

## Research Article

# **Fault-Aware Resource Allocation for Heterogeneous Data Sources with Multipath Routing**

## Xiaomei Zhang, Qiang Chen, Zhicai Shi, and Jianru Liang

School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, 333 Long Teng Road, Shanghai 201620, China

Correspondence should be addressed to Xiaomei Zhang; zxm\_ccnu@hotmail.com

Received 1 March 2017; Accepted 24 April 2017; Published 17 September 2017

Academic Editor: Chi-Hung Chi

Copyright © 2017 Xiaomei Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of cloud computing and big data, diverse types of traffic generated from heterogeneous data sources are delivered throughout communication networks, which consist of various node kinds such as digital sensors and smart actuators, and different applications. Due to the shared medium, communication networks are vulnerable to misbehaving nodes, and it is a crucial aspect to maintain an acceptable level of service degradation. This paper studies the fault-aware resource allocation problem by exploiting multipath routing and dynamic rate assignment for heterogeneous sources. We estimate the impacts of faults and formulate the resource allocation as a lossy network flow optimization problem based on these estimates. The traditional flow optimization solutions focus on homogeneous traffic. In our work, we model the performance of heterogeneous applications as a relaxed utility function and develop an effective utility framework of rate control for heterogeneous sources with multipath routing in presence of misbehaving nodes. We design a distributed algorithm to decide the routing strategy and obtain the rate assignments on the available paths in a lossy utility fair manner. Extensive performance evaluations corroborate the significant performance of our algorithm in effective utility fairness in the presence of misbehaving nodes.

## 1. Introduction

With the rapid development of cloud computing and big data, communication networks where a wide variety of devices can be connected are increasingly used in dataintensive applications, such as video surveillance, robots, industrial process control, and mobile entities [1]. Various types of traffic generated from heterogeneous data sources have increasing growth in demand for efficient transmission services, for example, traditional data, audio, video, and multimedia delivery through the network [2]. Different qualityof-service (QoS) requirements of these services are specified in the form of application performance metrics, which are not easy to be guaranteed in the homogeneous network service architecture. Therefore, communication networks are expected to support heterogeneous data sources with diverse QoS requirements supporting.

Most existing designs of communication networks are based on the assumption that each node is well behaved and cooperative; and packet loss that does occur is mainly due to contention or congestion. Built upon open transmission mediums, communication networks are vulnerable to channel impairments, failure, interference and fading, and so on [3, 4]. Misbehaving nodes always exist along the available paths between sources and destinations. All of these can cause unreliable data transmission, lower effective data rate received successfully at the destination node, and unfairness between different sources [5]. The network performance is significantly degraded by misbehaving nodes particularly for data sources with tight quality-of-service requirements such as real-time provision in city-wide wireless network [6]. How to maintain an acceptable level of network performance degradation for heterogeneous data sources still remains an open problem in the design of a communication network with the presence of misbehaving nodes.

The majority of antifault approaches make use of network redundancy. For example, reliable protocols may introduce multiple routing paths, different spectrums, or multiple wireless channels to curb the effects of malicious attacks or failures. In addition, multipath routing, which can be useful in enhancing the network performance, was actively studied in communication networks [7]. In this paper, we guarantee the QoS requirements based on the use of multiple routing paths. For various applications, higher effective throughput and better fairness offer better QoS. To make efficient utilization of this routing diversity, however, heterogeneous data sources must be able to perform an intelligent traffic allocation along the available paths while considering the potential impact of faults on the effective throughput.

In order to characterize the effect of misbehaving nodes on throughput, each source must rely on direct knowledge of the impact of faulty nodes in various parts of the network. Unfortunately, it is not an easy job to collect information on misbehaving nodes directly, in a realistic environment. Few current works consider uncertainties and dynamics in the adversarial environment. Most of them assume that the misbehavior is fixed with time. In fact, the extent of misbehaviors at each network node depends on many unknown parameters, including malicious nodes' actions, schemes used by attackers, mobility patterns, and other unknown external/internal faults [8-10]. Hence, the impact of faulty nodes is probabilistic from the perspective of the network. We estimate the impact of jamming and characterize the effect of faults as a random process. Each source performs traffic allocation based on statistical information at probabilistic faulty nodes.

To provide better traffic management on multiple paths, Optimal Flow Control (OFC) approach [11], which is regarded as the most successful result in the area of traffic allocation, optimizes the sum utility of homogeneous traffic. Wang et al. [12] have shown that if various applications are run over a network, the OFC approach usually leads to an unfair traffic allocation according to the utility performance for heterogeneous traffic. The objective of heterogeneous applications is no longer to solely maximize the sum utility of the sources. Instead, it is supposed to meet different QoS requirements related to heterogeneous applications. In order to support different traffic types, we model application performance as a generic utility function by relaxing the utility function conditions. Explicitly taking account of misbehaviors' effect, we generalize the OFC approach to obtain new problem formulations, namely, fault-aware utility flow control (FUFC), which can optimize relaxed utilities of lossy flows on multiple routing paths, having the ability to handle a number of heterogeneous traffic.

In this article, we investigate the problem of resource allocation in multiple-path routing strategies for heterogeneous data sources in the event of faulty behaviors. We first model the effect of misbehaviors at each node as a random process due to the misbehavior dynamic and mobility. Owing to traversing over the probabilistic faulty paths, the flow at the destination node must be studied using a stochastic framework and smaller than that from the source node. We formulate this rate allocation as a lossy flow optimization problem for multipath routing while considering the thinning feature of data flows across faulty paths. In order to support heterogeneous traffic, we relax the utility function conditions in our lossy optimization problem. Then we design a distributed rate control algorithm that allocates source rate so that the performance of heterogeneous data sources is guaranteed. Each source has the ability to compensate for misbehaviors in network performance degradation across multiple routing paths in terms of utilities, rather than performance degradation in terms of rates. In this way, our algorithm improves the utility performance of heterogeneous sources according to different QoS requirements resulting in overall improvement in system performance.

The main contributions of this paper are outlined as follows:

- (i) We formulate the problem of allocating traffic across multiple routing paths in the presence of faulty nodes as a network lossy flow optimization problem which can optimize relaxed utilities, having the ability to handle heterogeneous traffic.
- (ii) We propose an approach which allows network nodes to locally characterize the impact of the nondeterministic and dynamic faulty behaviors and aggregate this information for the heterogeneous source nodes. Each source can introduce bias into rate allocation and routing decisions, leading to compensating for misbehaviors in network performance degradation in terms of utility return.
- (iii) We provide a novel distributed algorithm, FUFC, to be friendly with heterogeneous applications and allocate the effective rate in lossy utility fair manner.
- (iv) Through comprehensive performance comparisons, we demonstrate the considerable gains in network performance including higher effective throughput and better fairness among heterogeneous sources that can be achieved by our algorithm.

