Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 9394613, 22 pages
https://doi.org/10.1155/2017/9394613

Research Article

Fault Activity Aware Service Delivery in Wireless Sensor Networks for Smart Cities

Xiaomei Zhang,[1,2] Xiaolei Dong,[3] Jie Wu,[4] Zhenfu Cao,[3] and Chen Lyu[5]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*
[2]*College of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai, China*
[3]*Shanghai Key Laboratory for Trustworthy Computing, East China Normal University, Shanghai, China*
[4]*Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA*
[5]*School of Information Management and Engineering, Shanghai University of Finance and Economics, Shanghai, China*

Correspondence should be addressed to Xiaolei Dong; dongxiaolei@sei.ecnu.edu.cn

Received 10 April 2017; Revised 1 July 2017; Accepted 24 July 2017; Published 20 September 2017

Academic Editor: Damianos Gavalas

Wireless sensor networks (WSNs) are increasingly used in smart cities which involve multiple city services having quality of service (QoS) requirements. When misbehaving devices exist, the performance of current delivery protocols degrades significantly. Nonetheless, the majority of existing schemes either ignore the faulty behaviors' variability and time-variance in city environments or focus on homogeneous traffic for traditional data services (simple text messages) rather than city services (health care units, traffic monitors, and video surveillance). We consider the problem of fault-aware multiservice delivery, in which the network performs secure routing and rate control in terms of fault activity dynamic metric. To this end, we first design a distributed framework to estimate the fault activity information based on the effects of nondeterministic faulty behaviors and to incorporate these estimates into the service delivery. Then we present a fault activity geographic opportunistic routing (FAGOR) algorithm addressing a wide range of misbehaviors. We develop a leaky-hop model and design a fault activity rate-control algorithm for heterogeneous traffic to allocate resources, while guaranteeing utility fairness among multiple city services. Finally, we demonstrate the significant performance of our scheme in routing performance, effective utility, and utility fairness in the presence of misbehaving sensors through extensive simulations.

1. Introduction

Wireless sensor networks (WSNs) have been integrated with smart cities and play an important role in smart city by providing versatile applications through sensors. With the demands for living and security standard of a city, it has become necessary for WSNs to support a series of city services, such as health monitoring, electricity consumption, intelligent transportation, visual target tracking, and multicamera surveillance [1, 2]. Sensors that are randomly distributed in a network cooperate with each other to deliver service data via multihop routing and rate control to the sink, which can communicate with conventional networks, for instance, the Internet.

Built upon open wireless medium, multiple city services in WSNs are particularly vulnerable to attackers which are attracted by sensitive information, less infrastructure, privacy, and so forth. Many service delivery protocols have been proposed and evaluated for countering different types of misbehaving nodes [3, 4]; however, most studies largely ignored the uncertainties and variabilities in the city environment. It is not an easy job to characterize the dynamics of dynamic ongoing or unknown attacks in an intuitionist way. Moreover, recent works in [5, 6] have demonstrated that the attackers with fixed strategy cannot disguise themselves as members of a city and are then marked as the adversaries. Inconsistent behaviors may exist in an intelligent misbehaving sensor or adapt its strategy under random attacks in smart grids [7], stealthy attacks in WSN-based IoT [8], and dynamic ongoing attacks in smart cities [9]. Hence, the impact of misbehaving sensors is probabilistic and time-varying in many cases.

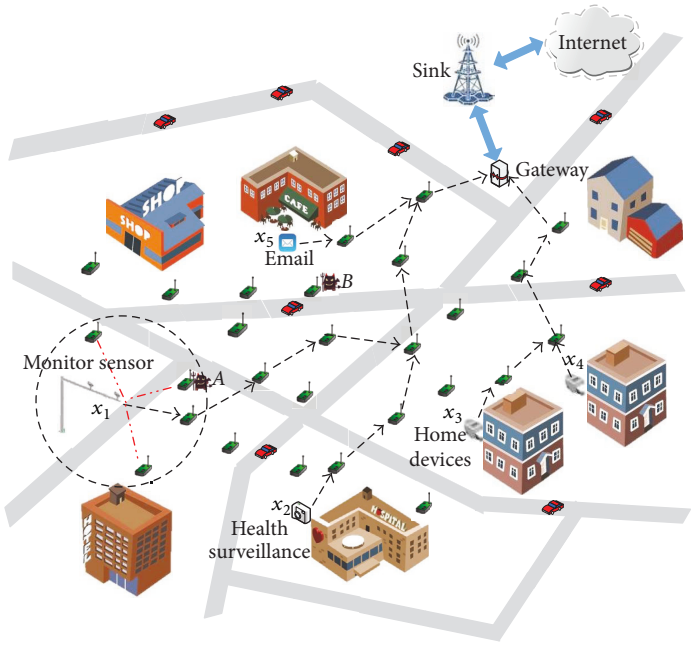


Figure 1: Multiservice delivery in a WSN of smart cities.

In order to characterize the effect of faulty behaviors on routing and throughput, we propose an impact collecting-based approach, which formulates the dynamics of faulty behaviors. A popular approach is to collect information about the direct impact of the misbehaviors, such as energy and delivery quality inside a sensor. Besides that, the delivery for city services is affected by some indirect impacts. For example, the vehicle misleads network routine and causes bandwidth consumption by announcing its various fake position simultaneously or the frequent time interval [10]. To defend against this type of misbehavior, a sensor needs to obtain trust verification from other sensors. The aim of our method is first to identify the state of a faulty sensor by, on direct impact and on indirect impact, gathering verification information received from its neighboring nodes. Then we model the state of being faulty at each sensor as a random process. Since the effect of faulty behaviors is probabilistic, the state of being faulty will also be nondeterministic and must be studied by applying a stochastic framework. Accordingly, we make each sensor establish novel metrics fault activity (FA) for modeling the stochastic state of being faulty in terms of statistical information about the probabilistic faulty nodes, which is also utilized to select next forwarding candidates for each hop and to allocate resource for each service.

Geographic opportunistic routing (GOR) is considered an effective and flexible way to improve network performance with the help of WSN localization and exploiting spatial diversity [11–14]. Moreover, GOR maintains high efficiency and scalability since each sensor only needs the local one-hop connectivity. In this paper, our FAGOR uses more candidates as backups and integrates fault activity model into the process of the forwarding candidate selection. For example, as shown in Figure 1, based on distance, energy, trust verification, and delivery quality inside a sensor, each sensor filter is prioritizing to choose a candidate sensor set of the neighbors. These candidates follow the priorities to deliver the packet opportunistically. Malicious sensors (node A and node B) have very low priorities or are even not included in the candidate set according to their direct impacts and indirect impacts.

Network service performance becomes lower when inside intrusions are present since the effective flow gets thinner when misbehaving nodes are on its routines [15, 16]. Therefore, it is necessary to apply rate-control design to complement secure routing and guarantee performance. A popular approach for reliable resource allocation is to design improved optimal flow control (OFC) algorithms, which solve network utility maximization (NUM) problems with constraints on fixed reliability requirements [17–19]. However, these approaches are unable to adopt their resource allocation and fairness dynamically according to the actual-receive rate of each service. We develop a FA-leaky-hop model in which each faulty sensor has potential effects on the resulting data throughput and incorporate the actual-receive rate at wireless hops into OFC approach.

Moreover, when multiple city services, for example, camera monitoring, health surveillance, email, and smart home, are run over a network as shown in Figure 1, the existing OFC approaches usually lead to a serious unfair resource allocation in terms of rates [20]. For example, real-time traffic which has its minimum required rate may get almost zero utility, despite nonzero rates. The utility function conditions of OFC need be relaxed to describe different services regarding heterogeneous traffic types. Based on FA-leaky-hop model, we formulate the problem of allocating rate among multiple services as a lossy flow optimization problem, namely, fault

activity utility OFC, through maximizing the sum of relaxed utilities subject to the network constraints. Considering the existence of faulty sensors, our FA-UOFC algorithm allocates traffic to various services and achieves fairness in terms of actual-receive utility, rather than that in terms of rate or utility. In particular, we define the utility fairness index which could measure the degree of fairness performance based on the achieved throughput in lossy networks and seek to gain its considerable value under our service delivery strategies.

In this article, we investigate multiple city service delivery of joint routing and rate-control that can minimize performance degradation in the event of misbehaving nodes. To the best of our knowledge, we are the first work to address both routing and rate-control for multiple services in WSNs via a fault-dynamic model-based approach. The main contributions of this paper are outlined as follows:

(i) We design a distributed framework of fault activity information at each sensor to locally characterize the impact of the nondeterministic and dynamic faulty behaviors and to incorporate fault activity information into data delivery for multiple city services.

(ii) We propose a fault activity-based geographic opportunistic routing protocol, FAGOR, which combines the direct and indirect impacts of faulty behaviors, to protect against a wide range of attacks.

(iii) We formulate the problem of allocating resources among multiple services in the presence of misbehaving nodes as a lossy flow optimization problem along leaky-hop model. A distributed algorithm, FA-UOFC, is developed to allocate the effective rate properly within the sensor networks and to achieve lossy utility fairness by sources with different traffic types.

(iv) We define a novel index, index of utility fairness, that quantitatively measure the degree of utility fairness among multiple city services in distributed systems.

The rest of the paper is organized as follows. Related work is described in Section 2. We depict our system model in Section 3, and we present methods that allow sensors to establish novel metrics fault activity (FA) according to the impact of misbehaviors in Section 4. In Section 5, we introduce the formulation of a GOR protocol based on FA metrics. In Section 6, we describe the leaky-hop model and formulate the optimal rate-control for multiple services in the presence of misbehaving nodes. The performance of our algorithm is evaluated in Section 7. Finally, we conclude the paper and give directions for future work in Section 8.

2. Related Work

Over the past few years, literatures investigated the multiple city service delivery over wireless networks. A resource management scheme is proposed in [21] to offer the delivery of various city services in the Internet of Things. Tang et al. [22] propose a cross-layer resource allocation model for guaranteeing the QoS requirements of elastic service (audio and video surveillance, habitat monitoring, and real-time traffic monitoring) based on the optimal achievable rate in Cloud Radio Access Network. Spachos et al. [23] design an energy-aware dynamic routing scheme to improve the QoS-aware routing of multimedia traffic by optimizing the selection of the forwarding candidate set. The feasibility of the schemes mentioned above does not consider the existence of malicious nodes, and there is no policy given to defend the misbehaviors of wireless nodes. There exist works that study particular misbehaviors of node-selfishness for multiservice delivery. Luo et al. [24] design an algorithm to select relay nodes in terms of residual energy metrics in WSN-based IoT. The "ground truth" status of each node in [25] is served as virtual credit to encourage data delivery according to its social and QoS behavior. The work in [26] presents a dynamic trust management for secure routing to deal with selfish behaviors and trust-related attacks. Our fault-aware routing and resource allocation scheme extends from these solutions with consideration given to a wider range of misbehaviors on the multiservice delivery in WSNs from the perspectives of both direct-impact factors and indirect impact factors.

Due to the misbehaving nodes' effect on network performance, various defense strategies dealing with the nodes' misbehaviors have been studied for wireless networks. However, most of these works only present countermeasure analysis for different types of faulty nodes and have not considered the uncertainties and dynamics of real environments. Most of the studies assume that the faulty nodes employ a constant strategy that will not change with time. In fact, a faulty node can adopt variable misbehaviors to maximize its intrusion strength [27]. Malicious nodes can be equipped with cognitive technology and can adapt their attacking strategy according to the legitimate users' actions [28]. The attackers decrease their attacks in frequency to disguise themselves and to avoid being detected [29]. Mitchell and Chen [30] characterize a malicious attacker by its capacity to perform random attacks. Similar to [30], our approach works against misbehaving behaviors which may exhibit inconsistent behaviors; a misbehaving node acts as a good node and does not launch attacks at first, in order to gain the trust of other nodes, or, it may perform on-off attacks with a random probability. Our work characterizes the impact of potential dynamic faults and incorporates statistical information into the resource allocation and routing protocols. This assumption not only provides efficient defense against stationary failures but also is suitable for mobile attacks and the uncertain losses from the various environments.

In the reliable routing of WSNs, geographic routing is an attractive approach since no end-to-end route is determined before data delivery [31]. A QoS-aware geographic opportunistic routing, QGOR, is explored in [14] for delivering packets with both time delay and reliability constraints in WSNs. Using location information, Wu et al. [32] design an efficient routing and load balancing algorithm in hybrid VANET. These studies, however, do not consider and respond to location-related attacks. Liu et al. [33] consider the use of the location verification such that neighbors exchange their location information to address a series of location-related attacks. One main limitation of this scheme is that

if the localization mechanism is separated from the routing protocol, the protocol will fail. FAGOR is similar to those schemes in terms of security requirements. FAGOR differs from them in that it uses RSS to detect location information and the verification from the other sensors to identify this type of misbehaviors with possibility.

An optimization problem is first applied to formulate the rate-control stack design of the wireline context by Kelly et al. [34]. This pioneering work was further advanced by studies in cellular wireless networks [35], ad hoc networks [36], and wireless sensor networks [37]. The fundamental assumption of the above research is that each application attains concave utility function and, thus, is only suitable for elastic traffic. It cannot deal with the resource allocation of multiple services in sensor networks where both elastic and inelastic traffic are commonly engaged. Lee et al. [38] show that instability and high network congestion may be caused by the mixing of inelastic and elastic traffic in the absence of appropriate rate controllers. Hande et al. [39] have further derived the sufficient and necessary conditions of system optimality in a mixed-traffic scenario and have proposed a link provisioning method which could potentially be used during the network-planning stage. Alternatively, Wang et al. [20] have developed a new rate-control framework that is able to deal with both elastic and inelastic traffic of multiple services such that the resulting utility is proportional fair. However, these works do not consider the existence of misbehaving nodes and assume that each wireless node is cooperative and well-behaved.

Recently, numerous protocols which maximize the sum of each application's utility by setting fixed reliability constraints have been proposed to allocate the resources of multiple services to provide reliable wireless transmissions [16]. Their works, however, are unable to adapt fairness dynamically in terms of the actual-receive resource of each application. Li et al. [19] incorporate rate, in addition to delay and reliability, into the utility function to support different QoS requirements of various traffic. In our paper, we take a similar approach that the utility is defined to be a function of effective utility received at destination nodes. By means of embodying QoS objectives in the extended utility function, our FA-UOFC is applicable for various services addressing their real utility requirements and improves the utility performance both of inelastic sources and elastic sources.

3. System Model and Assumptions

This section presents the network and the misbehaving-node model handled in this article, as well as the assumptions made in order to design the proposed architecture.

