several recent advances and results about the problem. The above methods ignored the fact that joint node and link attacks (simultaneous attacks on both nodes and links) may cause grave damage to a network. Dinh and Thai analyzed joint attack scenarios and introduced the disruption cost problem [11]. However, the method in [11] only considers the relative size (the number of nodes) of residual subnetworks and ignores the differences in the importance of different subnetworks in the network.

As same as critical nodes and links existing in a network, it has been shown that there are one or more critical subnetworks/areas with higher level of importance than others in any type of networks [13]. Particularly in the heterogeneous IoV applications, some specific areas are extremely important in terms of communications and services [22], [23]. In order to analyze the attacks targeting the critical areas in a network and identify the vulnerabilities, the authors in [24] formulated the *Critical Node Identification* problem and the *Critical Area Identification* problem to find the critical node and the critical area under regional attacks or failures. To consider each link's connection under regional/area attacks, the authors in [25] estimated the connection probability of each link when there is an area-based attacks, but the method does not consider the global connectivity, which is of great importance to a system. More importantly, AI technology has prominent advantage in the aspect of identifying critical areas in the heterogeneous IoV systems [26], but there is no suitable solution in the existing researches.

Based on the analysis above, when assessing unexpected risks and hidden vulnerabilities for the IoV systems, few researches consider both global connectivity and critical-area integrity of the systems. In addition, existing researches ignore the advantages of AI technology in analyzing connectivity vulnerabilities and identifying critical areas. To advance the security of the dynamic IoV systems, the intelligent vulnerability analysis is critically important.

III. PRELIMINARY AND DEFINITIONS

We abstract the IoV system model as a original network graph $G = (V, E)$, where V refers to a set of nodes (i.e., intelligent vehicles and roadside servers) and E refers to a set of links (i.e., communication lines). We use n and m to represent the number of nodes and links, respectively. In this paper, we consider the undirected network graph whose application is more widespread. For two nodes $i, j \in V$ in an undirected graph, they can communicate with each other if there exists a path (one or more links) between them, and $[i, j]$ is a connected pair of G.

Then we consider some definitions as follows.

1) Cost $c(\cdot)$: Let $c(\cdot)$ represent the cost (such as time, effort or money) for disrupting a network element (i.e. node or link) in the IoV systems, which is the protection cost assigned to each network element. In general, the more important network elements require the more protection costs. For example, some roadside servers and intelligent vehicles in the IoV systems are critical for ensuring system connectivity, which need stronger protections. Also, the services in some areas are confidential, thus the areas' elements require stronger protections to avoid being eavesdropped or attacked.

Due to the dynamics of the IoV environments and topology, the importance of each network element changes dynamically. Therefore, we consider an intelligent analysis scenario by using AI technology, in which roadside servers continuously learn IoV heterogeneous environments and dynamic topology. After that, we assign costs to the network elements based on the learning results, and then conduct the topological vulnerability analysis. The analysis results are used to further optimize the costs, thus intelligently improving the vulnerability.

Specifically, $c(i)$ and $c(i, j)$ are the costs of disrupting node i and edge (i, j), respectively. We assume that each network element's initial cost is quantified by its importance degree in the network topology, which provides initial values for AI intelligent learning. It is shown that degree centrality and betweenness centrality are two of the most critical centrality metrics to identify high importance central nodes or links [7]. Hence, the initial disruption costs of node i and link (i, j) are given by

$$c(i) = a * D_G(i) + b * B_G(i) \tag{1}$$

$$c(i, j) = B_G(i, j), \tag{2}$$

where $D_G(i)$ represents the normalized degree centrality of node i in graph G. It is defined as the number of nodes directly connecting to a node, and can identify the most influential nodes in the network. $B_G(i)$ and $B_G(i, j)$ are the betweenness centralities of node i and link (i, j), respectively in graph G. The betweenness centrality is defined as the number of the shortest paths that go through a node or link, and it can identify the nodes or links with the most bridging ability in the network.

In a real scenario of network foundation planning, the nodes with higher importance will be allocated stronger protections. Both $D_G(i)$ and $B_G(i)$ are key indicators for evaluating the importance degree of node i, so we set the parameters $a = b = 0.5$ when quantifying the cost $c(i)$ of disrupting node i. Moreover, for the links with stronger bridging ability, planners will set up reserve channels/transmission lines to defend against unexpected events, thus avoiding the impact of failure of these links on system connectivity. The cost $c(i, j)$ of disrupting link (i, j) is therefore determined by its edge betweenness centrality $B_G(i, j)$.

2) Critical area: In this paper, a critical area is the network area that is critical to network communication/transmission and network connectivity. More importantly, in our opinion, the critical area is not a network area with clear boundaries. It is an area where the total disruption cost is relatively high, but is a particularly vulnerable target because the network function will be severely damaged once the area has been attacked. The costs are dynamically obtained by the AI technology. Using AI technology, we can find out the topological rules and properties of a critical area in the dynamic environments. The following are specific examples.

- Fig. 1 shows a local area of a network or system. The area includes a node with high degree centrality (i.e., central black node), such as a roadside server in the IoV system. The blue shaded area in Fig. 1 has high-density connections. Moreover, the degree centrality of the nodes in the shaded area is generally high, especially the leader node with higher control ability.

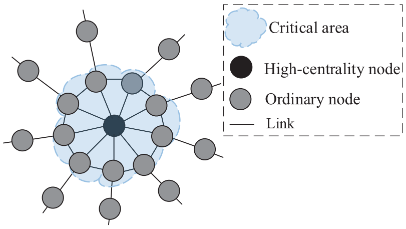


FIGURE 1. Local network area with high-density connections.

- Fig. 2 shows a bridge area of a network. The blue shaded area in Fig. 2 bridges the communication/transmission between subnetworks A, B, and C. The network elements in this area thus have high betweenness centrality. In addition, network connectivity will be greatly damaged once the bridge area fails.

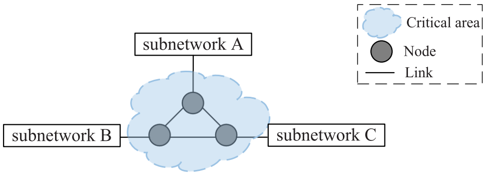


FIGURE 2. Bridge area of a network.