The rest of the paper is organized as follows. We depict our system model in Section 2. We propose methods that allow nodes to estimate the impact of misbehaviors and model the leaky-path flow in Section 3. In Section 4, we present the fault-aware utility flow control approach with multipath routing. The performance of our algorithm is evaluated in Section 5. Finally, we describe the related work in Section 6 and conclude the paper in Section 7.

#### 2. System Model and Assumptions

2.1. Network Model. We consider a network with a set  $\mathcal{L} = \{1, 2, ..., L\}$  of links of capacity  $c_l, l \in \mathcal{L}$ , and a set  $\mathcal{V} = \{1, 2, ..., V\}$  of nodes. We denote a link as a pair of nodes (i, j), where  $i \in \mathcal{V}$  is the transmitter of the link and  $j \in \mathcal{V}$  is the receiver. The network is shared by a set  $\mathcal{S} = \{1, 2, ..., S\}$  of sources, and  $\mathcal{S} \subseteq \mathcal{V}$ . Each source  $s \in \mathcal{S}$  has  $k_s$  available paths or routes from the source to destination. Denote  $L \times 1$  vector  $\mathcal{R}_{s,n}$  the set of links used by source  $s \in \mathcal{S}$  on its path  $n \in \{1, 2, ..., k_s\}$ , whose *l*th element is equal to 1 if and only if the path passes through link *l* and 0 otherwise. Then the set of all the available paths of source *s* is defined by

$$\mathcal{R}_{s} = \left[\mathcal{R}_{s,1}, \mathcal{R}_{s,2}, \dots, \mathcal{R}_{s,k_{s}}\right], \tag{1}$$



FIGURE 1: An example network with heterogeneous sources.

and the whole set of paths in the network is defined by a  $L \times K$  routing matrix  $\mathcal{R}$ 

$$\mathcal{R} = \left[\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_S\right],\tag{2}$$

where  $K = k_1 + k_2 + \dots + k_s$  is the total number of paths.

Denote the  $k_s \times 1$  vector  $A_{s,l}$  as the set flow s' paths pass through link l, whose *n*th element is equal to 1 if the path  $\mathcal{R}_{s,n}$  of flow s contains link l, and 0 otherwise. For each source s, define  $x_{s,n}$  be the rate of source s on the path  $\mathcal{R}_{s,n}$ , and obviously the total source rate  $x_s = \sum_{n=1}^{k_s} x_{s,n}$ , where  $x_s \in [m_s, M_s]$ , where  $m_s \ge 0$  and  $M_s < \infty$  are the required minimum and maximum source rate, respectively. Let

$$X = \left[x_{1,1}, \dots, x_{1,k_1}, x_{2,1}, \dots, x_{2,k_2}, \dots, x_{k,1}, \dots, x_{k,k_s}\right]^T \quad (3)$$

be the corresponding vector of all path rates of all sources and let the  $k_s \times 1$  vector  $F_s = [x_{s,1}, \ldots, x_{s,k_s}]^T$  denote the set of all path rates of source *s*.

Figure 1 illustrates an example network of the sources  $s_1, s_2, s_3, s_4$ . Each source consists of multiple routing paths:

$$\begin{aligned} \mathcal{R}_{s_{1},1} &= \{(A,B), (B,C), (C,F)\}, \\ \mathcal{R}_{s_{1},2} &= \{(D,E), (E,F)\}, \\ \mathcal{R}_{s_{2},1} &= \{(D,E), (E,F), (F,I)\}, \\ \mathcal{R}_{s_{2},2} &= \{(G,H), (H,I)\}, \\ \mathcal{R}_{s_{3},1} &= \{(A,B), (B,C), (C,F)\}, \\ \mathcal{R}_{s_{3},2} &= \{(G,H), (H,F)\}. \end{aligned}$$
(4)

For communication networks, usually, users focus on source rate and throughput at the destination node. However, since networks consist of various node types or modalities, as shown in Figure 1, there may exist different applications with diverse utility behaviors. Each application uses its utility as a measure of the QoS performance in terms of provided services. Regardless of the types of sources, we assume that utility  $U_s(x_s)$  is achieved by the traffic as a function of its rate  $x_s$ . More generally, utilities of multiple applications can be categorized as follows in terms of performance goal perspectives [12]:

- (i) Elastic utility for traditional data services such as file transfer, mail, and ftp;
- (ii) Real-time utility for delay-sensitive services such as video surveillance, real-time monitoring, and teleconferencing;
- (iii) Rate-adaptive utility for real-time rate-adaptive services which are able to adjust their rates dynamically;
- (iv) Stepwise utility for other types of services such as audio and video delivery services via a layered encoding and transmission model.

2.2. Misbehaving Node Model. In this article, we assume that the source nodes have no prior knowledge of the abnormal behaviors of nodes: failures of internal components, or some external attacks/interferences in the adversarial environment. That is, we make no assumption about the strategy used by malicious nodes, mobility patterns, or misbehaviors' goals. Instead of basing on direct of knowledge of the misbehaviors, we suppose that the network nodes characterize the impact of faulty behaviors in terms of their direct impact on throughput. We assume that packet loss occurs not due to contention or congestion but misbehaving nodes, since the former can be managed by the provision of the underlying network protocols. With the existence of misbehaving nodes, the increased packet loss ratio of each node usually occurs, which is caused by the increased probability of collisions for the transmission mechanism. Network nodes can then incorporate the information to the decision of source nodes' optimal rate allocation and routing.

## 3. Estimating the Impact of Misbehaviors and Models for Leaky-Path Flows

In this section, we provide methods for the network node to estimate and characterize the impact of misbehaviors and for a source node to obtain misbehavior information. Before incorporating the impact into traffic allocation and routing, each node j must estimate the effect of misbehaviors on transmissions over link (v, j) and relay it to source s. In the presence of misbehaving nodes, the increased probability of collisions usually leads to the increased packet loss ratio to the time interval *T* influences the qua

of each link for the transmission mechanism. Due to the impact of misbehaviors, network links are lossy in nature. If the international consequently, the flow rate turns into lower and lower across its routing path called leaky-path and the effective data rate

its routing path called leaky-path, and the effective data rate received successfully at the destination node is lower than the transmission rate at the source. To study this, we present the models for lossy links and leaky-path flows in the following.