3.1. Network Model. In a smart city, a wireless sensor network involves tiny devices, called sensor nodes $\mathbf{V} = \{1, 2, \ldots, V\}$, which have ability to cater to different applications. These devices are randomly deployed in a city area with a constant size, for example, a smart community containing residential buildings, hospitals, schools, shopping malls, cafes, and banks. Two SNs within the wireless transmission range R can send data and communicate with each other, and any two nodes with a distance greater than R would require a multihop to communicate with each other. A link is denoted as a pair as nodes (i, j), where $i \in \mathbf{V}$ is the transmitter and $j \in \mathbf{V}$ is the receiver. The data collected by sensors is sent to sinks which process data locally or through core networks such as the Internet.

The location of sinks as data, computation, and control center are known in the network. Each sensor knows the geographic coordinate of itself using one of secure localization algorithms [40]. Meanwhile, a sensor can adapt its location information with the help of some trusted mobile anchor nodes in neighbor set, for example, vehicle nodes equipped with GPS.

Due to the broadcast nature of the wireless medium, the transmitters contend in wireless channel capacity for the shared wireless medium if they are within the interference range of each other. Considering the protocol model [41] for successful transmission, the interference among the transmissions is characterized by the interference sets. Since the transmitters included in the interference set share the same common channel capacity, only one of the sensors may transmit over a channel in a time slot. Moreover, since energy is a major concern in WSNs, we assume that sinks are powerful services for collecting data and that other sensors have limited and unreplaceable batteries. We build a power dissipation model to guarantee the operational lifetime of the sensor network in Section 6.

3.2. City Services. WSNs provide a variety of services to city users that will force networks to support heterogeneous traffic. More generally, utilities of multiple city services in a smart city can be categorized as follows in terms of performance goal perspectives [20]:

(i) Elastic utility for traditional data services such as file transfer, mail, and ftp

(ii) Inelastic utility including real-time utility, rate-adaptive utility, and stepwise utility such as video surveillance, real-time monitoring, and teleconferencing

Figure 1 illustrates an example network with five flows s_1 to s_5 of source rates x_1 to x_5, respectively. There are different types of sensors embedded to support city services with different QoS requirements. The utility types of source nodes are given as follows: inelastic utility for the first four source nodes and elastic utility for the fifth source node. Note that, in comparison with other data delivery for elastic traffic, the assumption of mixed traffic in our rate-control model is practical for many smart city applications, such as water consumption, electricity consumption, target tracking, health surveillance, and smart home appliance.

3.3. Fault Activity Information. In this article, we assume that the source nodes have no prior knowledge of the abnormal behaviors of nodes being performed. That is, we make no assumption about the malicious nodes' strategies, misbehaviors' goals, or mobility patterns. We assume that the types of misbehaviors, like failure of internal components or external faults, are unknown to the network.

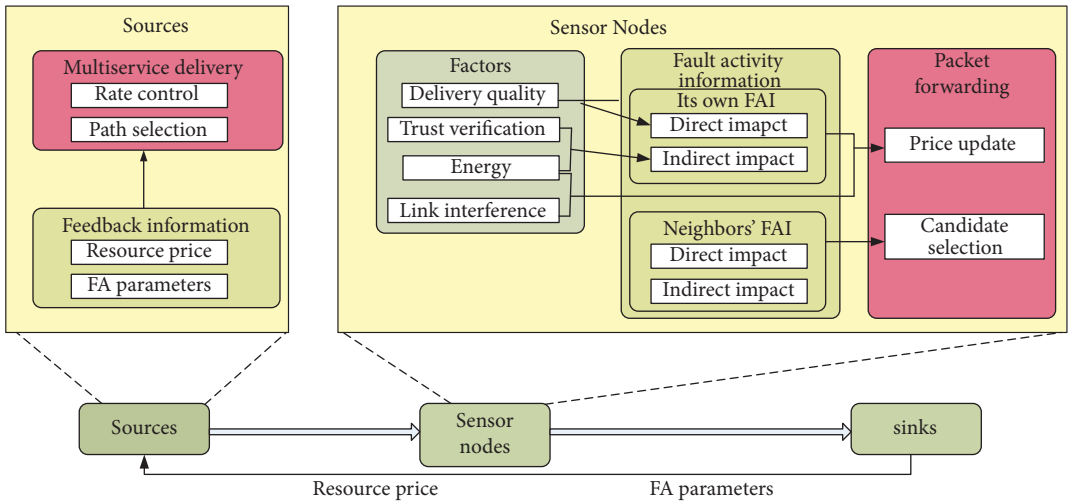


Figure 2: The delivery framework for multiple services based on the fault activity information.

In order to characterize the effect of nodes' misbehaviors on the multiservice delivery, each source must collect information on the impact of the misbehaviors in city parts of networks. However, due to the distributed characteristic of wireless sensor nodes, no central network entity collects the information on the misbehaviors' impact of all sensors and a fully distributed solution is required. Every source/SN should have its own fault activity information (FAI) for both its neighbors' and its own faulty behavior impact. The node FAI at each SN obtains the faulty activity impact of its neighbors and of itself in terms of direct and indirect impacts recommended by the SNs around it. Meanwhile, the direct and indirect impacts are affected by SNs' factors, that is, energy, trust verification, and delivery quality inside a sensor.

When sensor node i delivers multiservices to the sink via multihop communication, there are some candidates based on node i's knowledge of available forwarding neighbors. Nevertheless, since the node misbehaviors may degrade the reliability of the routing path, each hop selects the most reliable one of these candidates in terms of their FAI. Additionally, each sensor node tries to maximize the benefit by sending the feedback signal, the "resource price" determines the cost of consuming limited resources by competing services, to the source. Accordingly, each source is charged the resource price and is then allocated a certain amount of resources for delivering its service. For various types of services or applications, each source is associated with a utility function that reflects how much QoS benefit that source obtains at the allocated transmission rate. Here, the network model of the distributed framework of the candidate selection and rate allocation of the sources is shown in Figure 2.

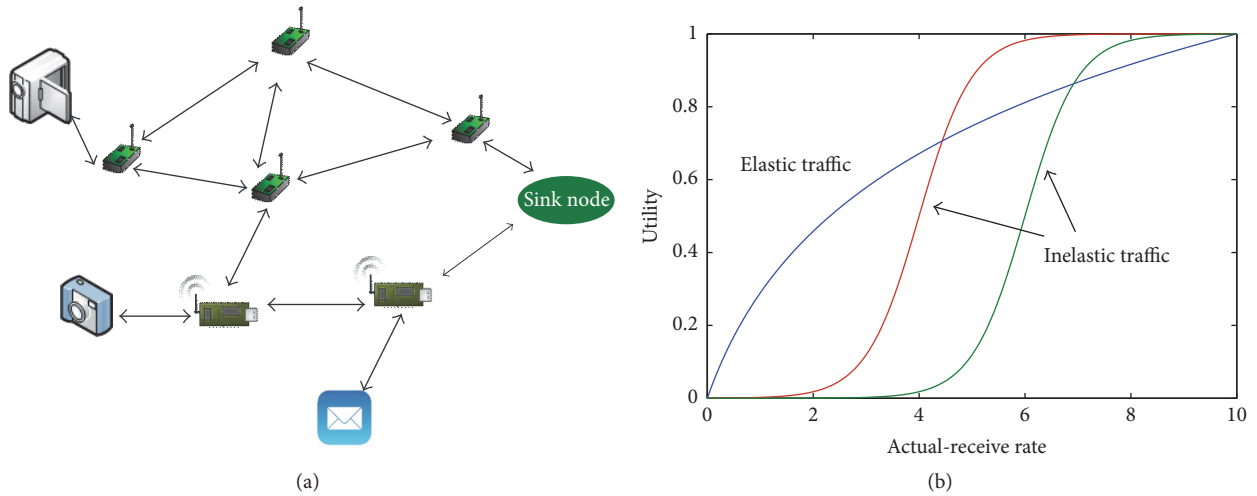
4. Characterizing the Impact of Faulty Activities

In this section, we propose techniques for sensor node estimation and characterization of the impact of faulty activities and for obtaining misbehavior information. Under the distributed framework of the fault activity information (FAI), the FAI of each sensor node consists of two parts: direct impact and indirect impact of misbehaviors on multiservice delivery. Based on FAI, we determine the node-faulty state and get the estimation of FA metric. Each relay sensor should incorporate its neighbors' estimates into its candidate selection for next-hop from its neighbor set. In order for a source node to incorporate the misbehavior impact in the rate-control problem, its own estimation of FA must be recorded in the data packets when the packets arrive at this intermediate sensor and be sent back to the source node when the packets arrive at the sinks.

4.1. Direct-Impact Model

4.1.1. Delivery Quality inside a Sensor. In a smart city, sensors with heterogeneous nature support and forward a mix of elastic and inelastic traffic. With the existence of misbehaving sensors along routing paths, the data rate of a flow gets thinner and thinner and the actual-receive rate at the sink is considerably lower than that at the source. Figure 3 shows the utility obtained by elastic and inelastic applications at different actual-receive rates. If an elastic service gets a rate slightly greater or lower than their minimum required rate, inelastic applications get zero utility. Therefore, the quality of delivery inside a sensor is a significant factor for utility of multiple services.

Although a faulty node may perform various behaviors, any good node exhibits the same behavior: delivering packets correctly. Similar to the approach in [42], we use the ratio of packets successfully delivered compared to those sent (packets may be corrupt even if received) in order to characterize the delivery quality inside a sensor. During a certain period $[t - T, t]$, each node (sender) enters the promiscuous mode and checks whether the packet is actually forwarded by its selected nodes. Additionally, it can record in the neighbor list the running average number $NR_i[t - T, t]$ of packets sent to node i and the running average number $NV_i[t - T, t]$ of valid



(a) (b)

Figure 3: Utility of elastic and inelastic services.

packets. Each sensor is aware of the delivery quality values of any node i and of its one-hop neighbors for the period $[t-T,t]$, denoted as $PR_i([t-T,t])$:

$$PR_i([t-T,t]) = \frac{NV_i[t-T,t]}{NR_i[t-T,t]}. \quad (1)$$

4.1.2. Energy. If some sensors malfunction due to the lack of energy, this degrades the overall network efficiency and performance. E_i is denoted as the remaining energy of node i. Let e_s, e_t, and e_r be the energy consumed in the sensing, transmitting, and receiving for one data packet per unit time.

$$E_i = \begin{cases} e_s + e_t & \text{if flow } s \text{ starts from node } i \\ e_t + e_r & s \in S(i) \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

In order to update the direct-impact metric, the location beacon of one-hop neighbors is extended to apply an additional field of remaining energy $E_i(t)$. We can use $PR_i([t-T,t])$ and E_i to update the estimate $DI(t)$ at the end of the time interval. In order to balance the stability and the accuracy of the estimation results, we update the estimation $DI(t)$ through iterations:

$$DI(t) = \kappa(\alpha DI(t-T) + (1-\alpha) PR_i([t-T,t])) + (1-\kappa) E_i(t), \quad (3)$$

where $0 < \alpha \leq 1$ is the parameter that controls the preference between current and historic samples and $0 < \kappa \leq 1$.

4.2. Indirect Impact Model

4.2.1. Trust Verification. In smart environments, the network also has one or more malicious users that control a number of malicious colluders. All colluders may cooperate with each other and turn their partner into an inside faulty node. During the initial stage or under a random attack strategy, these malicious nodes do not immediately launch packet dropping behaviors, and they modify their transmission power to disguise themselves. Hence, the impact of the disguised nodes' misbehavior is indirect on packet delivery from the perspective of the network, and a validation metric can be applied to distinguish malicious nodes with the voting-based scheme.

To keep consistency, we follow the assumption and variable definitions about GOR in [43]. Each node periodically broadcasts the location beacon with the location information to its one-hop neighbors. After receiving the beacon from node A, a neighbor B verifies the location information in terms of the received signal strength. RSS is given by the following [44]:

$$\text{RSS}_{AB}\ (\text{dBm}) = P_t - p_0 - 10\beta \lg\left[\frac{d_{AB}}{d_0}\right] + x, \quad (4)$$

where P_t is the node's transmission power in dBm and β is the path loss factor. Here, p_0 is the path loss at the reference distance d_0 and x is a random variable. However, if the RSS is susceptible, the above approach will lead to high false negatives against location-related attacks. Based on (4), the distance is estimated as $D_{AB} = d_{AB}(1 \pm \rho)$, where ρ is the measurement error. To reduce the effect of the disguised nodes, node A requires collecting more RSS value from the information of its common neighbors. We denote $\mathbf{H} = N^{(A)} \wedge N^{(B)} = \{H_1, H_2, \ldots, H_k\}$ as the intersection of A's neighbor set and B's neighbor set. A neighbor node R_j is selected by B to find the difference of the RSS value of the sender in H (e.g., node H_j). Even though the transmission power may be modified, the difference $R_{BR_j}^{H_j}$ is found to be constant [45]:

$$R_{BR_j}^{H_j} = \frac{\text{RSS}_{H_jB} - \text{RSS}_{H_jR_j}}{10\beta} = \lg\frac{d_{H_jR_j}}{d_{H_jB}}. \quad (5)$$

As either the node H_j or the chosen neighbor node R_j may use forged information of this distance value, $D_{H_jR_j}$ or

D_{H_jB} are used to replace the value of $d_{H_jR_j}$ and d_{H_jB}. We can get the inequality from (5):

$$\lg\frac{D_{H_jR_j}}{D_{H_jB}} + \lg\frac{1-\rho}{1+\rho} \le R_{BR_j}^{H_j} \le \lg\frac{D_{H_jR_j}}{D_{H_jB}} + \lg\frac{1+\rho}{1-\rho}. \quad (6)$$

Following this method, we can obtain $(R_{BR_j}^{H_1}, R_{BR_j}^{H_2}, \ldots, R_{BR_j}^{H_c})$ for other nodes in set **H**. In this round, two disguised nodes H_m and H_i are identified with R_j, provided that

$$R_{BR_j}^{H_i} + \lg\frac{1-\rho}{1+\rho} \le R_{BR_j}^{H_m} \le R_{BR_j}^{H_i} + \lg\frac{1+\rho}{1-\rho}. \quad (7)$$