Therefore, the blue shaded areas in Fig. 1 and Fig. 2 are considered as critical areas. In this paper, we highlight that the IoV systems rely heavily on the critical-area integrity because the areas are crucial to system communication/transmission. Once some critical areas are disrupted, the system is difficult to recover and its performance degrades dramatically [13].

3) Importance Degree $I_{\mathrm{mp}}(\cdot)$: In the analysis, we define the importance degree of subnetwork A as

$$I_{mp}(A) \triangleq \sum_{i\in A} c(i) + \sum_{(u,t)\in A} c(u,t), \tag{3}$$

where i and (u,t) are the node and link belong to subnetwork A. As we can see, $I_{\mathrm{mp}}(A)$ is the total cost of the nodes and links in subnetwork A. According to the definition of the disruption cost of network elements, it can be concluded that $I_{\mathrm{mp}}(A)$ represent the importance degree of subnetwork A. Thus, a larger value of $I_{\mathrm{mp}}(A)$ indicates that subnetwork A is more critical in G.

4) Connectivity $P(G)$: $P(G)$ is the number of total connected pairs of G. Apparently, $P(G)$ is maximized at $\binom{n}{2}$ when G is a (strongly) connected graph.

5) Disruption Level α $(0 \leq \alpha \leq 1)$: The variable α indicates the level of the reduction in network connectivity when the vulnerable elements are attacked as

$$P(G\backslash S) \leq (1-\alpha)\binom{n}{2}, \tag{4}$$

where S is the set of vulnerable elements, $P(G\backslash S)$ means removing S from G.

IV. PROBLEM FORMULATION

To improve the security of IoV applications, especially intelligently improve the robustness of connectivity, in this paper we propose an intelligent vulnerability analysis method considering connectivity and critical-area integrity (IVA-CC).

A. PROBLEM FORMULATION FOR IVA-CC

We define the objective function of IVA-CC as $VA_{\mathrm{goal}}(S)$, its goal is to identify a minimum-cost set S with the highest vulnerability level. On the one hand, the removal of set S can disrupt the integrity of the critical area. At the same time, the removal of the targeted set S degrades the network connectivity to a large extent (by a fraction α), breaking the network into two or more unconnected subnetworks. Without loss of generality, we take the disrupted network containing two unconnected subnetworks A and B as an example to formulate the designed goal function $VA_{\mathrm{goal}}(S)$ as

$$VA_{goal}(S) \triangleq \min \frac{c(S)}{\widetilde{I}_{mp}(A)\cdot \widetilde{I}_{mp}(B)} \tag{5}$$

where

$$c(S) = \sum_{i\in S} c(i) + \sum_{(u,t)\in S} c(u,t) \tag{6}$$

$$\widetilde{I}_{mp}(A) = 2I_{mp}(A) + c(S), \tag{7}$$

where S is the set of vulnerable elements (i.e., the vulnerable nodes and links in G) connecting subnetworks A and B in G, and $c(S)$ is the total cost of there vulnerable elements.

Hence, the goal of our IVA-CC method is transformed into a graph's partitioning problem of minimization (5). As minimizing a fraction is equivalent to simultaneously minimizing the numerator and maximizing the denominator, there are two partition criteria that must be satisfied simultaneously in the partitioning problem of (5). On the one hand, we aim to minimize the total cost of the elements connecting subnetworks A and B. It means that our IVA-CC attempts to identify network elements that are less costly to disrupt but crucial to the connection of subnetworks A and B. On the other hand, we aim to maximize the product of $\widetilde{I}_{\mathrm{mp}}(A)$ and $\widetilde{I}_{\mathrm{mp}}(B)$ by maximizing the total cost of elements in each subnetwork. Next, we give a proposition and then prove it.

Proposition 1: Maximizing the denominator of (5) can identify the network elements whose failure disrupts global connectivity and simultaneously damages critical-area integrity.

Proof: Based on (3) and (7), we can obtain the following equation as

$$\begin{aligned}\widetilde{I}_{mp}(A) + \widetilde{I}_{mp}(B) \triangleq \widetilde{I}_{mp}(G) &= 2I_{mp}(G)\\ &= 2\left(\sum_{i\in V} c(i) + \sum_{(u,t)\in E} c(u,t)\right),\end{aligned} \tag{8}$$

as can be seen that $\widetilde{I}_{mp}(G)$ is twice the total cost of the nodes and links in G, so it is a constant term.

According to the property of the product, when the sum of $\widetilde{I}_{\text{mp}}(A)$ and $\widetilde{I}_{\text{mp}}(B)$ is a constant, the smaller the difference between $\widetilde{I}_{\text{mp}}(A)$ and $\widetilde{I}_{\text{mp}}(B)$ leads to a larger value of $\widetilde{I}_{\text{mp}}(A) \cdot \widetilde{I}_{\text{mp}}(B)$. Furthermore, $\widetilde{I}_{\text{mp}}(A) \cdot \widetilde{I}_{\text{mp}}(B)$ reaches its maximum when $\widetilde{I}_{\text{mp}}(A) = \widetilde{I}_{\text{mp}}(B)$, and thus when $I_{\text{mp}}(A) = I_{\text{mp}}(B)$. Therefore, to maximize the denominator of (5), if there is a critical area in the network (i.e., the area with a relatively high $I_{\text{mp}}(\cdot)$), the communication/transmission of the area may be isolated or disrupted to balance the values of $I_{\text{mp}}(A)$ and $I_{\text{mp}}(B)$. In this case, the network is broken into two unconnected subnetworks and simultaneously the integrity of its critical area is disrupted. □

From the above description, we identify the minimum-cost and high-importance set of network elements by minimizing VA_{goal} in (5). This thereby achieves the goal of the vulnerability analysis in this paper, namely, identifying the most disruptive scenario of a network.