3.1. Estimating the Impact of Misbehaviors. In this paper, we assume that packet loss or corruption occurs only due to faulty nodes since contention or congestion can be controlled by the provision of the underlying network protocols. Although a faulty node may perform various malicious behaviors, any good node exhibits the same behavior: delivering packets correctly. During the updated period represented by the time interval [t - T, t], each node *j* can record the number of packets received over link and the number of valid packets which pass an error detection check. As the network has no knowledge of the misbehaving nodes actions, the impact of fault is uncertain and probabilistic from the perspective of the network. The behavior of node *v* is formulated as a random variable H(v). The outcomes of H(v) are defined as follows:

$$H(v) = \begin{cases} 1 & \text{if } v \text{ receives the packet successfully,} \\ 0 & \text{otherwise.} \end{cases}$$
(5)

The packet delivery ratio over each link (v, j) can be formulated as a random variable using statistics from node v. Due to the packet loss in faulty links, the data rate of a flow becomes thinner and thinner along its routing path. For a routing path, the behavior of a path  $p = [v_1, v_2, ..., v_p]$  can also be formulated as a random variable T(p). The outcomes of T(p) are defined as follows:

$$T(p) = \begin{cases} 1 & \text{if } p \text{ delivers the packet successfully,} \\ 0 & \text{otherwise.} \end{cases}$$
(6)

Then, the packet delivery ratio over node *j* can itself be characterized as  $h_j = \Pr\{H(j) = 1\}$ , a random variable using statistics from past network communication, due to the network's uncertainty in the faulty node's action. During the time interval [t - T, t], each node *j* records the number n([t - T, t]) of packets received over links, and the number m([t - T, t]) of valid packets. The packet delivery probability over link (i, j) for the update period ([t - T], t) is thus equal to the ratio

$$h_j([t-T,t]) = \frac{m([t-T,t])}{n([t-T,t])}.$$
(7)

In order to reduce significant variation, and to include memory of misbehaviors history, we update the estimation through the previous estimate  $\hat{h}_i(t - T)$  as

$$\widehat{h}_{j}(t) = \alpha \widehat{h}_{j}(t-T) + (1-\alpha)h_{j}([t-T,t]), \qquad (8)$$

where  $\alpha \in [0, 1]$  is a constant weight representing the relative preference between recent and historic samples. The constant

time interval *T* influences the quality of the estimate process. If the interval is too large, the estimate result will be outdated and cost more time. Otherwise, the dynamics of misbehaviors can not be captured, and the result of  $\hat{h}_j$  is not accurate enough. Hence, the choice of *T* depends on the application scenarios. We use a similar estimation procedure to update the variance  $v_l^2$ :

$$\nu_{j}^{2}(t) = \beta \nu_{j}^{2}(t - T_{s}) + (1 - \beta) \mu_{j}([t - T_{s}, t]), \qquad (9)$$

where  $\beta \in [0, 1]$  is a constant weight and  $\mu_j$  is the sample variance of packet delivery ratios computed using (7) during the time interval  $[t - T_s, t]$ . The node collects sample values during time interval  $[t - T_s, t]$ . Hence, the time interval  $T_s$  should be larger than the time interval T.

Given the packet delivery ratio estimates  $h_j(t)$  for the links (i, j) in the routing path  $\mathcal{R}_{s,n}$ , the source *s* needs to estimate the effective end-to-end packet delivery probability. The end-to-end packet success ratio  $\mathcal{R}_{s,n}$  for the path can be formulated as

$$g_{s,n} = \prod_{(i,j)\in\mathcal{R}_{s,n}} h_j,\tag{10}$$

which is also a random variable due to the randomness in variable  $h_j$ . We let  $\hat{g}_{s,n}$  denote as the mean of random variable  $g_{s,n}$  which is equal to the product of estimations  $\hat{h}_l$ :

$$\widehat{g}_{s,n} = \prod_{(i,j)\in\mathscr{R}_{s,n}} \widehat{h}_j.$$
(11)

Let  $\mathscr{R}_{s,n}^{i}$  denote the subpath of  $\mathscr{R}_{s,n}$  from source S to the intermediate node *i* and  $\overline{\mathscr{R}}_{s,n}^{i}$  denote the subpath of  $\mathscr{R}_{s,n}$ from the intermediate node *i* to the destination node of  $\mathscr{R}_{s,n}$ . The estimated packet delivery ratio of subpath  $\mathscr{R}_{s,n}^{i}$  can be computed using (10):

$$\widehat{g}_{s,n}^{i} = \prod_{(i,j)\in\mathscr{R}_{s,n}^{i}} \widehat{h}_{j}.$$
(12)

The covariance  $\phi_{s,n}^i$  is similar given by

$$\phi_{s,n}^{i} = \prod_{(i,j)\in\mathcal{R}_{s,n}^{i}} \left( \nu_{j}^{2} + \widehat{h}_{j}^{2} \right) - \left( \widehat{g}_{s,n}^{i} \right)^{2}.$$
 (13)

3.2. Leaky-Path Flow Model. Due to misbehaviors at nodes along the path, the effective rate is potentially reduced at each intermediate receiving node since data packets are lost. At a link (i, j) in the routing path  $\mathcal{R}_{s,n}$  with transmission source rate  $x_{s,n}$ , data is only received correctly on  $\hat{g}_{s,n}^i x_{s,n}$ . We define the goodput  $x'_{s,n}$  of a flow as the effective data rate received successfully at its destination node [13]. For a flow from source *s* traversing multiple hops, the goodput received at the destination node is given by

$$x_{s,n}' = \widehat{g}_{s,n} x_{s,n},\tag{14}$$

where  $x_{s,n}$  is the transmission rate at the source and  $\mathcal{R}_{s,n}$  is the set of links along the route. It can be seen that the data

rate of a flow declines every hop along its routing path, and it is in this sense that we call it a leaky-path flow.