With node B's neighbor nodes as reference nodes, each H_i belonging to H can be identified using this method. During the time period $[t-T, t]$, there are $q_i([t-T, t])$ disguised nodes that are faked by actually one node in a round and $f_{H_i}([t-T, t])$ rounds of the entire $m_{H_i}([t-T, t])$ rounds in the calculation. The estimate value $DS_{H_i}(t)$ of the possible disguiser H_i can be obtained by

$$\begin{aligned} DS_{H_i}(t) &= \gamma DS_{H_i}(t-T) \\ &\quad + (1-\gamma)\frac{1}{q_{H_i}([t-T,t])}\left(1 - \frac{f_{H_i}([t-T,t])}{m_{H_i}([t-T,t])}\right). \end{aligned} \quad (8)$$

An attacker can launch a spoofing attack by sending forged location beacons to attract SNs to choose one of them as the next-hop. In this paper, the FAI management makes use of the RSS to verify SNs' location and to address the location-related attacks by offering nodes the location with possibility. Based on the collected RSS values, we can compute the values $(R_{BH_1}^A, R_{BH_2}^A, \ldots, R_{BH_k}^A)$ for the set **H** whose size is k, where $R_{BH_i}^A = (\mathrm{RSS}_{AB} - \mathrm{RSS}_{AH_i})/10\beta = \lg(D_{AH_i}/D_{AB})$. Then the following inequality can be provided to decide whether node A is marked as a successful validation:

$$\lg\frac{d_{AH_i}}{d_{AB}} + \lg\frac{1-\rho}{1+\rho} \le R_{BH_i}^A \le \lg\frac{d_{AH_i}}{d_{AB}} + \lg\frac{1+\rho}{1-\rho}, \quad (9)$$

where d_{AH_i} and d_{AB} are the position announced in the received location beacon. If the inequality is satisfied, it means that node A with one neighbor $H_i \in \mathbf{H}$ can be marked as a successful validation, and $M_{H_i} = 1$. Otherwise, $M_{H_i} = 0$. We can obtain the ratio of successful validation of node A:

$$LC_A(t) = \frac{1}{k}\sum_{i=1}^{k} DS_{H_i}(t)\, M_{H_i}. \quad (10)$$

Furthermore, we introduce the indirect impact metric to address issues of location-related attacks. In order to gain the trust of other nodes, some malicious sensors claim themselves as legitimate nodes but transmit beacon messages containing false location information to confuse other sensors. Each network node may obtain the verification information of its candidates indirectly received from its neighboring nodes. Additionally, the impact of these disguised nodes' misbehavior which pollutes the network system with bogus information is indirect on packet delivery from the perspective of the network. We get the expression of indirect impact metric of node A:

$$IDI_A(t) = \delta_1 DS_A(t) + \delta_2 LC_A(t), \quad (11)$$

where $\delta_1 + \delta_2 = 1$ and $0 < \delta_i < 1$ which is the coefficient factor. The indirect impact metric of each node's one-hop neighbors can be calculated in terms of information in the beacon. To reduce the bandwidth consumption caused by beacon exchange, it is not necessary to contain the neighbor information in the beacon unless the information is changed.

4.3. Fault Activity Metric Based on Determining Node State. Due to the uncertainty in the faulty impact, we model the direct impact and the indirect impact as random processes and allow the sensor nodes to collect empirical data for characterizing the process. In order to identify the faulty state of each node, we design an impact metric which enables each node to measure faulty impact for both its own faulty impact and its neighbors' faulty impact based on its knowledge of available one-hop neighbors. The total impact value for node A can be given by

$$I_A(t) = \epsilon DI_A(t) + (1-\epsilon)\, IDI_A(t), \quad (12)$$

where ϵ is the factor with $0 < \epsilon \le 1$. Then we define the novel faulty state and FA metric as follows.

Definition 1 (the node-faulty state). $\Lambda_i(t_0)$ denotes the faulty status in node i at time t_0, where $\Lambda_i(t_0) = 1$ indicates that the node i is faulty where $I_i(t_0) \le I_0$; otherwise, $\Lambda_i(t_0) = 0$ indicates that node i is not faulty.

To determine the node-faulty state, we can use a heuristic approach to test whether the current node is experiencing "being faulty condition" in which the impact metric drops below a certain threshold. Any node whose impact metric is below the threshold can be regarded as a faulty node since we are unable to accomplish our objectives efficiently. We suppose that each node i updates DI_i and IDI_i after each update period of T seconds and estimates the FA metric after each update calculation period of $T_s \gg T$ seconds. Next, we define the FA which is the time that faulty nodes spend in each state per unit time.

Definition 2. The FA for node-faulty state denoted by A_i is the fraction of time during period $[t-T_s, t]$ for which the node i is in the state Λ_i, that is, $A_i = (T/T_s)\int_{t-T_s}^{t} \Lambda_i(x)dx$.

To facilitate observation, we illustrate an example of converting the impact value of a sensor node A (as shown in Figure 4) into the faulty state with I_0 being 0.6 in Figure 5 and the value of fault activity in Figure 6. Once we obtain the estimation of FA, we can get the fault-statistical information for routing path selection and resource allocation.

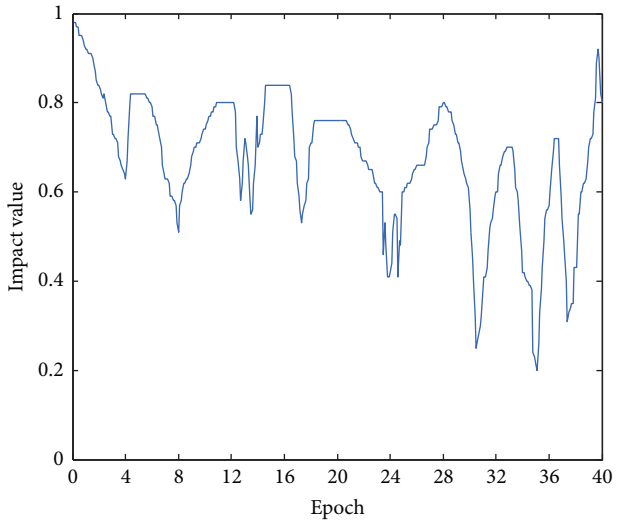


Figure 4: Impact value of a sensor node.

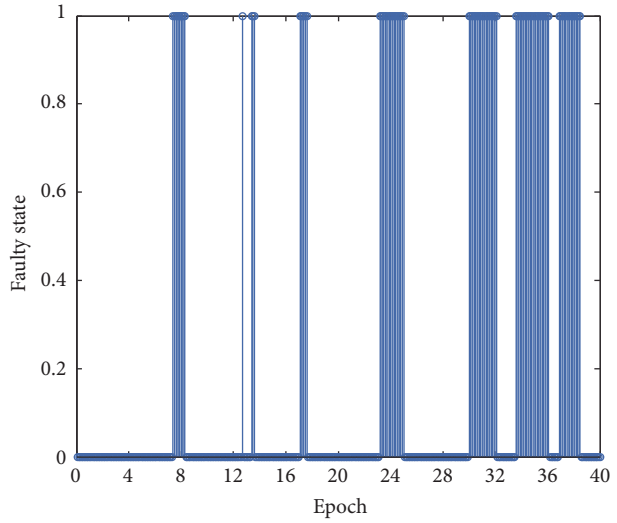


Figure 5: Distribution of faulty state.

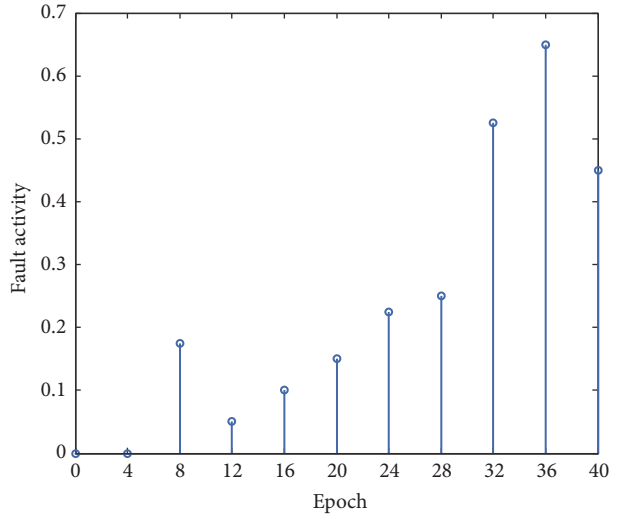


Figure 6: Estimation of FA.

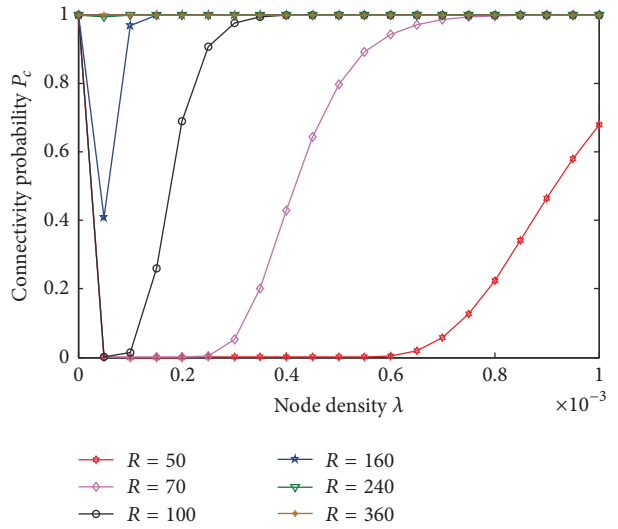


Figure 7: Connectivity probability with $S = 1000 * 1000\,\mathrm{m}^2$, $2 * 10^{-5} \leq \lambda \leq 1 * 10^{-3}$, and $50\,\mathrm{m} \leq R \leq 360\,\mathrm{m}$.

5. Fault Activity Geographic Opportunistic Routing Algorithm

In this section, a geographic routing protocol on fault activity metric is presented, providing methods for sensors to choose the candidates based on impact caused by faulty behaviors. FA-GOR selects more forwarding candidates based on the routing metric of available next-hop forwarders.

Before presenting our routing algorithm, we first discuss an intrinsic nature of WSNs that can support our idea: network connectivity. When sensors are distributed in area S randomly, the process that there are n sensors in an arbitrary area U is modeled according to Poisson distribution [40]:

$$P\{|N_n| U = n\} = \frac{(\lambda U)^n}{n!} e^{-\lambda U}, \tag{13}$$

where λ denotes node density, $|N_n|$ is the cardinality of N_n, and $\lambda = |N_n|/U$. In order to describe the full connection probability P_c, we first calculate the probability P_{iso} that no link exists between sensor N and other nodes:

$$P_{\mathrm{iso}} = P\{|N_n| \pi = R^2 0\} = e^{-\lambda \pi R^2}. \tag{14}$$

In terms of the isolation probability P_{iso}, the full connection probability is given by the following [46]:

$$P_c \geq e^{-\lambda S P_{\mathrm{iso}}}. \tag{15}$$

Figure 7 shows that when λ and R are set as proper values, the expected fully connected can be achieved in a WSN.

Assuming that $\mathrm{Dist}(y, \mathrm{Dest})$ is denoted as the distance from sending node y to the sink (denoted as Dest) and $\mathrm{Dist}(v, \mathrm{Dest})$ is denoted as the distance from its neighbor $v \in N^{(y)}$ to the sink, we have the routing metric for the forwarding candidates as follows:

$$\mathrm{metric}_{yv} = \vartheta \left(1 - \frac{\mathrm{Dist}(v, \mathrm{Dest})}{\mathrm{Dist}(y, \mathrm{Dest})}\right) + (1 - \vartheta)(1 - I_v), \tag{16}$$

Require: $v \in N^{(y)}$, the neighbor set of node y
Ensure: the next forwarder n
(1) start a retransmission timer;
(2) select the forwarding set $F^{(y)}$ including g candidates from neighbor nodes $N^{(y)}$, $F^{(y)} = \emptyset$, $g = 0$;
(3) **for** each node $i \in (N^{(y)} - F^{(y)})$ **do**
(4) **if** $\text{metric}_{yi} = \max\{\text{metric}_{yj}\}$, $\forall j \in (N^{(y)} - F^{(y)})$ and $n \leq g$ **then**
(5) add i to $F^{(y)}$; $g++$;
(6) **end if**
(7) **end for**
(8) prioritize the forwarder set using metric;
(9) broadcast the data packets;
(10) **for** each node $i \in F^{(y)}$ **do**
(11) receive the data packet;
(12) check the sender ID and start a timer and $\text{time}(i) = \kappa/\text{metric}_{yi}$, where κ is a constant;
(13) **end for**
(14) **if** node n which obtains the highest priority receives the data packet correctly **then**
(15) reply an ACK to notify the sender as well as other candidates to cancel their timers;
(16) **else**
(17) **if** the priority timer expire **then**
(18) set $n = n'$, node n' has the lower-priority;
(19) goto 14;
(20) **end if**
(21) **end if**
(22) **if** no forwarding candidate has successfully received the packet **then**
(23) **if** the retransmission timer does not expire **then**
(24) goto 2;
(25) **end if**
(26) **end if**
(27) return

Algorithm 1: FAGOR algorithm.

where $\vartheta \in (0, 1]$ is the constant weight indicating the relative preference between distance and fault impact value I_v. Each next-hop forwarder is assigned with its priority based on the metric value of (16).

We introduce the FAGOR algorithm to select the next relay node following the assigned priority in forwarder set F to relay the packets. Algorithm 1 depicts the pseudocode of FAGOR algorithm.

Our FAGOR could defend against a wide range of misbehaviors. For example, in Figure 8, as one candidate of node B's next-hops, node A lies about its location and associates with disguisers (H_4–H_7) as its colluders. The mutual neighbors of A and B, H_1–H_7, need to report their RSS values related to A to B and work based on majority voting. B could choose reference nodes from $N^{(A)} \wedge N^{(H)}$ to verify the validity of the voters. Node R sends the estimate value DS_{H_i} about H_4–H_7 to node B by (8). Node B calculates LC_A to incorporate it into indirect value of node A. Finally, node A is found as being faulty state during a period and could not be selected into the routing path.

6. Fault Activity Utility-Based Optimal Flow Control Approach

In this section, we present a leaky-hop model which explicitly takes account of faulty activities and then present fault activity-based utility optimal flow control (FA-UOFC) based on the leaky-hop model. One underlying assumption in the utility framework of rate control is that the same flow is present at all the hops along the route. In hostile environments, however, the data rate x_s of a given flow s becomes thinner along its path. Due to potential faulty behaviors on each node, all data deliveries are not successful.