B. PROBLEM TRANSFORMATION BY SPECTRAL PARTITIONING METHOD

Note that our goal function VA_{goal} is a multiconstraint problem, and it is difficult to solve such a problem. Spectral algorithms often give high-quality solutions of complex problems [27]. In this paper, we use a spectral partitioning method [18] to analyze the vulnerability of network topologies. It can transform the above complex problem into an optimal partitioning problem of a graph. When analyzing vulnerability for a network topological graph, it focuses on the links' weight (i.e., cost in this paper) in the graph, and transforms the continuous topology problem into a discrete clustering partition problem in terms of total weights. However, one disadvantage of the spectral partitioning method is that it only considers the links of the graph, and then the nodes' weights are ignored during the clustering partition. In other words, some critical nodes may be ignored in the vulnerability analysis. Previous works have shown that general disruptive events are joint attacks on nodes and links [11]. Therefore, to further analyze network vulnerability, as shown in Fig. 3, we construct an undirected auxiliary graph G' for G by splitting each node $i \in V$ into two representative nodes i_1 and i_2.

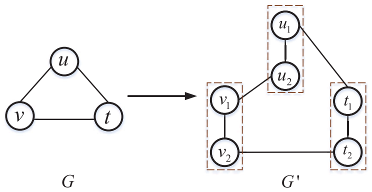


FIGURE 3. An example of constructing auxiliary graph G' for G.

Details are shown in Fig. 3. Specifically, for each node i in G, we carefully construct a newly added undirected link (i_1, i_2) in G' to map node i, and we set its disruption cost as $c'(i_1, i_2) = c(i)$. Meanwhile the number of node i's neighboring nodes in G is divided equally (or differ by one) among nodes i_1 and i_2 in G', ensuring that the added link (i_1, i_2) is meaningful and representative of node i. Moreover, for each link (i, j) in G, we construct an alternative undirected link (p_i, q_j) in G' to map (i, j), the alternative undirected link (p_i, q_j) is one of the four links: (i_1, j_1), (i_2, j_2), (i_1, j_2) or (j_1, i_2). Whatever the alternative link is, it does not change the connecting relationship between nodes i and j in G (since we think that either i_1 or i_2 in G' can represent i in G), and its weight is the same as the original link (i, j) (i.e., we set its disruption cost as $c'(p_i, q_j) = c(i, j)$). More importantly, it is shown that the aboved construction process preserves the relative performance guarantees [11]. Then, the sets of nodes and links in G' are expressed as

$$G' = (V', E') \begin{cases} V' = \{i_1, i_2 | i \in V\} \\ E' = \{(i_1, i_2) | i \in V\} & i \neq j. \\ \cup \left\{(p_i, q_j) | (i, j) \in E\right\}, \end{cases} \tag{9}$$

Therefore, the links in G' can be mapped to the nodes and links in G. We can then apply the spectral partitioning method to transform topological vulnerability analysis into a discrete partition problem about the total weights (i.e., costs). For the spectral partitioning method, the undirected auxiliary graph G' is valid for joint consideration of nodes' weights and links' weights in G, because it has the same weight for each element and connection relationship between each weight as G.

Next, we derive the objective function in (5) using the spectral partitioning method on the undirected auxiliary graph G'. In particular, we consider a n'-dimensional ($n' = 2n$) vector $\mathbf{x}$ where $x_i = 1$ if $i \in A$ and $x_i = -1$ otherwise. Let $\mathbf{W} = \{w_{ij}\}$ be the cost matrix of G' where $w_{ij} = c'(i, j)$ if $(i, j) \in E'$ and $w_{ij} = 0$ if $(i, j) \notin E'$. $\mathbf{D} = \{d_{ij}\}$ is a diagonal matrix where $d_{ii} = \sum_{j \in V'} c'(i, j)$ and zero elsewhere. The graph Laplacian matrix of G' is defined as $\mathbf{L} = \mathbf{D} - \mathbf{W}$. Here, the unconnected subnetworks in disrupted G' are denoted as A' and B' which can be mapped to A and B in G. We use $S_{G'}^{\text{link}}$ to represent the targeted links' set connecting A' and B', and it can be uniquely mapped to G and obtain the vulnerable elements set S in G. Then we can rewrite the VA_{goal} in G' as

$$\begin{aligned} VA_{\text{goal}}(S_{G'}^{\text{link}}) &= \min \frac{\sum_{i \in A', j \in B'} c'(i, j)}{\widehat{I}_{mp}(A') \cdot \widehat{I}_{mp}(B')} \\ &= \min_{\widehat{I}_{mp}(A') = \widehat{I}_{mp}(B')} \sum_{i \in A', j \in B'} c'(i, j) \\ &= \min_{\substack{\mathbf{x} \in \{-1, 1\}^{n'} \\ \mathbf{x}^T \mathbf{D} \mathbf{1} = 0}} \frac{1}{4} \sum c'(i, j)(x_i - x_j)^2 \\ &= \frac{1}{4} \min_{\substack{\mathbf{x} \in \{-1, 1\}^{n'} \\ \mathbf{x}^T \mathbf{D} \mathbf{1} = 0}} \mathbf{x}^T \mathbf{L} \mathbf{x}, \end{aligned} \tag{10}$$

where $\mathbf{1}$ is an n'-dimensional column vector whose all components are 1, and

$$\widehat{I}_{mp}(A') = \sum_{u \in A', t \in V'} c'(u, t) \tag{11}$$

$$\begin{aligned}\widehat{I}_{mp}(A') + \widehat{I}_{mp}(B') &\triangleq \widehat{I}_{mp}(G') \\ &= 2\sum_{(i,j)\in E'} c'(i,j) \\ &= \widetilde{I}_{mp}(G), \end{aligned} \tag{12}$$

and we have the equation that $\widehat{I}_{mp}(A') = \widetilde{I}_{mp}(A)$. $S^{\text{link}}_{G'} = \{(i,j)|(i,j) \in E',\ x_i = 1 \text{ and } x_j = -1\}$ is the set of the links (i.e., the vulnerable nodes and links in G) connecting subnetworks A' and B' in G'.