To define a set of constraints for the multipath rate allocation problem, we must consider the resource constraints and the reduction of data flow due to misbehaviors at intermediate nodes. The resource constraint in necessary conditions of network utility maximization was that the average data rate should be no more than average capacity of each link. We next generate the stochastic constraint through incorporating the fault statistics into the link capacity constraint. For a communication network under probabilistic misbehaviors, the data flow rate is reduced along each path with increased the hops from source s. Hence, if the data flow rate at the source s is chosen without considering the packet loss by misbehaviors, the actual aggregate rate  $\sum_{Q_s} x_{s,n}$  may not be tightly bounded by the average capacity, where  $Q_s = s \in$  $S((i, j)) \land \mathscr{R}_{s,n} \in \mathscr{R}_s \land (i, j) \in \mathscr{R}_{s,n}$ . Thus at the node *i* of path  $\mathscr{R}_{s,n}^{i}$ , the goodput is given by  $g_{s,n}^{i} x_{s,n}$ . The stochastic constraint is thus imposed by the capacity constraint on the total traffic traversing a link (i, j) which can be given as follows:

$$\sum_{Q_s} g_{s,n}^i x_{s,n} \le c_{(i,j)}.$$
(15)

In order to compensate for the randomness in (15), we use the expected value and variance to replace the packet delivery ratio  $g_{s,n}^i$ . The mean  $\hat{g}_{s,n}^i$  and variance  $\phi_{s,n}^i$  of  $g_{s,n}^i$  can be computed using (12) and (13), respectively. We replace  $g_{s,n}^i$  with the statistic value  $\hat{g}_{s,n}^i + \delta \phi_{s,n}^i$ , where constant  $\delta \ge 0$ . The link constraint can be expresses by

$$\sum_{Q_s} \left( \widehat{g}_{s,n}^i + \delta \phi_{s,n}^i \right) x_{s,n} \le c_{(i,j)}.$$
(16)

A principal objective in optimal flow control problem formulation is to maximize the overall effective network utility of all flows from different sources:

 $\max \sum_{s \in S} \left( U_s \left( \sum_{n=1}^{k_s} \widehat{g}_{s,n} x_{s,n} \right) \right)$ (17)

or

$$\max \sum_{s \in S} \left( U_s \left( \sum_{n=1}^{k_s} x'_{s,n} \right) \right), \tag{18}$$

where  $U_s(x_s)$  is the associated utility as a measure of performance (or equivalently QoS).

## 4. Fault-Aware Utility Flow Control with Multipath Routing

4.1. Utility Framework for Fair Flow Control. Even though the optimal flow control approach has made a success in dealing with resource allocation, it also processes serious limitations when different types of traffic exist in the network. If each source selects different utility functions with different QoS requirements, OFC may cause utility unfairness among contending users for practical use. Since the source with high demand may receive a low resource, this results in applications receiving low utility.

In big-data communication networks, sources with different traffic types offer various valuable information regarding the environment. In order to support numerous applications with different utility demands, the flow control strategy should have the ability to allocate traffic rates properly in order to balance the performance for different applications. When considering different QoS requirements of heterogeneous sources, it can not meet the practical demand to allocate source rate simply in terms of conventional fairness criteria. Therefore, we design a utility framework of fair flow control, which allocates source rate according to the different QoS utilities.

In this framework, each source *s* attains a utility  $U_s(x_s)$ , where  $x_s$  is the source rate. The utility function  $U_s(\cdot)$  is assumed to be continuous, strictly increasing, and bounded in the interval  $[m_s, M_s]$ . We define a "pseudo utility"  $u_s(x_s)$ as  $u_s(x_s) = \int_{m_s}^{x_s} 1/U_s(y)dy$ . The goal is to maximize the sum of the pseudo utility

Problem: max 
$$\sum_{s \in S} \left( \int_{m_s}^{\sum_{n=1}^{s}} \frac{1}{U_s(y)} dy \right)$$
  
s.t.: 
$$\sum_{Q_s} x_{s,n} \le c_{(i,j)}$$
$$m_s \le \sum_{n=1}^{k_s} x_{s,n} \le M_s.$$
(19)

We generalize the OFC approach to obtain new problem formulations, namely, utility optimal flow control (UFC), which replace the conventional utility function with pseudo utility  $u_s(x_s)$ .

The demand for different QoS utilities also motivates a new concept of the utility max-min fairness [14].

Definition 1. A source rate allocation  $\mathbf{X}^* = [x_1^*, x_2^*, \dots, x_S^*]^T$  is utility max-min fair, if it is feasible and for each source *s*, the utility  $U_s(x_s^*)$  cannot be increased while maintaining feasibility, without decreasing the utility  $U_{s'}(x_{s'}^*)$  for some source *s'* with a lower utility  $U_{s'}(x_{s'}^*) \leq U_s(x_s^*)$ .

The definition shows that we should design rate control protocols that try to achieve fairness in terms of utilities, rather than fairness in terms of rates. For heterogeneous sources, the utilities, rather than source rates, are meaningful metrics of QoS for the applications.

To apply the UFC in fault-aware wireless networks, one needs to specify the resource constraints as in (19). Due to the faulty nodes existence on the routing path, the traffic rate is potentially decreased at each receiver as faulty nodes are lossy. Then the UFC operates over faulty links as follows: at each link, the link resource constraint is calculated as in (19), but using the total actual received rate at the link, not the sum of the original rates; and the source node updates the flow rate according to the feedback parameter of resource constraints along its route. This straightforward application of the UFC framework takes account of the faulty links, but only in the way the feedback parameters are computed. The lossy nature of the routing path is not considered in the objective function in the UFC problem itself. In the following section, we will propose the fault-aware utility flow control algorithm, which takes account of the lossy nature of the faulty paths in the objective function and constraints, to achieve lossy utility-based fairness for heterogeneous sources and study the properties in detail.

4.2. Fault-Aware Utility Flow Control Algorithm with Multiple Paths. Since the optimization framework of utility flow control is primarily developed for fault-free network environments, it cannot be directly applied to adversarial environments. In order to guarantee the network performance in the presence of misbehaving nodes, we provide the lossy optimization framework of utility flow control based on leaky-path model. The objective in this problem formulation is to maximize the overall pseudo utility of all effective flows, subject to the link capacity including expected packet loss due to misbehaviors. Then we have the following optimization problem:

Problem: max 
$$\sum_{s \in S} \left( \int_{m_s}^{\sum_{n=1}^{k_s} \hat{g}_{s,n} x_{s,n}} \frac{1}{U_s(y)} dy \right)$$
  
s.t.: 
$$\sum_{Q_s} \left( \hat{g}_{s,n}^i + \delta \phi_{s,n}^i \right) x_{s,n} \le c_{(i,j)} \qquad (20)$$
$$m_s \le \sum_{n=1}^{k_s} x_{s,n} \le M_s.$$