6.1. Leaky-Hop Model. In Section 4, A_i is denoted as the fraction of time during the unit period for which node i exhibits misbehavior, while $1 - A_i$ is the time fraction during which node i accomplishes its communication effectively as a good node. A_i characterizes the probability of faulty behaviors over single hop. At a link (i, j) with transmission rate $\sum_{s \in S(i,j)} x_s$, since data is only received correctly on $1 - A_i$

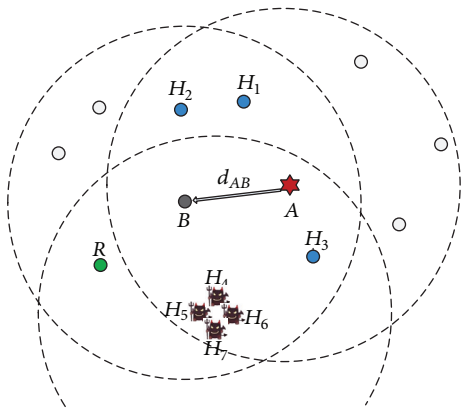


Figure 8: An illustration for misbehaving nodes.

from hop i, the correctly received data rate x_j' at hop j is presented by

$$x_j' = (1 - A_i) \cdot \sum_{s \in S(i,j)} x_s. \tag{17}$$

For path R_s traversing multiple hops, the end-to-end packet success ratio for path R_s is given by

$$\gamma_s = \prod_{(i,j) \in R_s} (1 - A_i). \tag{18}$$

R_s^i is denoted as the subpath of R_s between source S and the intermediate node i, and $\overline{R}_s^i$ is denoted as the subpath of R_s between the intermediate node i and the sink node of R_s. For subpath R_s^i of a data flow, the data delivery probability at leaky-hop i is given by $\gamma_s^i = \prod_{(i,j) \in R_s^i} (1 - A_i)$. It can be seen that the data rate of a given flow becomes "thinner and thinner" at each hop along its routing path, and we call the flow traversing every potential misbehaving hop to be a leaky-hop flow. We define goodput x_s' of flow s as the data rate received correctly at the sink [47]. Therefore, in the presence of misbehaving nodes, $x_s' = \gamma_s x_s$.

An example leaky-hop model is described in Figure 9. Flow 1 traverses along four leaky-hops: n_1, n_3, n_4, and n_6. Flow 2 traverses along three leaky-hops: n_2, n_3, and n_5. The goodput of flow 1 at the destination is $(1 - A_{n_1})(1 - A_{n_3})(1 - A_{n_4})(1 - A_{n_6})x_1$. It can be seen that the data rate of a flow becomes lower and lower along multiple hops. For example, $\gamma_1^{n_1} x_1 \to \gamma_1^{n_3} x_1 \to \gamma_1^{n_4} x_1 \to \gamma_1^{n_6} x_1$. There may exist different data delivery probabilities at a leaky-hop for different data flows. The leaky-hop n_3 for flow 1 and flow 2 has different data delivery probabilities: $\gamma_1^{n_3} = (1 - A_{n_3})\gamma_1^{n_1}$, $\gamma_2^{n_3} = (1 - A_{n_3})\gamma_2^{n_2}$. We call a potential faulty node on the routing path of flow s to be a leaky-hop for flow s.

The resource allocation problem in WSNs gives rise to many new challenges. Among the many unique characteristics of WSNs, we focus on two constraints in our formulation. Due to the broadcast nature of the wireless medium, all transmissions are not successful and the transmitters contend with each other in the broadcast domain. To apply the constraint of contention regions, we use the contention set concept from [48]. The contention set Ω is denoted as the subset of links belonging to a contention region that, at most, one link in Ω can transmit in each time slot successfully. Let $\Omega_{(i,j)}$ be the contention link set of link (i, j). If user s transmits over link (i, j), other flows in the contention set $\Omega_{(i,j)}$ cannot transmit packets simultaneously. Let $c_{(i,j)}$ be the capacity of link (i, j). We incorporate the node-faulty activity statistics into the link capacity constraint generation. Due to leaky-hops along the routing path, the flow rate is potentially reduced at each of the receiving hops as packets are lost. The availability metric in Definition 2 means the fraction of time for which the immediate sensor delivers packets correctly. The stochastic capacity constraint on the total flow rate traversing a link (i, j) is given by

$$\sum_{(i',j') \in \Omega_{(i,j)}} \sum_{s \in S_{(i',j')}} \frac{\gamma_s^i x_s}{c_{(i,j)}} \le 1. \tag{19}$$

Another major point in WSNs is the energy constraint caused by the energy consumption of sensing, transmitting, receiving, and relaying data. Let B_i denote the initial amount of initial battery (energy) at node i, $i \in N$.

We also incorporate the FA statistics into the energy constraint, in which the power consumption of each node i should not exceed the maximum allowed power generation $p_i^{\max}$:

$$(e_t + e_r) \sum_{s \in S(i)} \gamma_s^i x_s + (e_s + e_t) \lambda_i \le p_i^{\max}, \tag{20}$$

where $\lambda_i = \gamma_s^i x_s$, if flow s starts from sensor node i; otherwise, $\lambda_i = 0$. For a prespecified lifetime, T_d, the maximum node power consumption $p_i^{\max} = B_i/(T_d - \tau p_{\text{idle}})$, where τ and p_{idle} are the duty cycle and energy consumed in the idle state per unit time.

6.2. FA-UOFC for Multiple Services. For wireless sensor networks in a smart city, many different types of sensor are emerging to present numerous applications that exhibit different utility behaviors. Similar to [20], we observe that the operations of the data gathering involve both inelastic and elastic traffic. In order to support the multiple types of traffic, the flow control strategy should have the ability to allocate traffic rates properly in order to balance the performance for different applications. We will adopt the rate-control protocol, newly developed by Wang et al. [20], for handling elastic and inelastic traffic. When each source s transmits at rate x_s, it attains a utility $U_s(x_s)$. 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 "pseudoutility" $u_s(x_s)$ as

$$u_s(x_s) = \int_{m_s}^{x_s} \frac{1}{U_s(y)} dy, \quad m_s \le x_s \le M_s. \tag{21}$$

In order to provide a good performance balance for different applications in sensor networks, the flow control can be generalized to obtain new problem formulations, namely, utility optimal flow control (UOFC), which maximizes the

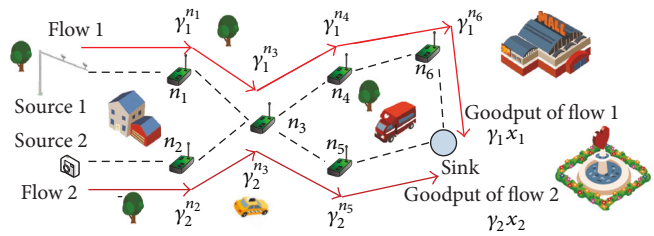


Figure 9: An example network with leaky-hop flows.

sum pseudoutility under the contention constraint [41] and the energy constraint.

At the sink of flow s, the correctly received data rate can be represented as $\gamma_s x_s$. The optimization problem introduced previously can be presented as a new formulation:

$$\begin{aligned} \text{Problem: max} \quad & \sum_{s\in S}\left(\int_{m_s}^{\gamma_s x_s}\frac{1}{U_s(y)}dy\right) \\ \text{s.t.:} \quad & \sum_{(i',j')\in\Omega_{(i,j)}}\sum_{s\in S_{(i',j')}}\frac{\gamma_s^i x_s}{c_{(i,j)}} \le 1 \\ & (e_t+e_r)\sum_{s\in S(i)}\gamma_s^i x_s + (e_s+e_t)\lambda_i \\ & \le p_i^{\max}. \end{aligned} \tag{22}$$

Since the objective function $U_s(\cdot)$ is nonnegative, continuous, and strictly increasing (not concave), the "pseudoutility" $\int_{m_s}^{\gamma_s x_s} 1/U_s(y)dy$ must be a strictly increasing concave function. Therefore, with linear, separable, convex, and compact constraints, the optimization problem in (22) has a unique optimal solution.

In the following, we use Lagrangian dual method and develop a rate-control algorithm. First, we form the Lagrangian as follows:

$$\begin{aligned} L\left(x',\underline{\lambda},\overline{\lambda}\right) = & \sum_{s\in S}\left(\int_{m_s}^{\gamma_s x_s}\frac{1}{U_s(y)}dy\right. \\ & -\gamma_s^i x_s\left(\left(\sum_{(i,j)\in L(s)}\sum_{(i',j')\in\Omega_{(i,j)}}\underline{\lambda}\right)+(e_r+e_t)\sum_{i\in N(s)}\overline{\lambda}\right. \\ & \left.\left.+(e_s+e_t)\iota_s\right)\right)+\sum_l\underline{\lambda}c_l+\sum_{i\in N}\overline{\lambda}p_i^{\max}, \end{aligned} \tag{23}$$

where $\underline{\lambda}=[\underline{\lambda}_1,\underline{\lambda}_2,\ldots,\underline{\lambda}_L]^T$, $\overline{\lambda}=[\overline{\lambda}_1,\overline{\lambda}_2,\ldots,\overline{\lambda}_S]^T$, and $u=(\underline{\lambda},\overline{\lambda})$ are all nonnegative. $\iota_s=\overline{\lambda}$, assuming flow s starts from node n. The objective function of dual problem is given by

$$\min_{\underline{\lambda},\overline{\lambda}} \quad D\left(\underline{\lambda},\overline{\lambda}\right) = \min_{\underline{\lambda},\overline{\lambda}\ge 0} \quad \max_{x'} L\left(x',\underline{\lambda},\overline{\lambda}\right). \tag{24}$$

We use the gradient method to solve the above dual problem. The Lagrangian multipliers for the dual can be updated as follows at each iteration t:

$$\begin{aligned} \underline{\lambda}_{(i,j)}(t+1) = & \left[\underline{\lambda}_{(i,j)}(t)+\varphi\left(\sum_{(i',j')\in\Omega_{(i,j)}}\sum_{s\in S_{(i,j)}}\left(x_s\gamma_s^i\right)\right.\right. \\ & \left.\left.-c_{(i,j)}\right)\right]^+, \end{aligned} \tag{25}$$

$$\begin{aligned} \overline{\lambda}_{(i)}(t+1) = & \left[\overline{\lambda}_{(i)}(t)\right. \\ & +\varphi\left(\left((e_t+e_r)\sum_{s\in S(i)}x_s+(e_s+e_t)\lambda_i\right)\gamma_s^i\right. \\ & \left.\left.-p_i^{\max}\right)\right]^+, \end{aligned} \tag{26}$$

where $\varphi>0$ is a small step size, and $z^+=\max\{0,z\}$. Here, $\underline{\lambda}_{(i,j)}$, $(i,j)\in L$, can be considered the price for using the resource of contention set $\Omega_{(i,j)}$. Similarly, $\overline{\lambda}_{(i)}$, $i\in N$, can be interpreted as the price for using energy at sensor node i. Given these two prices, each flow s, $s\in S$, adopts its rate according to

$$x_s(t+1)=\left[u_s'^{-1}\left(\lambda^s(t)\right)\right]_{m_s}^{M_s}, \tag{27}$$

where $[z]_b^a=\min(\max(z,a),b)$, $u_s'^{-1}$ is the inverse of u_s', and (27) can be replaced as follows:

$$x_s(t+1)=U_s^{-1}\left(\left[\frac{1}{\lambda^s(t)}\right]_{U_s(m_s)}^{U_s(M_s)}\right), \tag{28}$$

where $\lambda^s(t)=\sum_{(i,j)\in L(s)}\underline{\lambda}_{(i,j)}(t)+(e_r+e_t)\sum_{i\in N(s)}\overline{\lambda}_i(t)+(e_s+e_t)\iota_s(t)$. Hence, we propose Algorithm 2 based on the problem formulation of fault activity-based utility optimal control.

Our algorithm can be carried out in a distributed manner by message exchange in the network, as shown in Figure 10. To implement our scheme, no node in the network needs to know global information nor the individual variables of algorithm. The information needs to be updated by the receiving node and to be sent via piggybacking.

At each time $t = 1, 2, \ldots,$
(1) Update source rate: Each source node s calculates the source rate $x_s(t + 1)$ for the next period according to Eq. (28);
(2) Update resource prices: Using the information of aggregated transmission rate, link (i, j) computes a new sole contention price $\underline{\lambda}_{(i,j)}(t + 1)$ according to Eq. (25) and node i computes a new energy price $\overline{\lambda}_i(t + 1)$ according to Eq. (26);
(3) Deliver information towards the sink: Sensor node i adapts the contention price $\underline{\lambda}_{(i,j)}(t)$ and the energy price $\overline{\lambda}_i(t)$ along the path, and propagates towards the sink;
(4) Feedback message from the sink: The sink feedbacks the FA parameter and the aggregated resource price to the source via the reverse path.

Algorithm 2: FA-UOFC algorithm.