Minimizing (10) is a partitioning problem that finds the optimal vector $\mathbf{x}$, and it needs to minimize the numerator and maximize the denominator at the same time. Minimizing the numerator means that the set $S^{\text{link}}_{G'}$ corresponding to the optimal vector $\mathbf{x}$ is an elements set with low total disruption cost. To obtain the optimal vector $\mathbf{x}$, we transform (10) and formulate the following overall problem.

Problem (I)

$$\min\ \mathbf{x}^T\mathbf{L}\mathbf{x} \tag{13a}$$

$$\text{s.t. } \mathbf{x} \in \{1, -1\}^{n'} \tag{13b}$$

$$\mathbf{x}^T\mathbf{D}\mathbf{1} = 0 \tag{13c}$$

$$\mathbf{x}^T\mathbf{D}\mathbf{x} = \widehat{I}_{mp}(G'), \tag{13d}$$

since $\widehat{I}_{mp}(G') = \widetilde{I}_{mp}(G)$, it is a constant term. Note that Problem (I) is NP-hard because the element x_i of the vector $\mathbf{x}$ can only take the values ±1.

V. EQUIVALENT TRANSFORMATION AND SOLUTION

To solve the NP-hard problem in (13), we consider relaxing the constraint that the element x_i of the vector $\mathbf{x}$ can only take two values. Then, the above problem is transformed as

$$\min\ \mathbf{x}^T\mathbf{L}\mathbf{x} \tag{14a}$$

$$\text{s.t. } \mathbf{x} \in \mathbb{R}^{n'} \tag{14b}$$

$$\mathbf{x}^T\mathbf{D}\mathbf{1} = 0 \tag{14c}$$

$$\mathbf{x}^T\mathbf{D}\mathbf{x} = 1, \tag{14d}$$

where the constraint (14d) is the normalization of $\mathbf{x}$. To ensure the rationality of the constraint relaxation, given a solution of (14), it is still equivalent to a partitioning problem by setting a reasonable threshold τ and using the following *Spectral Partition* method [18].

Spectral Partition: Given a graph $G_1 = (V_1, E_1, w_e)$, where w_e is the weight of an edge in E_1 and $n_1 = |V_1|$, and $\boldsymbol{\varphi}$ is a n_1 dimensional vector. Consider the two-dimensional map as

$$i \rightarrow \varphi(i), \tag{15}$$

where i is the label corresponding to a node, and $\varphi(i)$ is the i^{th} component of $\boldsymbol{\varphi}$. Set a threshold τ and set

$$\begin{aligned} A_1 &= \{i \in V_1 : \varphi(i) \leq \tau\} \\ \text{and } B_1 &= \{i \in V_1 : \varphi(i) > \tau\}, \end{aligned} \tag{16}$$

where τ is the threshold chosen for the spectral partition. In the following, we choose $\tau = 0$ to map the partition values ±1 mentioned above.

To compute the optimal vector $\mathbf{x}$ easily, we convert (14) into an eigenvector problem by setting the vector $\mathbf{y} = \mathbf{D}^{\frac{1}{2}}\mathbf{x}$ and the matrix $\mathbf{N} = \mathbf{D}^{-\frac{1}{2}}\mathbf{L}\mathbf{D}^{-\frac{1}{2}}$. By doing so, Problem (I) can be re-expressed as the following minimization problem.

Problem (II)

$$\min\ \frac{\mathbf{y}^T\mathbf{N}\mathbf{y}}{\mathbf{y}^T\mathbf{y}} \tag{17a}$$

$$\text{s.t. } \mathbf{y} \in \mathbb{R}^{n'} \tag{17b}$$

$$(\mathbf{D}^{\frac{1}{2}}\mathbf{1})^T\mathbf{y} = 0 \tag{17c}$$

$$||\mathbf{y}||_2{}^2 = 1. \tag{17d}$$

Note that the matrix $\mathbf{N}$ is the normalized graph Laplacian matrix of the auxiliary graph G', which is symmetric positive-semidefinite. The matrix $\mathbf{N}$ has n' nonnegative and real-valued eigenvalues $0 = \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_{n'}$, and all of its eigenvectors are orthogonal to each other. We can easily verify that $\mathbf{y}_1 = \mathbf{D}^{\frac{1}{2}}\mathbf{1}$ is the eigenvector corresponding to the eigenvalue $\lambda_1 = 0$. Hence, $\mathbf{y}_1$ is the smallest eigenvector of the matrix $\mathbf{N}$ and is orthogonal to the other eigenvectors of matrix $\mathbf{N}$. Next, we use the *Rayleigh Quotient* [28] to obtain the optimal vector $\mathbf{x}$ for minimizing VA_{goal}.

Rayleigh Quotient: Let $\mathbf{M}$ be a real symmetric matrix. Under the constraint that vector $\mathbf{z}$ is orthogonal to the $t-1$ smallest eigenvectors $\mathbf{z}_1, \mathbf{z}_2 \ldots \mathbf{z}_{t-1}$, the quotient $\frac{\mathbf{z}^T\mathbf{M}\mathbf{z}}{\mathbf{z}^T\mathbf{z}}$ is minimized by the next smallest eigenvector $\mathbf{z}_t$.

Therefore, the second smallest eigenvector $\mathbf{y}_2$ of $\mathbf{N}$ is the solution to Problem (II). The optimal $\mathbf{x}$ in (14) is given by $\mathbf{x} = \mathbf{D}^{-\frac{1}{2}}\mathbf{y}_2$. We then use the optimal $\mathbf{x}$ to solve the partitioning problem of minimization for (10) by using *Spectral Partition*.

Then, $S^{\text{link}}_{G'} = \{(i,j)|(i,j) \in E',\ i \in A' \text{ and } j \in B'\}$ is the set of links connecting subnetworks A and B. We map $S^{\text{link}}_{G'}$ in G' to S in G, obtaining the targeted vulnerable nodes and links for G.