The Lagrangian function can be defined as

$$L\left(\widetilde{X},\lambda,\underline{\lambda},\overline{\lambda}\right) = \sum_{s\in S} \left( \int_{m_s}^{\sum_{n=1}^{k_s} \widehat{g}_{s,n} x_{s,n}} \frac{1}{U_s\left(y\right)} dy + \overline{\lambda} \left( M_s - \sum_{n=1}^{k_s} x_{s,n} \right) - \underline{\lambda} \left( m_s - \sum_{n=1}^{k_s} x_{s,n} \right) \right)$$
(21)
$$- \sum_{(i,j)} \lambda_{(i,j)} \left( \sum_{Q_s} \left( \widehat{g}_{s,n}^i + \delta \phi_{s,n}^i \right) x_{s,n} - c_{(i,j)} \right).$$

Here,  $\overline{\lambda} = [\overline{\lambda}_1, \dots, \overline{\lambda}_s]^T$ ,  $\underline{\lambda} = [\underline{\lambda}_1, \dots, \underline{\lambda}_s]^T$ ,  $\lambda = [\lambda_1, \dots, \lambda_L]^T$ , and  $u = (\overline{\lambda}, \underline{\lambda}, \lambda)$  are all nonnegative. The objective function of the dual problem is given by

$$D\left(\lambda,\overline{\lambda},\underline{\lambda}\right) = \max_{\{\overline{x}\}} L\left(\overline{x},\lambda,\overline{\lambda},\underline{\lambda}\right).$$
(22)

In terms of the Arrow-Hurwicz gradient method [15], we can obtain

$$\begin{aligned} x_{s,n}\left(t+1\right) &= \left[x_{s,n}\left(t\right) + \gamma \left(\frac{1}{U_s\left(\sum_{n=1}^{k_s}\widehat{g}_{s,n}x_{s,n}\left(t\right)\right)} + \overline{\lambda}_s\left(t\right) - \underline{\lambda}_s\left(t\right) - \lambda_{s,n}^r\left(t\right)\right)\right]^+, \end{aligned} \tag{23}$$

where  $\gamma$  is a small step size and  $\lambda_{s,n}^{r}(t)$  is the path price, which is composed of the link prices  $\lambda_{(i,j)}(t)$  along the particular route. Then the objective function of the dual problem is then

$$\min_{\{\lambda,\overline{\lambda},\underline{\lambda}\}} D\left(\lambda,\overline{\lambda},\underline{\lambda}\right).$$
(24)

The Lagrangian multipliers for the dual can be computed by the gradient method, as follows:

$$\lambda_{i,j}(t+1) = \left[\lambda_{i,j}(t) + \gamma \left(\sum_{Q_s} \left(\widehat{g}_{s,n}^i + \delta \phi_{s,n}^i\right) x_{s,n}(t) - c_{(i,j)}\right)\right]^+, \quad (25)$$

$$\overline{\lambda}_{s}(t+1) = \left[\overline{\lambda}_{s}(t) + \gamma \left(M_{s} - \sum_{n=1}^{k_{s}} x_{s,n}(t)\right)\right]^{T}, \qquad (26)$$

$$\underline{\lambda}_{s}(t+1) = \left[\underline{\lambda}_{s}(t) - \gamma \left(m_{s} - \sum_{n=1}^{k_{s}} x_{s,n}(t)\right)\right]^{+}.$$
(27)

We present our design of distributed algorithm based on proximal optimization steps for solving the utility max-min fair flow control with multiple paths problem. The FUFC algorithm for heterogeneous sources with multiple routing paths can be summarized in Algorithm 1.

For each source *s* with multiple paths, the property of updating formulations can easily lead to the oscillations in the Lagrangian algorithm. Since this kind of oscillation is detrimental to network control, we introduce an augmented variable  $f_{s,n}$  to solve the oscillation problem. The following modified objective function is used to replace the objective function of formulation (20):

$$\max \sum_{s \in S} \left( \int_{m_s}^{\sum_{n=1}^{k_s} \hat{g}_{s,n} x_{s,n}} \frac{1}{U_s(y)} dy \right) - \sum_{s \in S} \sum_{n=1}^{k_s} \frac{1}{2} \left( x_{s,n} - f_{s,n} \right)^2.$$
(28)

Denoting  $x_{s,n}^*$  as the optimal value of (20), the optimal value of the utility maximization problem with objective function (28) is  $x_{s,n} = x_{s,n}^*$ ,  $f_{s,n} = f_{s,n}^*$ . Therefore, (23) is slightly modified by applying the new objective function:

$$\begin{aligned} x_{s,n}\left(t+1\right) &= \left[ \left(1-\gamma\right) x_{s,n}\left(t\right) + \gamma f_{s,n}\left(t\right) \\ &+ \gamma \left(\frac{1}{U_s\left(\sum_{n=1}^{k_s} \hat{g}_{s,n} x_{s,n}\left(t\right)\right)} + \overline{\lambda}_s\left(t\right) - \underline{\lambda}_s\left(t\right) \\ &- \lambda_{s,n}^r\left(t\right) \right) \right]^+, \end{aligned}$$
(29)  
$$\left. - \lambda_{s,n}^r\left(t\right) \right) \right]^+,$$
$$f_{s,n}\left(t+1\right) &= \left(1-\gamma\right) f_{s,n}\left(t\right) + \gamma x_{s,n}\left(t\right). \end{aligned}$$

(i) Link (*i*, *j*)'s algorithm
At each time *t* = 1, 2, ..., each link (*i*, *j*):

(1) Aggregates flow rates *x<sub>s,n</sub>*(*t*) for all paths *R<sub>s,n</sub>* that contain link (*i*, *j*);
(2) Computes a new link price by formula (25);
(3) Communicates the new price λ<sub>(i,j)</sub>(*t* + 1) to all sources whose paths *R<sub>s,n</sub>* contain link (*i*, *j*).

(ii) Source *s*'s algorithm
At each time *t* = 1, 2, ..., each source *s*:

(1) Receives from the network the path prices
λ<sup>r</sup><sub>(i,j)</sub>(*t*)
(\*)
for all its paths *R<sub>s,n</sub>*, *n* = 1,..., *k<sub>s</sub>*;
(2) Updates the path rate *x<sub>s,n</sub>*(*t* + 1) using formula (23) and source rate *x<sub>s</sub>*(*t* + 1) = ∑<sup>k<sub>s</sub></sup><sub>*n*=1</sub> *x<sub>s,n</sub>*(*t* + 1);
(3) Communicates the new flow rate *x<sub>s,n</sub>*(*t* + 1) to all the links which are contained in path *R<sub>s,n</sub>*.