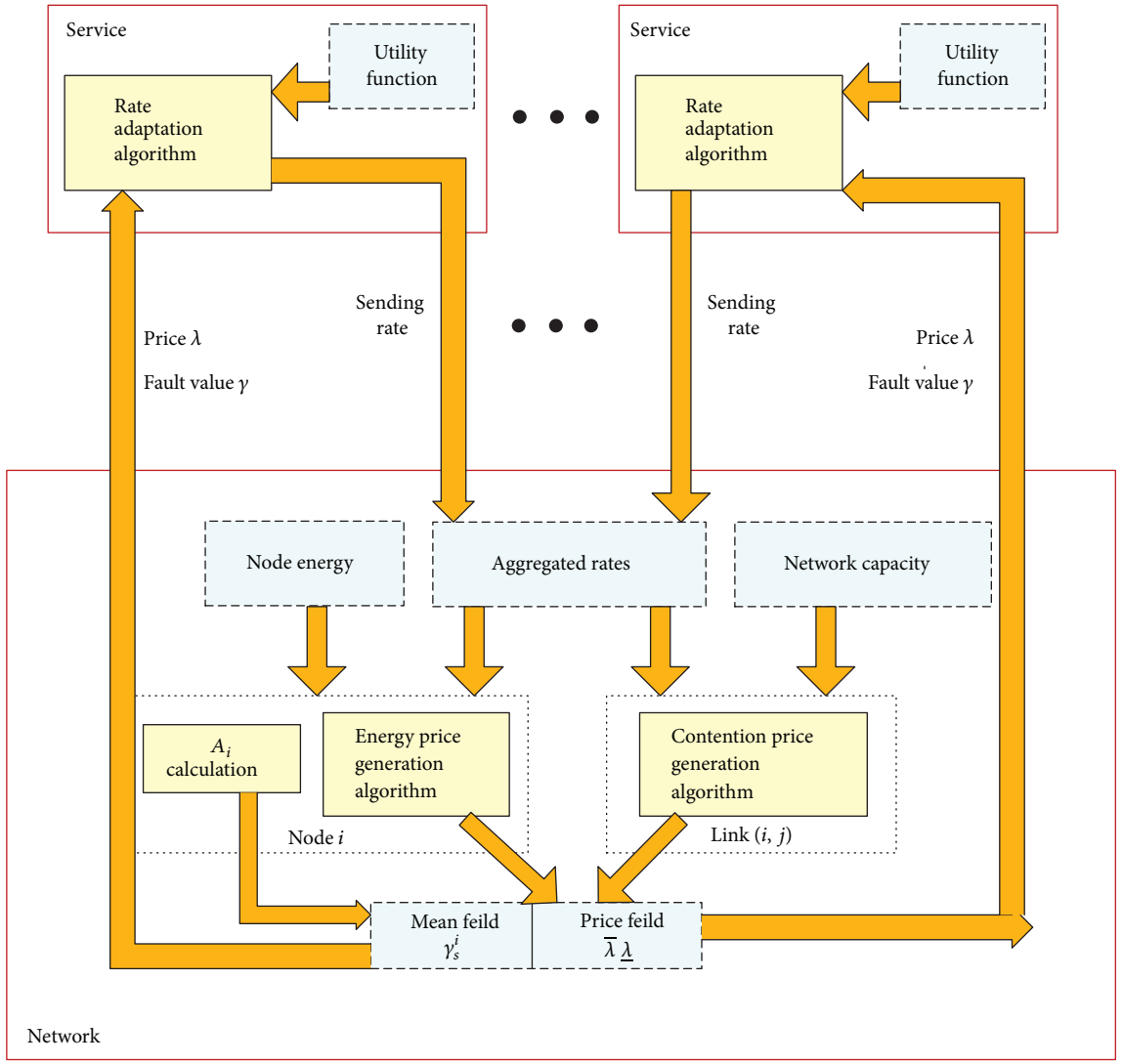


Figure 10: System model for Algorithm 2.

First, each sensor node estimates and updates the resource price locally, the fault activity information of its neighbors, and its own fault activity information; then we apply two additional header fields, mean field and price field, to both data packets and control packets. When a new packet arrives, the updated FAI is multiplied together and the local prices are added to the price of the packets that arrive from the upstream node. When the packet arrives at the sink, values of the two fields will be feedback to the source node by the acknowledgement packet.

Second, when the packet arrives at the sink, the aggregated FAI and resource prices will be piggybacked to the source node in the acknowledgement packet.

Third, each node can construct its local contention set by exchanging information from neighbors instead of knowing the entire network topology.

Hence, the total number of additional exchange operations is within $O(LN)$, where N is the number of source S' routing paths and L is the number of network's links. The proposed fault activity utility optimal flow control algorithm is practical and realizable in WSNs.

6.3. Utility Fairness. The goal of our rate-control approach is to able to maintain an acceptable level of service degradation, including effective network throughput and fairness, in the presence of misbehaving nodes. In this section, we establish the existence and uniqueness of a utility fair solution with the presence of misbehaving nodes and define a novel index, utility fairness index, which quantitatively measures the degree of utility fairness in distributed systems.

Considering the performance of different services, the utility OFC (UOFC) with the resource constraints in WSNs allocates flow rates of different applications according to their utility requirements, and, what is more, the optimization approach yields utility fairness [20]. In WSNs without faulty nodes, the set of goodput rate vector X for each flow s that satisfies the resource constraints in problem (22) with $\gamma_s^i = 1$ for $i \in N$ is called the rate region $X(c, s, 1)$. In hostile environments, the set of goodput vector X' that follows from problem (22) with $\gamma^i \neq 1$ is denoted as $X(c, s, \gamma)$. It is clear that $\gamma_s^i \leq 1$ and that $X(c, s, \gamma) \subseteq X(c, s, 1)$.

When the rate-control Algorithm 2 with $A_i = 0$ leads to equilibrium $(x^*, \underline{\lambda}^*, \overline{\lambda}^*)$ at convergence, the pseudoutility function $u(x)$ is maximized within the feasible solution. Here we can employ both a utility proportional fairness as described in [20] and utility max-min fairness proposed in [48]. For any other feasible allocation $x \neq x^*$, if $\sum_{s\in S}(\partial u(x_s^*)/\partial x_s)(x_s - x_s^*) = \sum_{s\in S}((x_s - x_s^*)/U_s(x_s^*)) \leq 0$, the source rate allocation $X^* = [x_1^*, x_2^*, \ldots, x_s^*]^T$ is utility proportionally fair. $U(x)$ is the strictly concave function; the strict inequality holds and meets the utility proportional fairness definition. Therefore, the source rate allocation in Algorithm 2 with $\gamma_i = 1$ is utility proportionally fair. To achieve utility max-min fairness, we give a new distributive flow control algorithm. If the aggregate price of Algorithm 2 is replaced with $\lambda^s(t) = \max\{\max_{(i,j)\in L(s)}\underline{\lambda}_{(i,j)}(t), \max_{i\in N(s)}\overline{\lambda}_i(t)\}$, which is the maximum of the contention prices and the energy prices along the path, the updated algorithm could provide a utility max-min fair allocation among all data flows.

6.3.1. Utility Fairness of $X(c, s, \gamma)$. We relate the arguments on utility OFC based on the leaky-hop model to a case without leaky-hop by proving a continuity property of fair allocation as γ_i approaches 1. Let the ratio of node-faulty activities drop to zero: $\lim_{k\to\infty}\min_{(i,j)\in R_s}\gamma_i^k = 1$. Then the rate regions in WSNs containing faulty nodes converge the rate regions in the corresponding WSNs without faulty nodes, and utility fair solution converges to the corresponding utility fair solution without faulty nodes [47].

The goal of our rate-control approach is to be able to maintain an acceptable level of service degradation, including effective network throughput and fairness, in the presence of misbehaving nodes. In this section, we establish the existence and uniqueness of a utility fair solution with the presence of misbehaving nodes and define a novel index, utility fairness index, which quantitatively measures the degree of utility fairness in distributed systems.

In the homogeneous traffic context, Jain et al. [49] propose a quantitative measure called Index of Fairness to tell how far the resource allocation is from equality. With considering QoS requirements of different applications, it may be undesirable to allocate resources simply according to conventional measurements such as Index of Fairness [49]. Hence, we define a novel index, *index of utility fairness* $f(x)$, which measures the utility fairness of various applications and addresses their utility requirements:

$$f\left(x'\right) = \frac{\left(\sum_{s=1}^{n} u\left(x_s'\right)\right)^2}{|N|\sum_{s=1}^{n} u\left(x_s'\right)^2}, \tag{29}$$

where x_s' is the goodput of flows and $|N|$ is the number of flows in WSNs. This index measures the "equality" of user utility allocation. If all sources get the same amount of utility, that is, if $u(x_i')$ are all equal, then the utility fairness index is 1. As the disparity increases, the utility fairness decreases and is near 0 as only a selected few users will be favored. A higher value of $f(\cdot)$ means a higher degree of utility fairness.

7. Performance Evaluations

In this section, we conduct simulation experiments to evaluate the performance of the proposed FAGOR protocol and FA-UFOC scheme when misbehaving nodes exist in the network. We first describe the simulation setup and then compare the simulation results with GPSR [12], DWSIGF [13], QGOR [14], and our proposed FAGOR protocol in a variety of experiments. Next, we illustrate the advantage of the FA-UOFC over the traditional OFC approach without considering misbehavior of faulty nodes. Finally, we show the effectiveness of our proposed FAGOR protocol combined with our FA-UOFC algorithm for WSNs in adversarial environments, and we simulate the fairness of our proposed scheme in terms of utility fairness index and the convergence discussed in Section 6.3.1.

The extensive simulations have been conducted in OPNET and C++ simulator. The OPNET simulator is

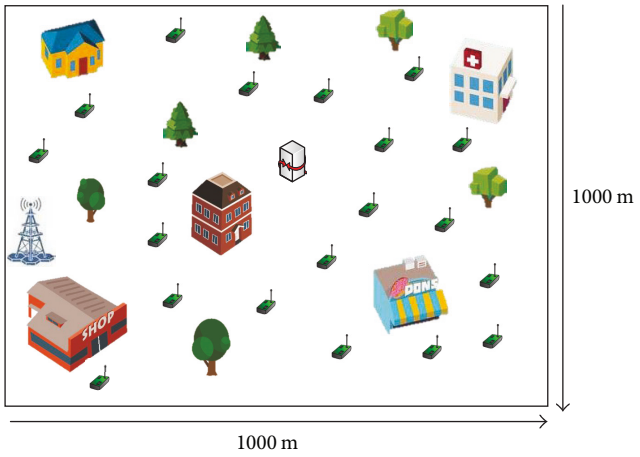


Figure 11: Simulation scenario.

designed for the network design and performance test. It is further enhanced to support for wireless sensor networks in city environments. In original OPNET, the calculation of received power only considers the propagation model of free space. In the urban communication environment, wireless channel is affected by the diffraction of signals by various buildings and trees. A Rician model is used as a channel fading model to illustrate effects due to buildings, obstacles, and trees in the city. We incorporate Rician distribution into the receiver power module in OPNET in accordance with radio wave propagation model in practical scenarios.

We consider static WSNs for a smart city. Therefore, mobility is not considered in experiments. As shown in Figure 11, 100 to 400 wireless sensors, which include both misbehaving sensors and well-behaved sensors, are randomly deployed in an area of 1000 m × 1000 m. The percentage of misbehaving nodes to all the nodes which is a simulation parameter is varied from 0 to 0.4 in different experiments. Each sensor has IEEE 802.15.4 based technology. The sources send data to 10 sinks which have sufficient power. The initial power of each sensor is set to 9 mW. The parameters for energy consumption are set to $e^t = 150$ nJ/bit, $e^r = 158$ nJ/bit, and $e^s = 100$ nJ/bit, respectively [50]. Each simulation runs 3000 iterations, and the default simulation parameters are listed in Table 1.

7.1. The Effectiveness of FAGOR. In this section, we show how our FAGOR protocol can provide effective routing with the existence of an arbitrary number of misbehaving nodes. The proposed FAGOR protocol is benchmarked against other three routing protocols: (1) DWSIGF, (2) GPSR, and (3) QGOR (a QoS-aware GOR which provides routing service based on the end-to-end QoS metric [22]). The following two metrics are used to compare the performance of the protocols:

(i) PDR: the ratio of the total number of data packets by the sink packet delivery to the total amount of data packets sent by the source

(ii) End-to-end delay: the time interval for the data packet to be transmitted from the source node to the sink

Table 1: Parameter values in simulations.

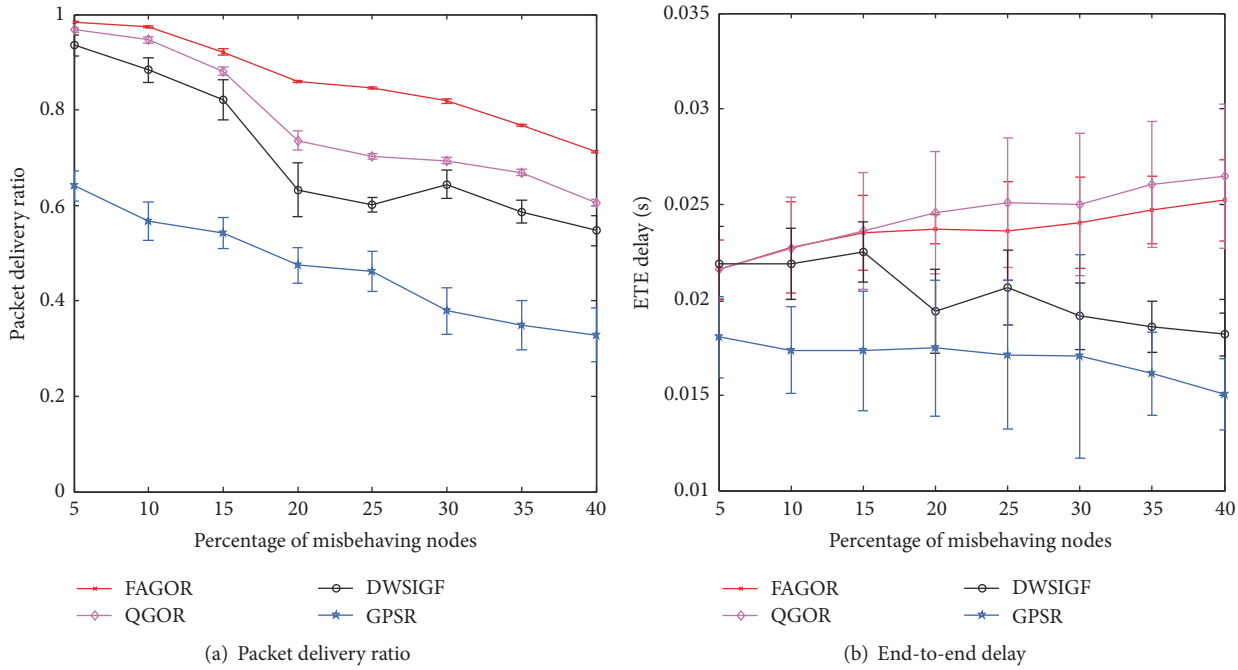
Parameter	Value
Simulation iterations	3000
Numbers of nodes	100, 200, 300 or 400
Percentage of misbehaving nodes	0~0.4
Network size	1000
MAC protocol	802.15.4
Packet size	512 byte
Numbers of candidates	$N = 3$
Maximum power consumption	9 mW
Power parameters	$e^t = 150$ nJ/bit, $e^r = 158$ nJ/bit, $e^s = 100$ nJ/bit
Weight values	$\alpha = 0.7$, $\delta_1 = 0.4$, $\delta_2 = 0.6$, $\kappa = 0.7$ $\gamma = 0.7$, $\vartheta = 0.7$, $\epsilon = 0.8$, $\varphi = 0.002$

We simulate Sybil attacks with 4 Sybil nodes which perform random attacks with a configurable probability. The Sybil nodes create more virtual locations by altering their transmission power, which is similar to location spoofing attackers. We model randomly distributed misbehavior nodes such as black holes, gray holes, and nodes in jamming regions which drop data packets with variable possibility. The routing protocol is simulated attacking with varied probabilities to evaluate performance under various misbehaviors.