A. ALGORITHM FOR MINIMIZING VA_{goal}

To dynamically predict potential threats in IoV environments, in our proposed IVA-CC method, the roadside servers intelligently find critical areas and vulnerable elements in the system. For a given disruption level α, the process of our solution is shown in Algorithm 1. First, IVA-CC uses the spectral partitioning method to identify a minimum-cost element set $S^{\text{link}}_{G'}$ with the smallest $VA_{\text{goal}}(S^{\text{link}}_{G'})$, breaking the network into two unconnected subnetworks and disrupting critical-area integrity. Then repeating this process in the subnetworks until disruption level α is reached. Afterwards, IVA-CC conducts *LocalSearch* on the results of the spectral partitioning method, finding the most vulnerable elements in critical area. Based on this, the set of vulnerable elements S can be obtained. The goal of *LocalSearch* is to find vulnerable elements set with smaller $VA_{\text{goal}}(S)$ value as follows:

1. If there are $t(t \geq 2)$ links $(i, j_1), \ldots, (i, j_t) \in S$, determine whether $i \in G\backslash S$ can replace $(i, j_1), \ldots, (i, j_t)$;

2. For each element $e \in S$, determine whether its neighbor $e' \in G\backslash S$ can replace it;

Algorithm 1 Algorithm for Minimizing VA_{goal}

```
1:  Initialize: $S = \phi$, $S_{G'}^{\text{link}} = \phi$, $\tau = 0$, $\sigma = 0.05$;
2:  Construct the undirected auxiliary graph $G' = (V', E')$;
3:  Construct matrix $\mathbf{N}$;
4:  Solve **Problem (II)** to get $\mathbf{y}_2$ and get $\mathbf{x} = \mathbf{D}^{-\frac{1}{2}}\mathbf{y}_2$;
5:  Use *Spectral partition* to get subnetworks $A'$ and $B'$;
6:  **if** $u \in A'$, $v \in B'$ and $(u, v) \in E'$ **then**
7:      $(u, v) \in S_{G'}^{\text{link}}$;
8:  **end if**
9:  Map $S_{G'}^{\text{link}}$ back to $G$, get $S$;
10: **while** $P(G \backslash S) > (1 - \alpha + \sigma)\binom{n}{2}$ **do**
11:     **for** subnetworks $A$ and $B$ **do**
12:         Step 3-8, get $S_{A'}^{\text{link}}$, $S_{B'}^{\text{link}}$
13:         Find among $S_{G'}^{\text{link}} + S_{A'}^{\text{link}}$ and $S_{G'}^{\text{link}} + S_{B'}^{\text{link}}$ with
            the minimum $VA_{\text{goal}}$ and update $S$ (i.e., $S = S + S_A$ or $S + S_B$);
14:     **end for**
15: **end while**
16: **for** each network element $e \in S$ **do**
17:     *LocalSearch*$(e)$;
18: **end for**
19: Output $S$
```

3. If it is possible, merge two subnetworks in $G \backslash S$ by removing the links or nodes between them from S until $(1-\alpha-\sigma)\binom{n}{2} < P(G \backslash S) \leq (1-\alpha+\sigma)\binom{n}{2}$, where σ is used to extend the limit of α moderately [11], and we set $\sigma = 0.05$.

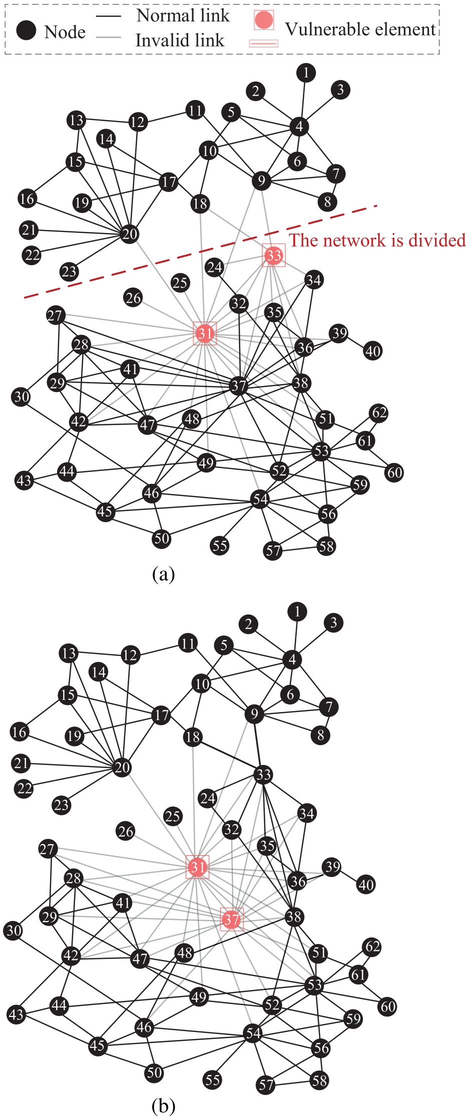
Solving for the Second Smallest Eigenvector: We use the eigenvector calculation tool with Python-NetworkX package to complete the calculation, and we have verified the accuracy by using the Conjugate gradient method with Gram-Schmidt orthogonalisation method provided in [28].

VI. PERFORMANCE EVALUATION

A. CASE STUDY

To verify the effectiveness of our IVA-CC method in the practical IoV environment, we evaluate its performance on a real network. Fig. 4 shows an actual terrorist network [29] with 62 nodes and 153 links, reflecting the communication connection between the terrorists. Node 31 is the critical node of this network, which represents the ringleader of the conspiracy.

Degree centrality is a well-known classic method to identify critical nodes and critical areas. Therefore, here we compare the proposed IVA-CC method with the degree-centrality-based method [6] to verify our advantages, as shown in Fig. 4(a, b). The IVA-CC method aims to find a targeted set whose removal breaks the network into two parts. With the aim of achieving the same total disruption cost of the IVA-CC's vulnerable elements, the degree-centrality-based method aims to find the nodes with the highest degree centrality. In Fig. 4(a), on the basis of disrupting the network into two unconnected subnetworks, the IVA-CC method effectively locates the critical node 31 and 33 of this network, because IVA-CC gives priority to analyzing the critical-area vulnerability. In Fig. 4(b), we see that removing nodes 31 and 37 according to [6] has a less significant impact on the network connectivity and performance compared to IVA-CC, which will be considered in more detail in Fig. 7. Therefore, the proposed IVA-CC method identifies the most damaging scenario in the case of a real terrorist network. This shows that IVA-CC is effective in analyzing the topology vulnerability of real network. Moreover, for heterogeneous IoV applications, our solution can not only intelligently identify critical areas but also provide theoretical evidence for promoting system security.