ALGORITHM 1: Fault-aware utility flow control FUFC algorithm.

4.3. Lossy Utility Max-Min Fairness. Based on the assumption of nonadversarial environments, each node in the network is well-behaved and  $h_i = 1$ . Our distributed algorithm with  $h_i = 1$  can allocate rates to achieve the utility max-min fairness among sources. The path rate algorithm of (23) simplifies to

$$x_{s,n}(t+1) = \left[ x_{s,n}(t) + \gamma \left( \frac{1}{U_s \left( \sum_{n=1}^{k_s} x_{s,n}(t) \right)} - \lambda_{s,n}^r(t) \right) \right]^+.$$
(30)

We can obtain that  $1/U_s(\sum_{n=1}^{k_s} x_{s,n}(t)) = \lambda_{s,n}^r(t)$  or  $x_{s,n}(t+1) = 0$  at convergence. In steady state, nodes attain a normal utility  $U_s^* = 1/\lambda_s^{r^*}$ . Let  $S_\lambda$  denote the set of nodes which have at least one path rate by the link price  $\lambda$ . Let us first consider the highest link price  $\lambda_0$ ; all the sources  $s \in S_{\lambda_0}$  get the smallest utility  $U_s = 1/\lambda_0$ . They are feasible and no source utility can be increased without decreasing another source utility that has the maximum price  $\lambda_0$ . So for these flows with price  $\lambda_0$ , they are utility max-min fair.

Then we consider the second highest link price  $\lambda_1$ . All the sources  $s \in S_{\lambda_1}$  attain the same utility  $U_s = 1/\lambda_1$ . No source utility can be increased without decreasing another source utility of  $s' \in S_{\lambda_0} \cup S_{\lambda_1}$  having a lower utility  $U_s < U_{s'}$ . All other flows traversing this link will be assigned a price of  $\lambda_1$  and equally share the remaining utility, which is also a utility max-min fair allocation.

Let us keep selecting all the link prices in the order  $\lambda_0$ ,  $\lambda_1, \ldots, \lambda_{k-1}, \lambda_k$ ; it is concluded that the algorithm with  $h_i = 0$  allocates source rate in utility max-min fair manner and that the global fairness is achieved.

When h = 1, the source rate in our algorithm can achieve utility max-min fairness, while the source rate can achieve lossy utility max-min fairness with h < 1. The following corollary establishes that utility max-min fair solutions also have the convergence property as loss ratios tend to zero.

**Corollary 2.** As the node fault ratio drop to zero:  $\lim_{k\to\infty} \min_{(i,j)\in R_{s,n}}(h_j)^k = 1$ , lossy utility max-min fair solutions converge to the lossless utility max-min fair solution.

The continuity of solutions can be proved using standard techniques in convergence analysis of Pompeiu-Hausdorff distance [13]. For the sake of limited space, we omit the proof here.

With the rapid process of Internet of Things and smart cities, the nature of the network is gradually evolving heterogeneously. There are various types of nodes, such as camera, robots, and mobile entities, in distributed heterogeneous systems. Our approach caters for a variety of service performance metrics related to heterogeneous sources. The network performance and QoS requirements are guaranteed through providing both effective throughput and fairness among various sources. We show the numerical results of our proposed algorithm in the following section.

#### 5. Performance Evaluations

In this section, we evaluate through simulations the performance of our proposed rate control algorithm with multiple routing paths in two case studies. In the first case, we apply our flow control algorithm to a specific multipath communication network and demonstrate the dynamics of behaviors. We use numerical examples to illustrate the advantage of the FUFC over the UFC approach without considering the impact of faulty nodes. In the second case, we extend the scale of network topology in order to observe the performance trends and shows the convergence of utility fair flow control solutions established in Section 4.

We consider two network cases with four heterogeneous sources  $S_1$ ,  $S_2$ ,  $S_3$ , and  $S_4$  which support multiple services with different QoS requirements. Therefore, we set utility functions consisting of heterogeneous traffic. The utility function of each source node with source rate  $x_i$  is given as  $U_1(x_1) = 1/(1 + e^{-2(x_1-6)})$ ,  $U_2(x_2) = \log(x_2 + 1)/\log 11$ ,  $U_3(x_3) = 1/(1 + e^{-2(x_4+4)})$ , and  $U_4(x_4) = 0.1x_3$ . The linear utility function represents that the satisfaction of an application increases linearly. The logarithmic utility function corresponds to the real-time application which the sigmoidal function approximates.

TABLE 1: Parameter values in simulations.

Parameter	Value
Link capacity	$c_l, c_2, c_3, c_4 = 4, 6, 8, 10 \text{ Mbps}$
Maximum data rate	$M_s = 10 \text{ Mbps}$
Minimum data rate	$m_s = 0$ Mbps
Step size	$\gamma = 0.1$
Update time interval	T = 0.05  s
Update relay time interval	$T_s = 0.2  \mathrm{s}$
Simulation steps	1000



FIGURE 2: The network topology of Case 1.

Each fault parameter  $h_j$  is modeled as an independent beta random variable with parameters  $(\delta_j, \beta_j)$  as  $h_j = \delta_j/(\delta_j + \beta_j)$ . For example,  $h_C = 0.9$  has corresponding parameters  $\delta_C = 39.6$  and  $\beta_C = 4.4$ . Other simulation parameters are summarized in Table 1.

5.1. Case 1. In this case, we show how our FUFC protocol can provide effective flow control with the existence of misbehaving nodes. The proposed FUFC protocol is benchmarked against the standard utility flow control (UFC) protocol [12]. Figure 2 depicts the topology of the network with 7 links, 6 nodes, and four sources  $S_1, S_2, S_3$ , and  $S_4$ .  $S_1$  routes its flow along two paths  $(A \rightarrow C \rightarrow B)$  with path rate  $x_{1,1}$ , and  $(A \rightarrow D \rightarrow B)$  with path rate  $x_{1,2}$ .  $S_2$  routes its flow along two paths,  $(A \rightarrow D \rightarrow B \rightarrow F)$  with path rate  $x_{2,1}$ , and  $(A \rightarrow E \rightarrow B \rightarrow F)$  with path rate  $x_{3,1}$ , and  $(A \rightarrow C \rightarrow B)$  with path rate  $x_{3,2}$ .  $S_4$  routes its flow along a single path  $(B \rightarrow F)$  with path rate  $x_{4,1}$ .