First we show the effectiveness of FAGOR under varied the number of misbehaving nodes. Figure 12(a) reports the packet delivery ratio of FAGOR in comparison with the other three routing protocols. We have the following observations: (a) the PDR of FAGOR is consistently higher than GPSR and DWSIGF with the existence of a varied number of misbehaving nodes, and (b) the PDR of FAGOR declines more slowly than GPSR and DWSIGF as the percentage of misbehaving nodes increases. The reason is that the misbehaving nodes are more likely to be chosen as the next-hop nodes in GPSR and DWSIGF, while FAGOR incorporates faulty impacts for choosing more reliable candidates to set up the routing paths.

The PDR in QGOR is higher than in other routing protocols except FAGOR. This can be explained as follows. QGOR also selects more reliable relays according to the QoS priority of neighboring nodes. However, without the ability to identify location-related attacks, QGOR may select a Sybil node as the next-hop relay. Our FAGOR gives low reliability values to Sybil nodes based on majority voting and to other misbehaving nodes based on direct-impact values. In terms of the compound of reliability value by the proposed FA metric, FAGOR transmits packets with faulty hops, and the impact of misbehaviors on the network performance is stable.

As the number of misbehaving nodes increases, the end-to-end delay of GPSR and DWSIGF plotted in Figure 12(b) decreases. For hostile sensor networks, misbehaving nodes in the routing path would cause links to break. The decline of the end-to-end delay means that only the data packets



(a) Packet delivery ratio

(b) End-to-end delay

Figure 12: Packet delivery ratio and end-to-end delay versus percentage of misbehaving nodes.

from the nodes that are closer to the sink can be successfully delivered to the sink in GPSR and DWSIGF, while it is hard to successfully transmit the data packets to a distant destination with more hops. However, FAGOR and QGOR encourage suboptimal candidates to collaboratively relay data packets that the delay of such packets raises. As the number of misbehaving nodes increases, FAGOR and QGOR spend more time maintaining uninterrupted communication, and higher end-to-end delays are consequently achieved.

Furthermore, FAGOR gets a lower end-to-end delay than QGOR because of the existence of Sybil nodes among misbehaving nodes. Since the reliability of neighbors is unknown at the beginning, FAGOR uses majority voting to decrease the probability of location attacks. Compared to QGOR which operates without identifying location attacks, FAGOR mitigates Sybil attacks in advance and saves the network delay time.

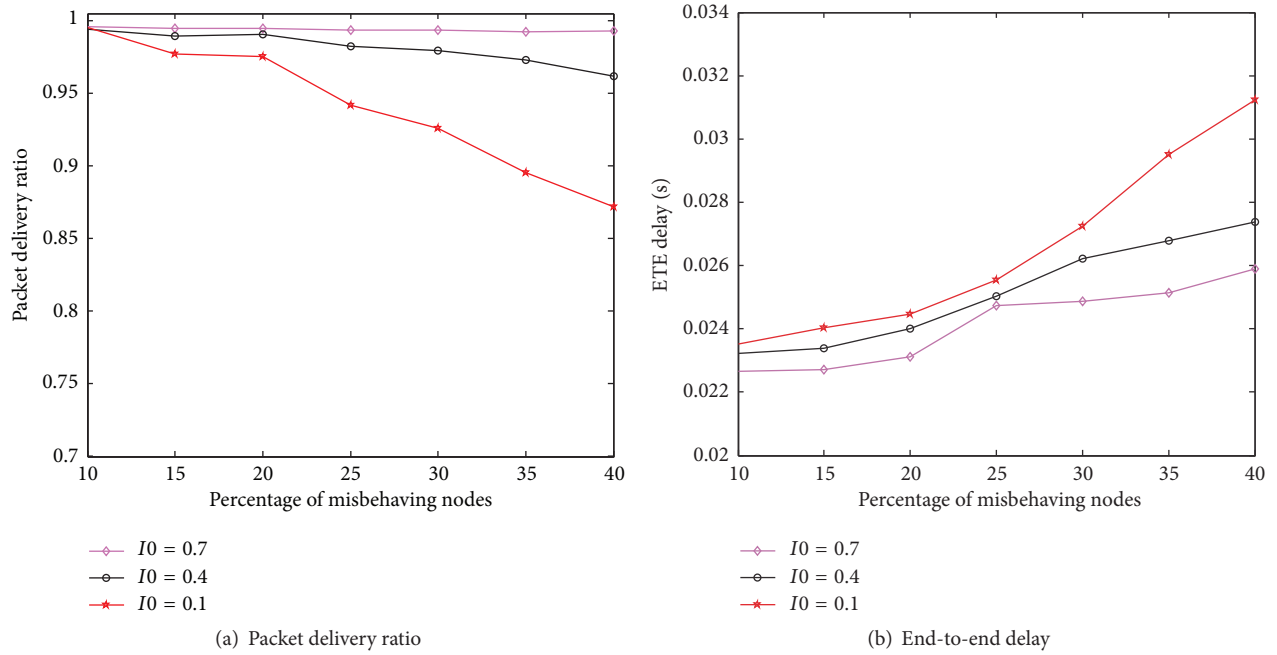
We further study the effect of I_0 on the performance of FAGOR. The packet delivery ratio under varied values of I_0 is shown in Figure 13(a). In this simulation, we find out that underestimating the parameter I_0 will lead to imprecise next-hop choosing results and will affect the performance of FAGOR. On the other hand, overestimating I_0 as shown in Figure 13(b) may make the routing algorithm yield less feasible next-hops, lead to repeated candidate discovery, and result in higher delay. This result illustrates that there is trade-off between the PDR and time delay and choosing a proper value of I_0 gives better performance of FAGOR.

Figure 14 compares the performance of four protocols for different network size by increasing the numbers of nodes from 100 to 400. Compared with GPSR and DWSIGF, our FAGOR improves the delivery ratio by approximately 40% and keeps stable with the different random topologies.

In order to evaluate the number of candidates of the performance of FAGOR, we consider network scenarios with different numbers of misbehaving nodes. From Figure 15(a), we see that PDR increases and the gap of PDR between $I_0 = 0.1$, $I_0 = 0.4$, and $I_0 = 0.7$ gets smaller as the number of candidates increases. Thus more candidates in FAGOR can relieve the performance degradation under more misbehaving nodes. Figure 15(b) shows that the transmission delay decreases when $N = 1$. This is because, in FAGOR, when packet dropping ratio is high, there will be fewer hop counts which means that the data delivery would not last long. As the number of candidates increases, transmission time delay when $I_0 = 0.1$ increases faster than when $I_0 > 0.1$ due to a long one-hop delay in the presence of more misbehaving nodes. The simulation results show that there is a trade-off between the time delay and robustness on the selection of the candidates' numbers.

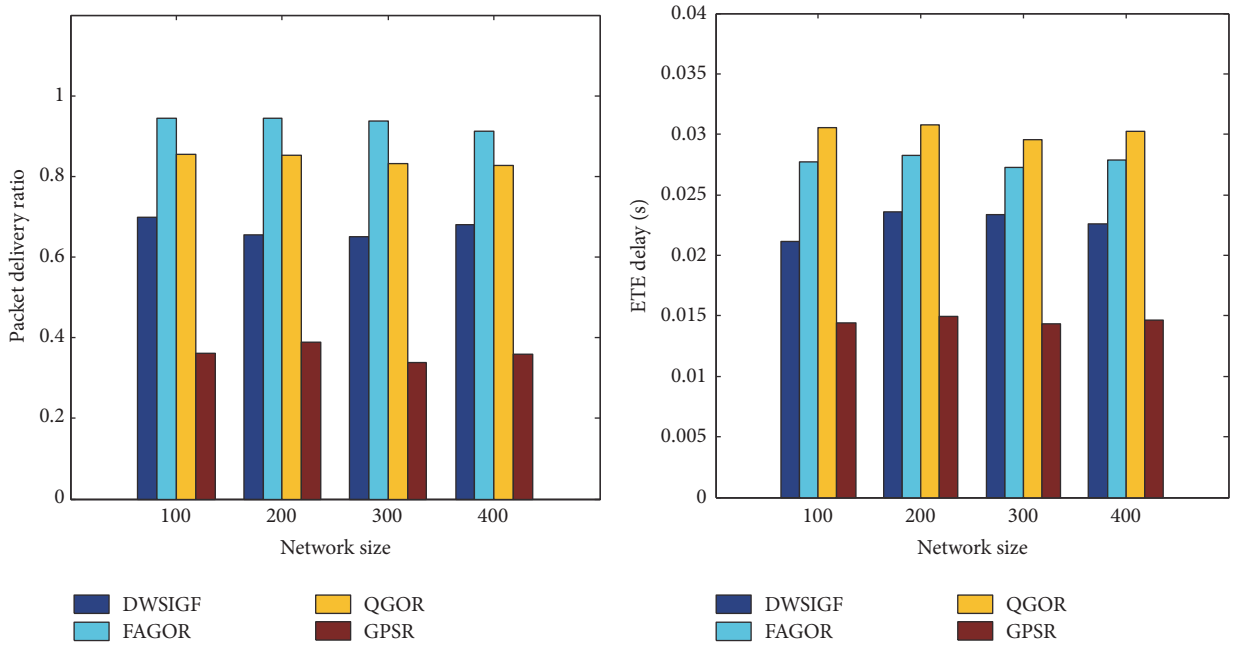
One object of FAGOR is to ensure the ability to operate effectively under dynamic misbehaving networks. In our simulation study, we set up a configurable probability of misbehaving nodes which behave well at the beginning of the experiment. They change to misbehaving nodes at random points of time. In Figure 16, we show the PDR performance of four protocols with a varied percentage of behavior-changing nodes. The following observations can be obtained from these figures. First, the packet delivery ratio of FAGOR is consistently higher than that of the other three protocols with different percentages of changing misbehaving nodes. Second, since FAGOR selects faulty nodes in the routing path, the impact of misbehaviors on the network performance is stable.

7.2. The Effectiveness of FA-UOFC. In this subsection, we use numerical examples to illustrate the advantage of FA-UOFC



(a) Packet delivery ratio (b) End-to-end delay

FIGURE 13: Packet delivery ratio and end-to-end delay with different values of I_0.

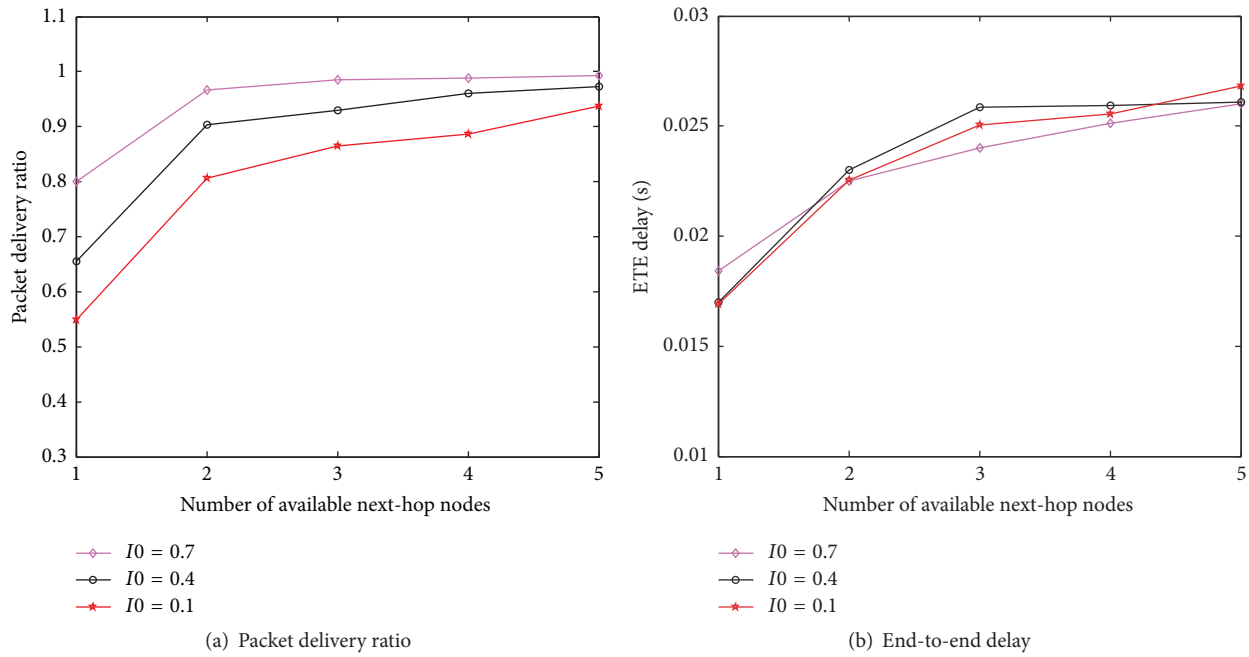


(a) Packet delivery ratio (b) End-to-end delay

FIGURE 14: Scalability evaluation.

algorithm over the OFC with same resource constraints. In the simulation, the sensor nodes turn to misbehaving nodes with probability 0.35. The network topology for one sink is depicted in Figure 17. We assume a link capacity of 4 kbps and a maximum node power consumption of 4 mW. In smart cities, there are various types of sensors embedded in networks to support multiple services with different QoS requirements. Therefore, we set utility functions consisting of elastic and inelastic traffic. The utility function of each source node is given as $U_1(x_1) = 1/(1 + e^{-2(x_1-6)})$, $U_2(x_2) = \log(x_2+1)/\log 11$, $U_3(x_3) = 0.1x_3$, $U_4(x_4) = 1/(1+e^{-2(x_4+4)})$. All the sources have their maximum rates at 10 Mbps.

We compare the effectiveness of two flow control strategies: (1) NE-OFC (OFC with noneffective utility



(a) Packet delivery ratio (b) End-to-end delay

Figure 15: Candidate number evaluation.