(a)

(b)

FIGURE 4. Terrorist network with vulnerable elements in two methods: (a) proposed IVA-CC method, (b) degree-centrality-based method [6].

B. SIMULATION RESULTS AND ANALYSIS

In this section, we evaluate the proposed IVA-CC method in a Python simulation environment to verify its feasibility in the IoV. In addition, an NS2 network simulator is adopted for network environment simulation.

As mentioned above, a key contribution of this paper is: when analyzing topological connectivity vulnerability, we intelligently give priority to analyzing the critical area in the network. Degree centrality and betweenness centrality are two well-known classic methods to identify critical nodes and critical areas. Therefore, we compare our IVA-CC method with these two methods to verify our advantages. Specifically, we compare the following vulnerability analysis methods (for a fair comparison, we adopt the same *LocalSearch* used in IVA-CC):

- Node Vulnerability analysis with Degree (NVD) iteratively removes the node with the highest degree centrality [6], and then performs *LocalSearch*;
- Node Vulnerability analysis with Betweenness (NVB) iteratively removes the node with the highest betweenness centrality [7], and then performs *LocalSearch*.

In the simulations, we consider two types of networks: (1) the terrorist network [29]; (2) the NW small world network model [30], which shares many important properties with real networks.

Fig. 5 shows the total cost (the smaller the better) of vulnerable elements in three methods as a function of the disruption level α for the terrorist network. Specifically, the smaller the total costs of the vulnerable elements, the more vulnerable they are, i.e., the harder they are to defend against attack. This figure demonstrates that the cost increases with disruption level α increasing because of the positive correlation between them. Meanwhile, the IVA-CC method performs far better than the NVD and NVB methods, regardless of disruption level α, especially when $\alpha = 50\%$. The costs in IVA-CC are only about one-third of that in the other methods when the disruption level is 50%. This is because the IVA-CC method identifies the network elements that are low in cost and of great importance to network connectivity. Therefore, our solution can identify the connection weakness in the IoV systems.

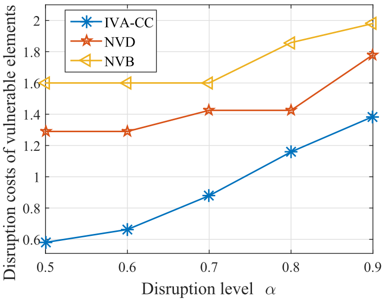


FIGURE 5. Total costs versus disruption level α.

To further verify the advantages of our IVA-CC method in intelligently identifying critical areas, in Fig. 6 (a, b), we consider the NW network topology with different network sizes as represented by the number of nodes. We focus on the performance of the methods at disruption level $\alpha = 50\%$, and we show the average results of 20 testings. Fig. 6(a) depicts the total cost of the vulnerable elements in three methods as a function of network size. It is clear that the IVA-CC method outperforms the NVD and NVB methods regardless of network size, because the cost in IVA-CC is at least one-half that in the other methods.

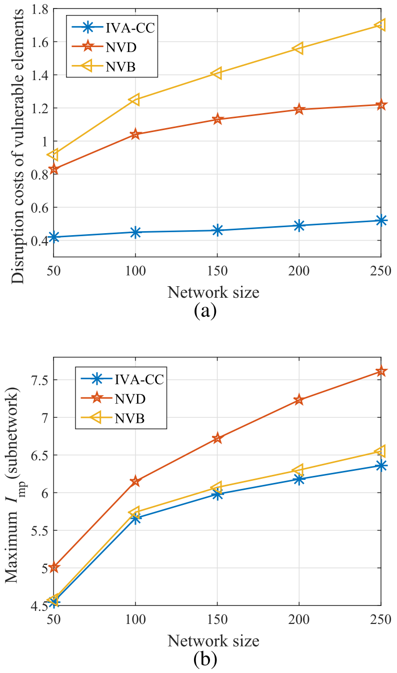


FIGURE 6. (a) Total costs with $\alpha = 50\%$ versus network size, (b) Maximum I_{mp}(subnetwork) with $\alpha = 50\%$ versus network size.

As mentioned above, the value of $I_{\mathrm{mp}}(A)$ can indicate the importance degree of subnetwork A. We assume that the vulnerable elements as Fig. 6(a) in the three methods are disrupted by attackers, and we utilize the maximum I_{mp}(subnetwork) to find the most important subnetwork in the residual network. Therefore, a smaller value of maximum I_{mp}(subnetwork) indicates greater disruption to critical-area integrity. Fig. 6(b) depicts the maximum I_{mp}(subnetwork) in three methods as a function of network size. It demonstrates that the IVA-CC outperforms the NVB and NVD methods. Meanwhile, the IVA-CC method exhibits the outstanding performance according to the Figs. 6(a) and (b). Compared with the NVD and NVB methods in Figs. 6(a) and (b), the set of vulnerable elements in IVA-CC is a smaller-cost set, and the disruption of the vulnerable elements set in IVA-CC leads to greater disruption of critical-area integrity than that in the NVD and NVB methods. This is because IVA-CC gives priority to finding minimum-cost elements that can jointly disrupt network connectivity and critical-area integrity. Therefore, our solution can intelligently find the critical area of high vulnerability, and it is well-suited for heterogeneous IoV systems.

In addition, to visualize the impact of the failure of vulnerable elements on system performance and reflect the high vulnerability of the results in IVA-CC, we compare the terrorist network and the NW network using NS2 simulator, and further simulate the disruption of the vulnerable elements in three methods. For a fair comparison, we analyze the three sets of vulnerable elements with the same disruption cost (i.e., the cost in IVA-CC at $\alpha = 50\%$) in the three methods. Fig. 7 shows the total throughput of 12 communication node pairs in the three disrupted terrorist networks (i.e., the networks in which the vulnerable elements in the three methods are disrupted) as a function of time, together with that of the normal terrorist network. Fig. 8 shows the total throughput of 12 communication node pairs in the three disrupted NW networks as a function of time, together with that of the normal NW network. We show the average results of 20 tests in the NW network with 100 nodes.