We denote that x is the data rate of one flow at the source node, and x' as the goodput at the destination node. Note the time scale in all the relevant figures is in terms of number of iterations. In the UFC approach, we use the algorithm in Problem (19) calculated based on the flow rate on each link and link price on each path. Figure 3 shows the utility of flow rates x at four source nodes using the UFC approach. Two utilities  $U_1$  of  $x_1$  and  $U_3$  of  $x_3$  converge to 0.9876, while  $U_2$  of  $x_2$  and  $U_4$  of  $x_4$  converge to 0.6381. Without considering the effect of faulty links, the algorithm computes  $U_1$  and  $U_3$  to share the bottleneck resource with an equal utility. The UFC approach provides a utility max-min fair resource allocation in which  $U_1$  is equal to  $U_3$ , and  $U_2$  is equal to  $U_4$  of their source rates x.



FIGURE 3: The utility of flow rates at four source nodes.



FIGURE 4: The effective utility in UFC.

In fact, the effective utilities of four flows cannot maintain the utility fairness at their destination node after traveling along the leaky-paths. The effective utilities of goodput for four sources in the UFC approach are depicted in Figure 4. The effective utilities decrease to 0.9099, 0.5756, 0.8075, and 0.6023 among four sources. For FUFC, the effective rates in Algorithm 1 are shown in Figure 5. It can be seen that FUFC yields higher effective utilities (0.987, 0.6381, 0.9883, and 0.6381) for four sources than UFC. We take a closer look at utility allocation among flows and effective flows in Figures 4 and 5. In Figure 3, four flows share a max-min fair utility allocation of source rate that  $U_1$  of  $x_1$  is equal to  $U_3$  of  $x_3$ , and  $U_2$  of  $x_2$  is equal to  $U_4$  of  $x_4$ . However, the utility fairness is broken due to different faulty effects on four paths by faulty links.  $U_3$  of  $x'_3$  and  $U_2$  of  $x'_2$  are lower than  $U_1$  of  $x'_1$  and  $U_4$  of  $x'_4$ , respectively, in Figure 4. In Figure 5, the effective utilities  $U_1$  of  $x'_1$  and  $U_3$  of  $x'_3$  in FUFC are closer to each other than





those in the UFC approach. The same situation happens in  $U_2$  of  $x'_2$  and  $U_4$  of  $x'_4$ . It demonstrates that better utility fairness is attained among effective flow rates by FUFC.

Figures 6 and 7 report the goodput at the destination node of UFC and FUFC, respectively. It can be seen that FUFC yields higher effective rates (6.185, 3.619, 8.196, and 6.381) for flows than UFC with goodput (5.156, 2.976, 6.717, and 6.023). This is because in our algorithm, multiple source nodes allocate traffic across multiple routing paths adaptively to compensate for faulty nodes, whose effects on throughput are taken into account in utility functions and constraints. Thus the network performance in presence of faulty nodes is improved through higher effective utility, higher effective throughput, and better utility fairness among effective flows by our algorithm FUFC.

*5.2. Case 2.* We investigate the performance while increasing *k* faulty links from 1 to 8 between *A* and *C*, *A* and *D*, *A* and



FIGURE 7: The goodput in FUFC.



FIGURE 8: The network topology of Case 2.

*E*, and *B* and *F* in the network of Case 1. Consider a wireless network given in Figure 8 where each flow travels multiple hops.

With an increasing number of links, the equilibrium utilities  $U_2$  and  $U_4$  of effective flow over the above paths of four sources for both UFC and FUFC are plotted in Figure 9. As the number of links increases, the effective utilities of goodput in both UFC and FUFC decline. Clearly, the effective utility of FUFC can be significantly higher than that of UFC. Meanwhile, the effective utilities of the flows in FUFC are closer to each other than those in the UFC approach, indicating that better fairness among effective utilities is achieved by FUFC. The gain of FUFC over UFC increases as the number of hops increases. Each source increases its flow rate adaptively to compensate for the higher data loss as the number of hops increases.

We can see from Figure 10 that, with decreasing the number of faulty links, the rate allocation is convergent to the rate allocation in wireless lossless condition. As discussed in Section 4, the rate region in our algorithm converges to the rate region in the corresponding lossless network while a sequence of link loss rate converges to zero (the number of faulty links converges to zero). The lossy utility max-min fairness can be achieved in our algorithm and converges to the corresponding lossless fairness with a sequence of loss



FIGURE 9: The effective utilities  $U_2$  and  $U_4$  in UFC and FUFC.



FIGURE 10: The trend of rate allocation.

rates converging to 0 in Figure 11. Figures 10 and 11 show the trends of rate region and utility fairness of four sources.

## 6. Related Work

There has been much work on resource allocation approaches for providing reliable transmissions (see, e.g., [16–18]). Some of these approaches are obtained as distributed solutions to an optimization problem first motivated by Kelly et al. in [11], with setting fixed reliability constraints. Saad et al. focus on effective rate allocation by maximizing the network utility with quality-of-service (QoS) constraints [18]. Hosseinabadi and Vaidya allocate data rates using a cross-layer approach



with the presence of misbehavior nodes [16]. To ensure secure communication, [17] formulate resource allocation as an optimization problem considering QoS metrics and artificial noises. Their work, however, is unable to adjust the effective rate and fairness adaptively in terms of the actual receiveresource at destination nodes. In our work, we define effective utility function associated with the effective rate at receivers and make the fairness objectives involve in optimization problem. Thus, our flow control approach could maintain an acceptable level of network performance degradation through getting better fairness and more effective utility in the presence of misbehaving nodes.

Existing techniques for secure communication under misbehaving nodes provide methods for reaction to misbehaviors by classifying each receiving node as either faulty or regular. For example, the authors of [19] provide a technique to divide the network links into reliable and unreliable ones and route around the region of the network being faulty, and the authors of [20] propose an approach to detect misbehaving nodes and perform coordinated channelhopping. However, the state of being faulty at each node is uncertain under random attacks, smart attacks, or stochastic software/hardware failures. Our approach incorporates the impact of potential dynamic faults into the traffic allocation and routing protocol and provides sufficient protection from stationary failures, mobile interferences, and the uncertain losses from the various environments.