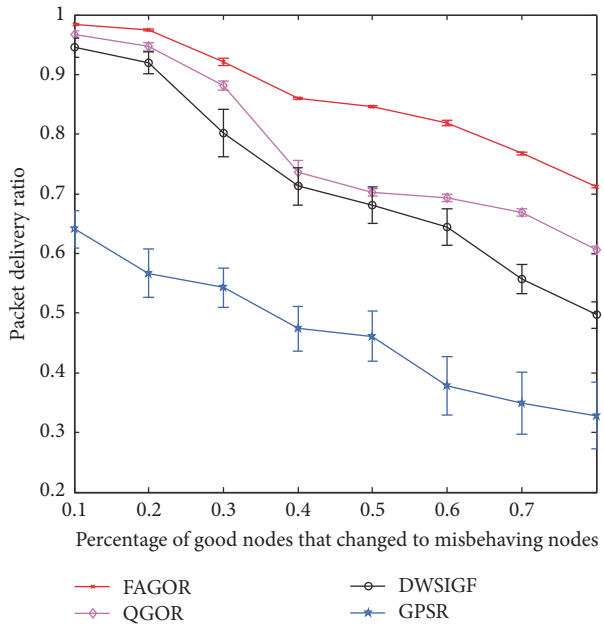


Figure 16: Packet delivery ratio versus percentage of behavior-changing nodes.

functions and constraints); (2) FA-UOFC (our improved OFC approach). NE-OFC approach subject to contention and energy constraints for WSNs is with utility functions of allocated flow rate without considering the faulty impact caused by misbehaving nodes. Figure 18 shows the comparison of the goodput for each flow at sink between our proposed FA-UOFC and NE-OFC. The proposed FA-UOFC can be seen to have achieved higher performance in terms of effective throughput compared to the conventional flow control method. Obviously this is due to the introduction of the faulty activity metric. The source adjusts its flow rate on its route adaptively to compensate for data loss in our FA-UOFC algorithm, which takes into account the effect of misbehaving nodes in utility function and constraints.

According to Section 6, x is denoted as the injection rate at the source node and x' is denoted as the goodput at the sink. Figure 19 verifies that the rate-control algorithm in NE-OFC converges and is able to provide utility proportional fairness (we use the sum of contention price and energy price) among four source nodes according to the utilities of x on the source nodes. Without considering faulty nodes, the source algorithm controls the flow rates to provide a utility fair resource allocation in which S_1 achieves a utility $U_1(x_1) = 1$ and S_2, S_3, and S_4 then share the remaining network resources with an equal utility of 0.52.

In fact, the goodputs of four flows cannot maintain the utility fairness at their sink nodes after traveling along the leaky-hops. The utilities of goodputs for four flows in the NE-OFC approach and FA-UOFC approach are shown in Figure 20. It can be seen that FA-UOFC yields higher utilities of goodput for four flows than NE-OFC. In Figure 19, three flows share a fair utility allocation that $U_2(x_2)$ is equal to $U_3(x_3)$ and $U_4(x_4)$. However, the utility fairness is broken due to different faulty effects on three paths consisting of misbehaving nodes. $U_3(x_3')$ and $U_4(x_4')$ of goodputs at the sinks both from NE-OFC and FA-UOFC in Figure 20 are lower than those of rates at the source nodes in Figure 19. Meanwhile, $U_2(x_2')$ of goodput from FA-UOFC increases, yet $U_2(x_2')$ from NE-OFC decreases. We calculate two indexes of utility fairness, 0.7 and 0.86, according to (29) for NE-OFC and FA-OFC, respectively. It demonstrates that better

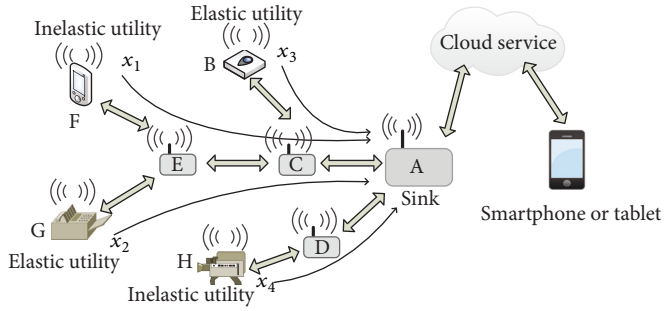


Figure 17: The network topology for one sink.

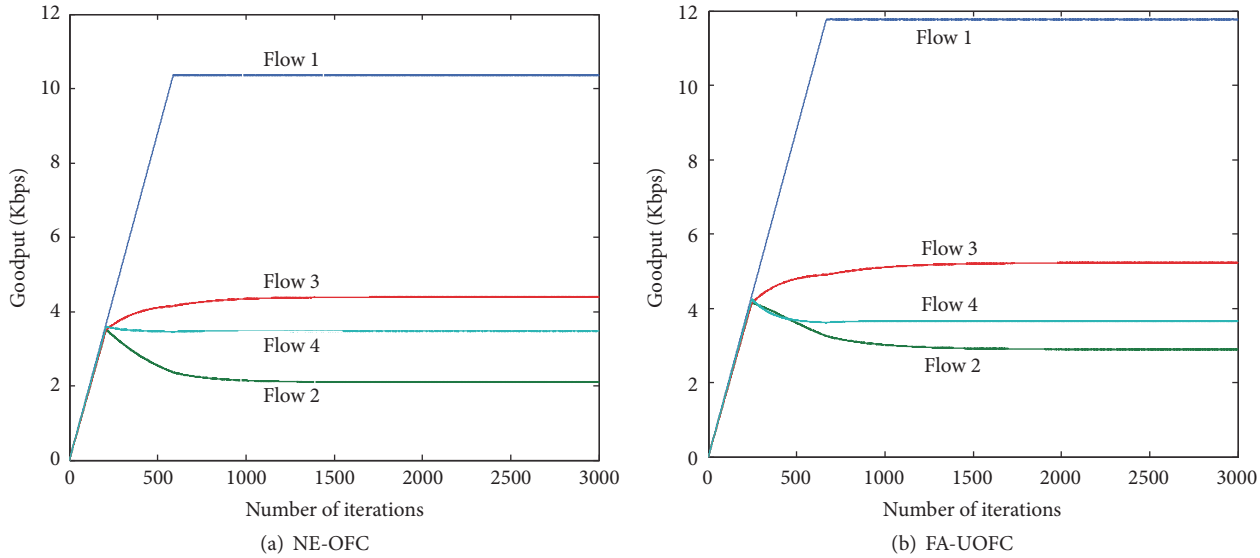


Figure 18: Goodput at sink.

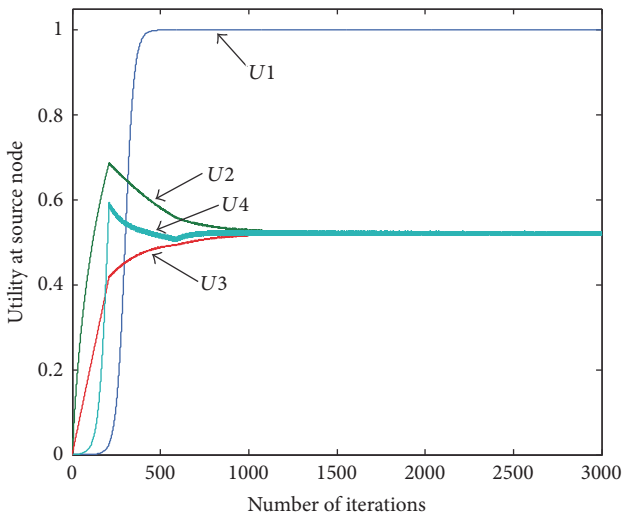
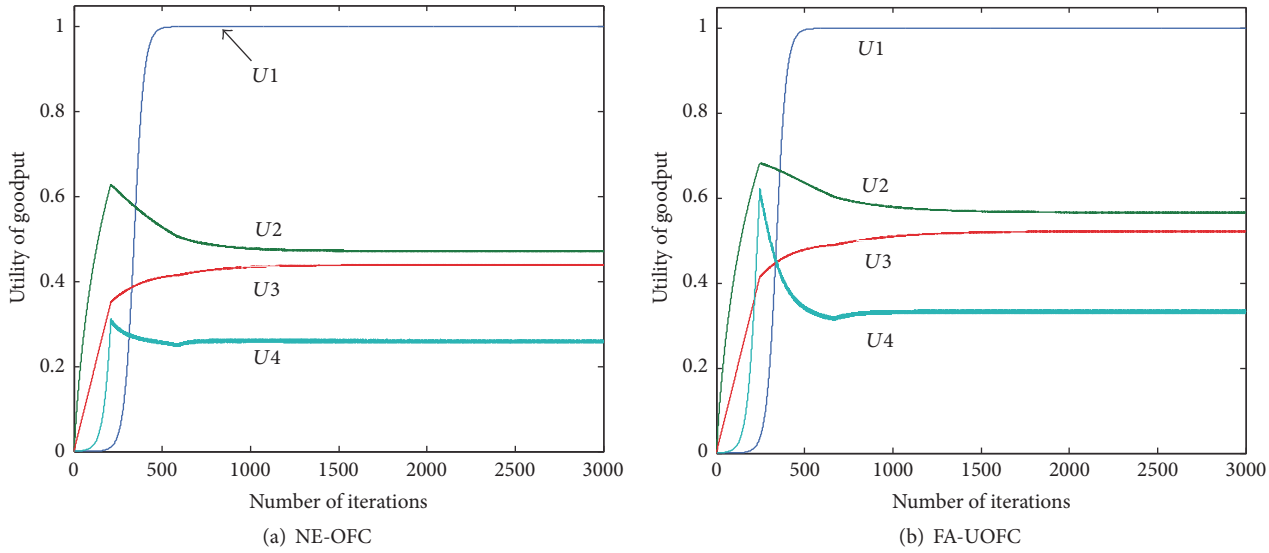


Figure 19: Utility of flow rate at source in NE-OFC.

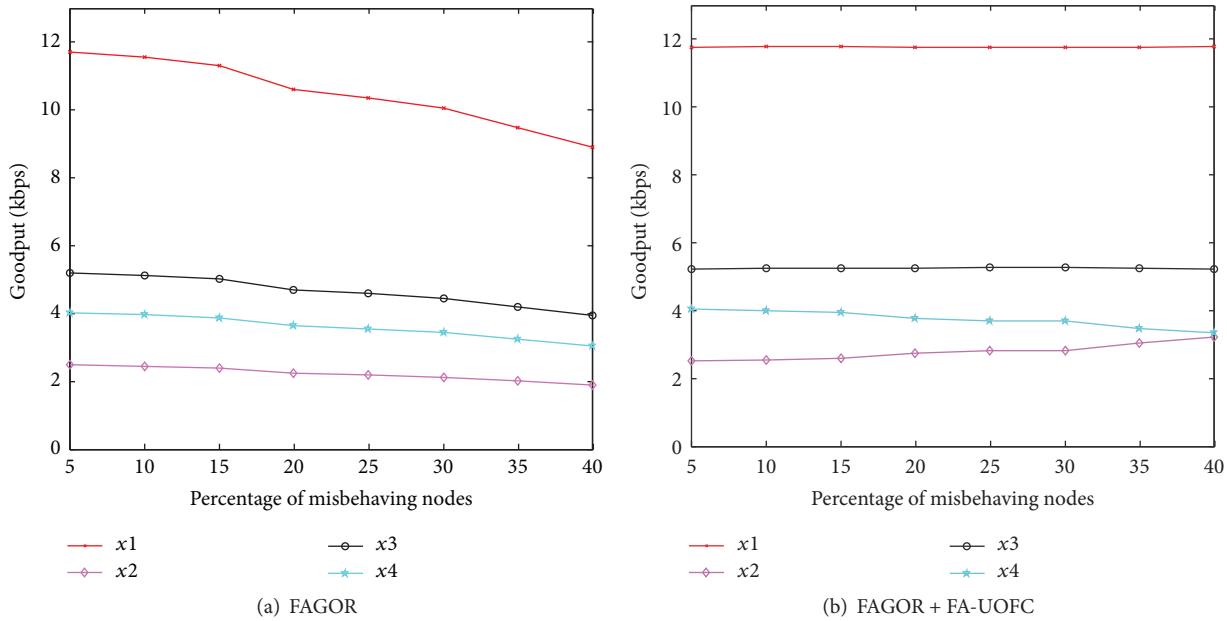
utility fairness is attained among flows by FA-UOFC. Our proposed algorithm effectively adjusts the resource allocation by explicitly taking into account the faulty effects in utility functions and constraints. Clearly, the network performance under misbehaving nodes is improved by our proposed FA-UOFC algorithm through both better utility fairness and higher effective throughput.

7.3. The FAGOR Protocol Combined with FA-UOFC Algorithm. In the following, we investigate the performance of our proposed FAGOR protocol combined with FA-UOFC algorithm for WSNs in adversarial environments. The proposed FAGOR + FA-UOFC scheme is benchmarked against the scheme with only FAGOR which does not employ any optimal flow control algorithm. Figures 21 and 22 plot the goodputs and the goodputs' utilities obtained by FAGOR and FAGOR + FA-UOFC while increasing the percentage of misbehaving nodes in the network from 5% to 40%. Clearly, our proposed method significantly outperforms FAGOR in terms of the goodputs and goodputs' utilities obtainable under a varied percentage of misbehaving nodes. The benefit of our proposed method over FAGOR increases as the number of misbehaving nodes increases. The result demonstrates that the FA-UOFC complements secure routing and alleviates the performance degradation caused by the misbehaving nodes along the routing paths.



(a) NE-OFC (b) FA-UOFC

Figure 20: Utility of goodput.



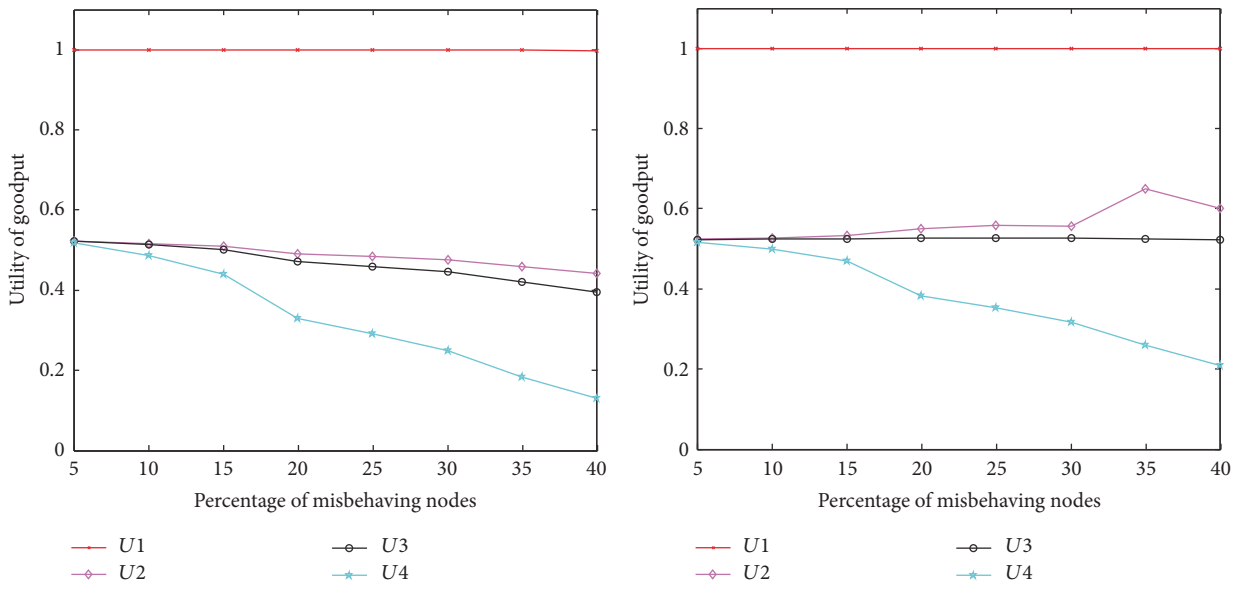
(a) FAGOR (b) FAGOR + FA-UOFC

Figure 21: Goodput at sink.