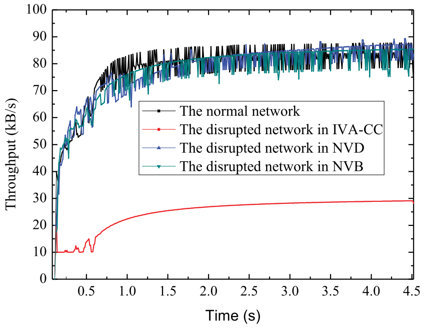


FIGURE 7. Throughput versus time for the terrorist network.

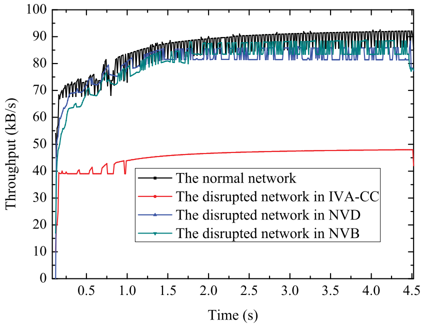


FIGURE 8. Throughput versus time for the NW network.

As can be seen from Figs. 7 and 8, when the vulnerable elements of the two networks in the three methods fail, the throughput of the disrupted terrorist network in IVA-CC drops substantially to about one-third of that of the normal terrorist network, and the throughput of the disrupted NW network in IVA-CC drops substantially to about one-half of that of the normal NW network. However, the throughputs of the two disrupted networks in NVD and NVB are close to those of the corresponding normal networks. There are two reasons for this difference. On the one hand, the vulnerable elements in IVA-CC contain critical elements with strong control or bridging ability, and these disrupted critical elements have strong negative effects on network connectivity. On the other hand, the failure of the vulnerable elements in IVA-CC leads to greater disruption to network connectivity than that of the other methods at the same disruption cost. This also demonstrates that network connectivity and critical-area integrity are vital to network throughput performance.

Therefore, by intelligently identifying critical areas, IVA-CC is particularly effective for analyzing the weakness of system connectivity. Meanwhile, the results from IVA-CC can provide a reliable theoretical basis for the security planning of the IoV systems.

VII. CONCLUSION

In a heterogeneous and dynamic IoV system, increasing the robustness of the system usually requires installing redundant resources or over provisioning, which is very costly. Fortunately, AI technology can intelligently identify critical areas in the current environment, and vulnerability analysis can effectively predict the occurrence of risks. Therefore, we focus on the intelligent vulnerability analysis for the IoV systems.

Physical interconnection is the functional premise of the IoV applications. Meanwhile the failure of network's critical areas poses a serious threat. To identify the most fatal damage to a network or system, in this paper we consider the worst-case scenario and propose an intelligent vulnerability analysis method considering connectivity and critical-area integrity. We consider an intelligent analysis scenario where roadside servers continuously learn IoV heterogeneous environment and dynamic topology, and then obtain the costs of network elements. Based on this, our goal is to find the network elements that are of vital importance to network connectivity and critical-area integrity, but the elements are vulnerable owning to not given adequate protection. Simulation results indicate that our proposed method exhibits outstanding advantages in locating vulnerable elements and preventing performance loss in the IoV systems.

REFERENCES

[1] J. Zhang, L. Fu, Q. Wang, L. Liu, X. Wang, and X. Wang, "Connectivity analysis in wireless networks with correlated mobility and cluster scalability," *IEEE/ACM Trans. Netw.*, vol. 25, no. 4, pp. 2375–2390, Aug. 2017.

[2] Z. Ning, R. Y. K. Kwok, K. Zhang, X. Wang, M. S. Obaidat, L. Guo, X. Hu, B. Hu, Y. Guo, and B. Sadoun, "Joint computing and caching in 5G-envisioned Internet of vehicles: A deep reinforcement learning-based traffic control system," *IEEE Trans. Intell. Transp. Syst.*, early access, Feb. 5, 2020, doi: 10.1109/TITS.2020.2970276.

[3] A. Reggiani, P. Nijkamp, and D. Lanzi, "Transport resilience and vulnerability: The role of connectivity," *Transp. Res. A, Policy Pract.*, vol. 81, pp. 4–15, Nov. 2015.

[4] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, Aug. 2019.

[5] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[6] S. P. Borgatti and M. G. Everett, "A graph-theoretic perspective on centrality," *Social Netw.*, vol. 28, no. 4, pp. 466–484, Oct. 2006.

[7] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and vulnerability analysis of key nodes in power grid based on complex network centrality," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 3, pp. 346–350, Mar. 2018.

[8] X. Liu, "Survivability-aware connectivity restoration for partitioned wireless sensor networks," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2444–2447, Nov. 2017.

[9] Y. Shen, N. P. Nguyen, Y. Xuan, and M. T. Thai, "On the discovery of critical links and nodes for assessing network vulnerability," *IEEE/ACM Trans. Netw.*, vol. 21, no. 3, pp. 963–973, Jun. 2013.

[10] T. N. Dinh, Y. Xuan, M. T. Thai, P. M. Pardalos, and T. Znati, "On new approaches of assessing network vulnerability: Hardness and approximation," *IEEE/ACM Trans. Netw.*, vol. 20, no. 2, pp. 609–619, Apr. 2012.

[11] T. N. Dinh and M. T. Thai, "Network under joint node and link attacks: Vulnerability assessment methods and analysis," *IEEE/ACM Trans. Netw.*, vol. 23, no. 3, pp. 1001–1011, Jun. 2015.

[12] Y. Yu, S. Liu, L. Guo, P. L. Yeoh, B. Vucetic, and Y. Li, "CrowdR-FBC: A distributed fog-blockchains for mobile crowdsourcing reputation management," *IEEE Internet Things J.*, early access, May 21, 2020, doi: 10.1109/JIOT.2020.2996229.