Rate control stack design has been studied for the Internet in the 90s. Recently, rate control mechanisms for wireless networks are studied in [21–23]. The basic idea is that each application attains concave utility function and, thus, is appropriate only for homogeneous traffic. Further, Lee et al. [24] show that instability may be caused by heterogeneous traffic without appropriate rate controllers. Wang et al. [12] have provided a rate control framework that is able to deal with various types of traffic, such that the resulting utility is proportional fair. All these results are based on the assumption of nonadversarial environments where each wireless node is cooperative and well-behaved.

#### 7. Conclusion

In this paper, we studied the problem of traffic allocation across multiple routing paths for heterogeneous data sources in the presence of misbehaving nodes whose effects can be characterized statistically. We have presented methods for each network node to estimate the impact of misbehaving nodes and for data sources to these estimates into our traffic allocation and routing algorithm. We formulated multiplepath traffic allocation as a lossy network flow optimization problem based on leaky-path model. In order to handle heterogeneous traffic, we extended the concept of solving the lossy network flow optimization problem which maximizes effective relaxed utility function and proposed a FUFC algorithm to allocate the effective rate in lossy utility fair manner. We showed that considerable gains in effective network utility and utility fairness among heterogeneous sources are achieved by the FUFC approach.

#### **Conflicts of Interest**

The authors declare that there are no conflicts of interest regarding the publication of this paper.

### Acknowledgments

This work was supported by the Program of Shanghai Shentong Metro Group Co., Ltd., "The Research on Safety Control and Detection Devices for Centralized Shielding Doors"(Grant no. JS-KY13R036-2).

#### References

- C. Yang, C. Liu, X. Zhang, S. Nepal, and J. Chen, "A time efficient approach for detecting errors in big sensor data on cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 329–339, 2015.
- [2] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, 2016.
- [3] R. He, H. Rutagemwa, and X. Shen, "Differentiated reliable routing in hybrid vehicular ad-hoc networks," in *Proceedings* of the IEEE International Conference on Communications, (ICC '08), pp. 2353–2358, Beijing, China, May 2008.
- [4] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 16–30, 2015.
- [5] J. M. Gormally and R. L. Richards, "Application layer protocols for disruption tolerant remote sensor SATCOM links," in *Proceedings of the 33rd Annual IEEE Military Communications*

*Conference*, (*MILCOM '14*), pp. 975–982, Baltimore, MD, USA, October 2014.

- [6] A. Hava, Y. Ghamri-Doudane, G.-M. Muntean, and J. Murphy, "Increasing user perceived quality by selective load balancing of video traffic in wireless networks," *IEEE Transactions on Broadcasting*, vol. 61, no. 2, pp. 238–250, 2015.
- [7] L. Chen and J. Leneutre, "On multipath routing in multihop wireless networks: security, performance, and their tradeoff," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Article ID 946493, 2009.
- [8] W. Wang, M. Chatterjee, K. Kwiat, and Q. Li, "A game theoretic approach to detect and co-exist with malicious nodes in wireless networks," *Computer Networks*, vol. 71, pp. 63–83, 2014.
- [9] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, 2013.
- [10] V. Karyotis, S. Papavassiliou, and B. Maglaris, "Modeling framework for the study and analysis of mobile attack propagation in wireless ad-hoc networks," in *Proceedings of the 12th European Wireless Conference on Enabling Technologies for Wireless Multimedia Communications, European Wireless 2006*, Athens, Greece, April 2006.
- [11] F. P. Kelly, A. K. Maulloo, and D. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research Society*, vol. 49, no. 3, pp. 237–252, 1998.
- [12] W. H. Wang, M. Palaniswami, and S. H. Low, "Applicationoriented flow control: fundamentals, algorithms and fairness," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1282– 1291, 2006.
- [13] V. G. Subramanian, K. R. Duffy, and D. J. Leith, "Existence and uniqueness of fair rate allocations in lossy wireless networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3401–3406, 2009.
- [14] Z. Cao and E. W. Zegura, "Utility max-min: an applicationoriented bandwidth allocation scheme," in *Proceedings of the IEEE 18th Annual Joint Conference of Computer and Communications Societies (INFOCOM '99)*, vol. 2, pp. 793–801, NY, USA, March 1999.
- [15] K. J. Arrow, L. Hurwicz, and H. Uzawa, *Studies in Linear And Non-Linear Programming*, Stanford University Press, Palo Alto, Calif, USA, 1958.
- [16] G. Hosseinabadi and N. Vaidya, "Selfish misbehavior in scheduling algorithms of wireless networks," CRHC, University of Illinois at Urbana-Champaign, Albuquerque, NM, USA, http:// www.crhc.illinois.edu/wireless/papers/tech-report-Ghazale-SelfishCrossLayered-March.pdf.
- [17] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3528–3540, 2011.
- [18] M. Saad, A. Leon-Garcia, and W. Yu, "Optimal network rate allocation under end-to-end quality-of-service requirements," *IEEE Transactions on Network and Service Management*, vol. 4, no. 3, pp. 40–49, 2007.
- [19] M. H. Eiza, Q. Ni, T. Owens, and G. Min, "Investigation of routing reliability of vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, 2013.

- [20] G. Yan, S. Olariu, and M. C. Weigle, "Providing location security in vehicular Ad Hoc networks," *IEEE Wireless Communications*, vol. 16, no. 6, pp. 48–55, 2012.
- [21] M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, "Layering as optimization decomposition: a mathematical theory of network architectures," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 255–312, 2007.
- [22] Y. Xue, B. Li, and K. Nahrstedt, "Optimal resource allocation in wireless ad hoc networks: a price-based approach," *IEEE Transactions on Mobile Computing*, vol. 5, no. 4, pp. 347–364, 2007.
- [23] X. Zhang, X. Dong, N. Xiong, J. Wu, and X. Li, "Fault-aware flow control and multi-path routing in VANETs," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1090–1107, 2015.
- [24] J.-W. Lee, R. R. Mazumdar, and N. B. Shroff, "Non-convex optimization and rate control for multi-class services in the internet," *IEEE/ACM Transactions on Networking*, vol. 13, no. 4, pp. 827–840, 2005.





The Scientific World Journal





Applied Computational Intelligence and Soft Computing





Computer Networks and Communications



Submit your manuscripts at https://www.hindawi.com



Modelling & Simulation in Engineering





Advances in Computer Engineering

Robotics



International Journal of Computer Games Technology



Advances in Human-Computer Interaction





Computational ntelligence and Neuroscience









Journal of Electrical and Computer Engineering