We also take a closer look at Flow 2 and Flow 3 in Figure 22. As the number of the misbehaving nodes increases, the goodputs' utilities of Flow 2 and Flow 3 in our scheme increase, whereas they decrease in FAGOR. Accordingly, our scheme achieves higher goodputs' utilities for Flow 2 and Flow 3 than FAGOR. This is due to the source nodes in our scheme, which are able to compensate for faulty nodes in the allocation of traffic based on the real performance requirements of services and which can achieve utility fairness among the goodputs.

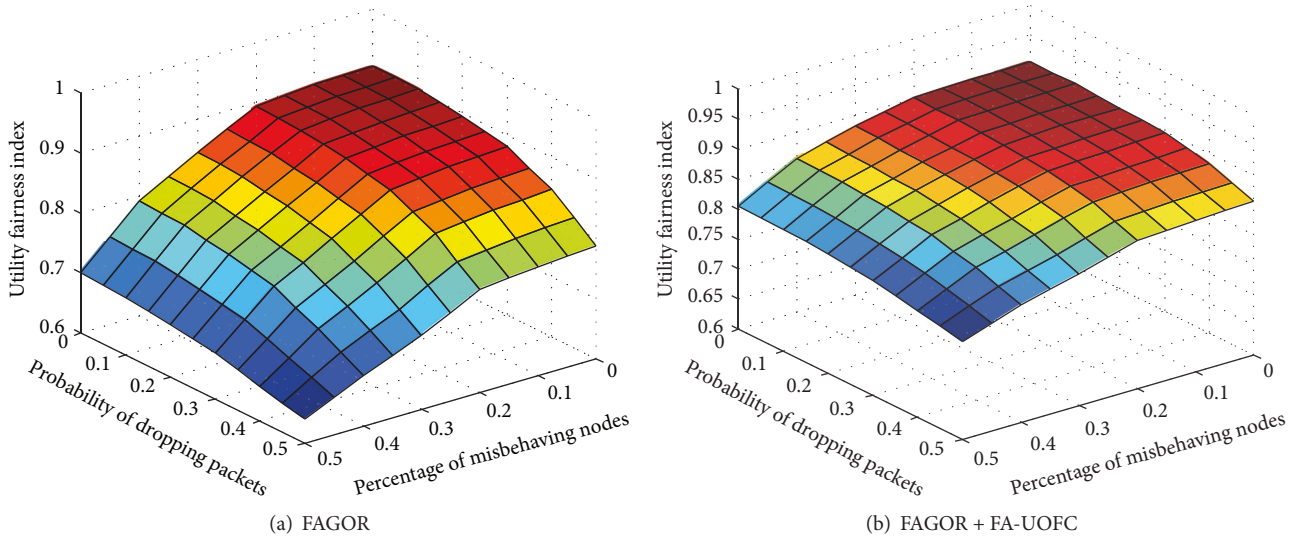
To demonstrate the fairness of FAGOR and FAGOR + FA-UOFC, we point to the variation of $f(x)$ in (29). With various values for the percentage of misbehaving nodes p_1 and the probability of dropping packets p_2 in Figure 23, our proposed scheme can be seen to achieve a higher degree of utility fairness in terms of utility fairness index $f(x)$ for goodput than the FAGOR scheme. This is because our proposed scheme explicitly takes into account the loss feature of faulty nodes and embodies the utility fairness objectives in the utility function that are concerned with the goodputs.

For a sequence of networks with decreasing impact with misbehaving nodes, we can see in Figure 23 that the utility fairness index converges to 0.92. As discussed in Section 6, the rate allocation and utility fairness in our scheme converge to those of the corresponding lossless networks when the ratios of nodes' faulty activities drop to zero. Figure 23



(a) FAGOR (b) FAGOR + FA-UOFC

Figure 22: Utility of each flow.



(a) FAGOR (b) FAGOR + FA-UOFC

Figure 23: Utility fairness index.

shows the trends of utility fairness for goodput in adversarial environments.

8. Conclusion

In this paper, we studied the problem of routing and rate control for multiple city services over wireless sensor networks in the presence of misbehaving nodes whose effect can be characterized statistically. We presented methods for each sensor to probabilistically characterize the impact of a variable fault. To address how to maintain an acceptable level of network performance degradation, we utilized fault activity information in the next-hop selection of each sensor and incorporated this information into the rate-control algorithm for data sources. An improved, fault-aware version of the routing algorithm FAGOR is proposed, and we explicitly added fault activity information into the routing metric. We formulated resource allocation for multiple services as a lossy network flow optimization problem using relaxed utility functions. In addition, we developed a distributed rate-control algorithm called FA-UOFC which can achieve the lossy utility fairness among sources with different traffic types. Through comprehensive performance comparisons, we demonstrate that FAGOR protocol achieves a better performance with an acceptable overhead and that FA-UOFC algorithm achieves a higher effective utility and better utility

fairness when various misbehaving nodes exist in a WSN. Finally, we show that our proposed FAGOR protocol combined with FA-UOFC algorithm proves effective in improving effective utility and utility fairness compared to the scheme with only FAGOR protocol.

Even through the development of our research is based on the wireless sensor network setting, the framework can generally be extended to other energy-constrained wireless ad hoc network models. In the future, mobility aspects can be considered in order to model more realistic wireless networks in smart cities. We also plan to model smart malicious behaviors and study their effects on data delivery.

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 National Natural Science Foundation of China (Grants nos. 61373154, 61672239, and 61632012) and Shanghai High Technology Field Project (Grant no. 16511101400).

References

[1] F. Sanchez-Rosario, D. Sanchez-Rodriguez, J. B. Alonso-Hernandez et al., "A low consumption real time environmental monitoring system for smart cities based on ZigBee wireless sensor network," in *Proceedings of the 11th International Wireless Communications and Mobile Computing Conference, IWCMC 2015*, pp. 702–707, August 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] J. Xu, K. Wang, C. Wang et al., "Byzantine fault-tolerant routing for large-scale wireless sensor networks based on fast ECDSA," *Tsinghua Science and Technology*, vol. 20, no. 6, Article ID 7350015, pp. 627–633, 2015.

[4] B. Zhang, Z. H. Huang, and Y. Xiang, "A novel multiple-level trust management framework for wireless sensor networks," *Computer Networks*, vol. 72, pp. 45–61, 2014.

[5] I. M. Atakli, H. Hu, Y. Chen, W. Ku, and Z. Su, "Malicious node detection in wireless sensor networks using weighted trust evaluation," in *Proceedings of the Spring Simulation Multiconference (SpringSim '08)*, pp. 836–843, April 2008.

[6] 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.

[7] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 5, pp. 1198–1209, 2015.

[8] C. M. Ahmed, S. Adepu, and A. Mathur, "Limitations of state estimation based cyber attack detection schemes in industrial control systems," in *Proceedings of the 2016 Smart City Security and Privacy Workshop, SCSP-W 2016*, pp. 6–10.

[9] J. Wu, K. Ota, M. Dong, and C. Li, "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities," *IEEE Access*, vol. 4, pp. 416–424, 2016.

[10] A. S. Lal and R. Nair, "Region authority based collaborative scheme to detect Sybil attacks in VANET," in *Proceedings of the International Conference on Control, Communication and Computing India, ICCC 2015*, pp. 664–668, November 2015.

[11] K. Zeng, J. Yang, and W. Lou, "On energy efficiency of geographic opportunistic routing in lossy multihop wireless networks," *Wireless Networks*, vol. 18, no. 8, pp. 967–983, 2012.

[12] B. Karp and H. T. Kung, "GPSR: greedy Perimeter Stateless Routing for wireless networks," in *Proceedings of the MobiCom*, pp. 243–254, Boston, Mass, USA, 2000.

[13] I. A. Umar, Z. M. Hanapi, A. Sali, and Z. A. Zulkarnain, "A forwarding strategy for DWSIGF routing protocol," in *Proceedings of the 5th International Conference on IT Convergence and Security, ICITCS 2015*, August 2015.

[14] L. Cheng, J. Niu, J. Cao, S. K. Das, and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1864–1875, 2014.

[15] 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 2014*, pp. 975–982, October 2014.

[16] I. Al-Anbagi, M. Erol-Kantarci, and H. T. Mouftah, "A survey on cross-layer quality-of-service approaches in WSNs for delay and reliability-aware applications," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 525–552, 2016.

[17] G. Hosseinabadi and N. Vaidya, "Selfish misbehavior in scheduling algorithms of wireless networks," in *Proceedings of the 2010 IEEE 29th International Performance Computing and Communications Conference, IPCCC 2010*, pp. 214–221, December 2010.

[18] M. Tahir and S. K. Mazumder, "Delay constrained optimal resource utilization of wireless networks for distributed control systems," *IEEE Communications Letters*, vol. 12, no. 4, pp. 289–291, 2008.

[19] Y. Li, M. Chiang, A. R. Calderbank, and S. N. Diggavi, "Optimal rate-reliability-delay tradeoff in networks with composite links," in *Proceedings of the IEEE INFOCOM 2007: 26th IEEE International Conference on Computer Communications*, pp. 526–534, May 2007.

[20] W. H. Wang, M. Palaniswami, and S. H. Low, "Application-oriented flow control: fundamentals, algorithms and fairness," *IEEE/ACM Transactions on Networking*, vol. 14, no. 6, pp. 1282–1291, 2006.

[21] M. Chaqfeh, N. Mohamed, I. Jawhar, and J. Wu, "Vehicular cloud data collection for Intelligent Transportation Systems," in *Proceedings of the 3rd Smart Cloud Networks and Systems, SCNS 2016*, December 2016.

[22] J. Tang, W. P. Tay, and T. Q. S. Quek, "Cross-layer resource allocation with elastic service scaling in cloud radio access network," *IEEE Transactions on Wireless Communications*, vol. 14, no. 9, pp. 5068–5081, 2015.

[23] P. Spachos, D. Toumpakaris, and D. Hatzinakos, "QoS and energy-aware dynamic routing in wireless multimedia sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '15)*, pp. 6935–6940, London, UK, June 2015.

[24] J. Luo, D. Wu, C. Pan, and J. Zha, "Optimal Energy Strategy for Node Selection and Data Relay in WSN-based IoT," *Mobile Networks and Applications*, vol. 20, no. 2, pp. 169–180, 2015.

[25] X. Kang and Y. Wu, "Incentive Mechanism Design for Heterogeneous Peer-to-Peer Networks: A StackelbergGame Approach," *IEEE Transactions on Mobile Computing*, vol. 14, no. 5, pp. 1018–1030, 2015.

[26] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[27] R. Mitchell and I.-R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Transactions on Reliability*, vol. 62, no. 1, pp. 199–210, 2013.

[28] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proceedings of the IEEE INFOCOM 2007: 26th IEEE International Conference on Computer Communications*, pp. 1307–1315, May 2007.

[29] W. Wang, M. Chatterjee, and K. Kwiat, "Coexistence with malicious nodes: A game theoretic approach," in *Proceedings of the 2009 International Conference on Game Theory for Networks, GameNets '09*, pp. 277–286, May 2009.

[30] 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.

[31] M. Zorzi and R. R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: energy and latency performance," *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 349–365, 2003.

[32] D. Wu, J. Luo, R. Li, and A. Regan, "Geographic load balancing routing in hybrid vehicular ad hoc networks," in *Proceedings of the 14th IEEE International Intelligent Transportation Systems Conference (ITSC '11)*, pp. 2057–2062, IEEE, Washington, DC, USA, October 2011.

[33] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, "Location verification and trust management for resilient geographic routing," *Journal of Parallel and Distributed Computing*, vol. 67, no. 2, pp. 215–228, 2007.

[34] 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. 206–217, 1997.

[35] 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.

[36] Y. Xue, L. I. Baochun, 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, 2006.

[37] S. Eswaran, A. Misra, F. Bergamaschi, and T. La Porta, "Utility-based bandwidth adaptation in mission-oriented wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 8, no. 2, article no. 17, 2012.

[38] 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.

[39] P. Hande, S. Zhang, and M. Chiang, "Distributed rate allocation for inelastic flows," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1240–1253, 2007.

[40] A. Boukerche, H. H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 96–101, 2008.

[41] L. Tan, X. Zhang, L. L. H. Andrew, S. Chan, and M. Zukerman, "Price-based max-min fair rate allocation in wireless multi-hop networks," *IEEE Communications Letters*, vol. 10, no. 1, pp. 31–33, 2006.

[42] R. Fonseca, O. Gnawali, K. Jamieson, and P. Levis, "Four-bit wireless link estimation," in *Proceedings of the HotNets VI*, 2007.

[43] K. Zeng, W. Lou, J. Yang, and D. R. Brown III, "On throughput efficiency of geographic opportunistic routing in multihop wireless networks," *Mobile Networks and Applications*, vol. 12, no. 5-6, pp. 347–357, 2007.

[44] K. Zeng, K. Govindan, D. Wu, and P. Mohapatra, "Identity-based attack detection in mobile wireless networks," in *Proceedings of the IEEE INFOCOM 2011*, pp. 1880–1888, April 2011.

[45] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the WoWMoM 2006: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 564–568, June 2006.

[46] S. Yang, C. K. Yeo, and B.-S. Lee, "Toward reliable data delivery for highly dynamic mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 1, pp. 111–124, 2012.

[47] 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.

[48] Z. Cao and E. W. Zegura, "Utility max-min: an application-oriented bandwidth allocation scheme," in *Proceedings of the IEEE 18th Annual Joint Conference of Computer and Communications Societies (INFOCOM '99)*, vol. 2, pp. 793–801, New York, NY, USA, March 1999.

[49] R. Jain, D. Chiu, and W. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," Tech. Rep., 1984.

[50] "Chipcon Inc, CC2420, True single-chio 2.4 GHz IEEE 802.15.4/ZigBee RF transceiver with MAC support," http://www.chipcon.com.