[13] S. Trajanovski, F. A. Kuipers, A. Ilic, J. Crowcroft, and P. Van Mieghem, "Finding critical regions and region-disjoint paths in a network," *IEEE/ACM Trans. Netw.*, vol. 23, no. 3, pp. 908–921, Jun. 2015.

[14] Z. Ning, Y. Li, P. Dong, X. Wang, M. S. Obaidat, X. Hu, L. Guo, Y. Guo, J. Huang, and B. Hu, "When deep reinforcement learning meets 5G-enabled vehicular networks: A distributed offloading framework for traffic big data," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1352–1361, Feb. 2020.

[15] M. Yi, X. Xu, and L. Xu, "An intelligent communication warning vulnerability detection algorithm based on IoT technology," *IEEE Access*, vol. 7, pp. 164803–164814, Nov. 2019.

[16] Y. Yu, F. Li, S. Liu, J. Huang, and L. Guo, "Reliable fog-based crowdsourcing: A temporal-spatial task allocation approach," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3968–3976, May 2020.

[17] X. Wang, Z. Ning, X. Hu, L. Wang, L. Guo, B. Hu, and X. Wu, "Future communications and energy management in the Internet of vehicles: Toward intelligent energy-harvesting," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 87–93, Dec. 2019.

[18] W. Asif, M. Lestas, H. Khaliq Qureshi, and M. Rajarajan, "Optimization based spectral partitioning for node criticality assessment," *J. Netw. Comput. Appl.*, vol. 75, pp. 279–292, Nov. 2016.

[19] M. Lalou, M. A. Tahraoui, and H. Kheddouci, "The critical node detection problem in networks: A survey," *Comput. Sci. Rev.*, vol. 28, pp. 92–117, May 2018.

[20] T. N. Dinh, M. T. Thai, and H. T. Nguyen, "Bound and exact methods for assessing link vulnerability in complex networks," *J. Combinat. Optim.*, vol. 28, no. 1, pp. 3–24, Jul. 2014.

[21] Y. Yu, L. Guo, J. Huang, F. Zhang, and Y. Zong, "A cross-layer security monitoring selection algorithm based on traffic prediction," *IEEE Access*, vol. 6, pp. 35382–35391, Jul. 2018.

[22] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T. Qiu, and R. Y. K. Kwok, "Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach," *IEEE J. Sel. Areas Commun.*, vol. 99, pp. 1–16, Mar. 2020.

[23] Y. Yu, L. Guo, S. Liu, J. Zheng, and H. Wang, "Privacy protection scheme based on CP-ABE in crowdsourcing-IoT for smart ocean," *IEEE Internet Things J.*, early access, Apr. 22, 2020, doi: 10.1109/JIOT.2020.2989476.

[24] W. Peng, Z. Li, Y. Liux, and J. Su, "Assessing the vulnerability of network topologies under large-scale regional failures," *J. Commun. Netw.*, vol. 14, no. 4, pp. 451–460, Aug. 2012.

[25] M. N. Kabir, M. A. Rahman, S. Azad, M. M. A. Azim, and M. Z. A. Bhuiyan, "A connection probability model for communications networks under regional failures," *Int. J. Crit. Infrastruct. Protection*, vol. 20, pp. 16–25, Mar. 2018.

[26] Z. Ning, K. Zhang, X. Wang, L. Guo, X. Hu, J. Huang, B. Hu, and R. Y. K. Kwok, "Intelligent edge computing in Internet of vehicles: A joint computation offloading and caching solution," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 5, 2020, doi: 10.1109/TITS.2020.2997832.

[27] J. Shi and J. Malik, "Normalized cuts and image segmentation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 8, pp. 888–905, Aug. 2000.

[28] G. H. Golub and C. F. Van Loan, *Matrix Computations*. Baltimore, MD, USA: Johns Hopkins Univ. Press, 2012.

[29] V. Krebs, "Uncloaking terrorist networks," *1st Monday*, vol. 7, no. 4, Apr. 2002.

[30] M. E. J. Newman and D. J. Watts, "Renormalization group analysis of the small-world network model," *Phys. Lett. A*, vol. 263, nos. 4–6, pp. 341–346, Dec. 1999.

SHUMEI LIU received the B.S. degree in electronics and information engineering from Shanxi University, Taiyuan, China, in 2016, and the M.S. degree in electronics and communication engineering from Northeastern University, Shenyang, China, in 2018, where she is currently pursuing the Ph.D. degree in communication and information systems. Her research interests include the Internet-of-Things (IoT), mobile edge computing, vulnerability analysis, and physical layer security. She has received the Best Paper Award from the National Postdoctoral Academic Forum, China, in 2018.

YAO YU (Member, IEEE) received the B.S. degree in communication engineering and the Ph.D. degree in communication and information systems from Northeastern University, Shenyang, China, in 2005 and 2010, respectively. From 2010 to 2011, she was a Postdoctoral Fellow of the Department of Computing, The Hong Kong Polytechnic University, Hong Kong. She is currently an Associate Professor with the School of Computer Science and Engineering, Northeastern University. Her current research interests include network security and big data.

WENJIAN HU received the B.S. degree in detection guidance and control technology from Shenyang Ligong University, Shenyang, China, in 2019. He is currently pursuing the master's degree in information and communication engineering with Northeastern University. His research focuses on network security.

YUHUAI PENG (Member, IEEE) received the Ph.D. degree in communication and information systems from Northeastern University, in 2013. He is currently an Associate Professor with Northeastern University. His research interests include the Internet of Things (IoT), industrial communication networks, and health monitoring.

XIAOLONG YANG (Member, IEEE) received the B.Eng., M.S., and Ph.D. degrees in communication and information systems from the University of Electronic Science and Technology of China, Chengdu, China, in 1993, 1996, and 2004, respectively. He is currently a Professor with the School of Computer and Communication Engineering, Institute of Advanced Networking Technologies and Services, University of Science and Technology Beijing, Beijing, China. He has fulfilled more than 30 research projects. He has authored more than 80 articles. He holds 16 patents in his research areas. His current research interests include the next-generation Internet, network security and defense, and anonymity networking.