IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 17 August 2022, accepted 12 October 2022, date of publication 19 October 2022, date of current version 26 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3216066

RESEARCH ARTICLE

Fault-Tolerant Ad Hoc On-Demand Routing Protocol for Mobile Ad Hoc Networks

DUC N. M. HOANG[1], (Graduate Student Member, IEEE), JONG MYUNG RHEE[2], (Member, IEEE), AND SANG YOON PARK[1], (Member, IEEE)

[1]Department of Electronic Engineering, Myongji University, Yongin 17058, South Korea
[2]Department of Information and Communications Engineering, Myongji University, Yongin 17058, South Korea

Corresponding author: Sang Yoon Park (sypark@mju.ac.kr)

This work was supported by the National Research Foundation of Korea (NRF) funded by the Korean Government (MSIT) under Grant 2020R1A2B5B02002201 and Grant 2021R1F1A1050040.

ABSTRACT Mobile ad hoc networks (MANETs) are particularly suited for scenarios that demand rapid deployment of a communication system without any existing network resources. For instance, a MANET can facilitate the intercommunication process between members of a rescue party in a natural disaster, where the underlying routing protocol is crucial to maintaining the dissemination capability of data-critical packets. However, the backbone of every MANET, i.e., their routing protocol, is limited by the communication range of nodes, their high-speed mobility, and the capacity constraints of energy. This study proposed a fault-tolerant ad hoc on-demand routing protocol (FT-AORP) that relies on these characteristics of MANET nodes to determine reliable paths for data transmission. Subsequently, two of the discovered paths were used to transmit the duplicates of an original data packet to maximize fault tolerance. Further, using the OMNeT++ network simulator, the performance of the proposed system was evaluated through extensive simulation experiments against three simulation parameters: the number of network nodes, node speed, and data packet sending rate. The simulation results demonstrated that FT-AORP greatly improved the packet delivery ratio, reduced end-to-end delay, and maintained a higher residual energy level of the transmission path, compared to other baseline routing protocols.

INDEX TERMS Mobile ad hoc network, fault tolerance, network mobility, on-demand routing protocol.

I. INTRODUCTION

A Mobile ad hoc network (MANET) is a wirelessly interconnected class of networks where nodes can freely move and communicate directly with any nearby neighbors. Owing to this mobility characteristic, MANET is normally a self-configuring and infrastructure-less network and thus, can be dynamically formed under any topology [1]. However, there should not be any centralized infrastructure in a MANET. In contrast to the infrastructure-based wireless network, where the deployment of administering devices, e.g., base stations or access points, is required for the network operation, each node in a MANET must be able to send, receive, and relay network packets [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Bijoy Chand Chand Chatterjee.

Owing to the flexibility in the architecture, MANETs are highly versatile and thus, can be beneficial for a variety of applications [3]. For example, they can be employed by many military units [4], [5], [6] because their rapid deployment does not require any previously installed network resources, thus facilitating the establishment of an information communication system between the soldiers on duty. In addition, MANETs can be exploited for public safety and disaster management [7], [8]. For instance, during natural hazards, existing telecommunication towers may be dysfunctional and an instant installation of a wireless ad hoc communication system is extremely critical for the rescue party to communicate with one another while supporting the endangered victims [9]. Furthermore, the dynamic topology nature of this network type enables the rescuers to change their positions without losing connectivity with the rest of the team [10].

Considering these application areas, MANET routing protocols have been intensively studied in the literature [11], [12] owing to their importance in deciding the successful operation of a MANET system. However, despite the ease of the establishment process, MANET routing protocols are uniquely presented with many challenges [3], [13]. First, owing to the limited range of radio communication links, nodes within the network must maintain multi-hop paths between one another [14], [15]. In addition, as the nature of MANET is typically characterized by numerous properties, MANET routing protocols must be designed to address them upon discovering the paths. A few examples are limited battery capacity [16], security [17], neighboring signal strength [18], link reliability [19], or their combinations [20], [21]. Moreover, following the determination of the paths, a fault-tolerant transmission strategy is required to guarantee that critical data packets are sent to the destination without substantial delays. To the best of the authors' knowledge, only a few of the proposed routing protocols focus on both an efficient routing scheme and a fault-tolerant capability for packet transmissions.

This study proposed a fault-tolerant ad hoc on-demand routing protocol, referred to as *FT-AORP*. It provides reliable transmission for the deployment of MANETs in scenarios where safety-critical information must be guaranteed to be successfully exchanged amongst nodes in the network. The main contributions of this study are as follows.

- A path selection strategy employing three different routing metrics relevant to MANET characteristics: node mobility, radio signal strength measurement, and energy usage rate, was proposed to identify the optimal paths to the destination for data transmission. These routing metrics can be easily collected without requiring any supplemental sensor devices.
- We developed a simple multipath discovery scheme that returns, if possible, more than one path towards the destination for the requesting source node. Based on these determined paths, the source node can select the two desired ones using the aforementioned selection strategy. Then, we introduced a fault-tolerant transmission technique that involves duplicating the important data packets and transmitting them using two separate node-disjointed paths. This fault-tolerant design ensured that packets were delivered successfully even if transmission issues occurred in one path.
- We implemented the proposed protocol as a simulation framework using OMNeT++ [22] and modeled the evaluation testbed as close to the real-world environment as possible with various configurable simulation parameters. Moreover, by employing several evaluation metrics, the better performance of the proposed protocol compared to other revisited routing protocols was demonstrated in many testing scenarios.

The rest of this paper is organized as follows. In Section II, certain relevant state-of-the-art studies that have addressed the MANET routing problem are reviewed. Section III presents the problem formulation through a system model and introduces the proposed routing metrics for the path selection issue. In Section IV, the routing protocol is described in detail, including the route request, route reply, and node discovery schemes. The performance of the proposed routing protocol indicated by simulation results is evaluated in Section V. Finally, the conclusions are presented in Section VI.

II. RELATED WORK

A. FUNDAMENTAL ROUTING PROTOCOLS

Routing schemes for MANETs have been extensively studied in the literature. Pioneering routing protocols can be classified into two main categories: proactive and reactive protocols [23]. Several well-known proactive protocols are destination-sequenced distance vector (DSDV) [24], global state routing (GSR) [25], and optimized link state routing (OLSR) [26]. Meanwhile, certain popular reactive routing solutions that have been proposed to reduce the overheads of proactive approaches are ad hoc on-demand distance vector [27], dynamic source routing (DSR) [28], and temporally ordered routing algorithm (TORA) [29]. Such protocols have mostly been adapted from traditional routing schemes for wired networks with minor modifications for wireless networks. Consequently, they were originally designed to select the route with the minimum hop count to transmit the packets through. Although this hop count metric is straightforwardly useful in cabled networks as the network components are often static, MANETs are more dynamic and the number of intermediate nodes between the source and destination is thus highly likely to change over time.

B. STATE-OF-THE-ART ROUTING METRICS

Considering the limits of the hop count, many studies have incorporated different routing metrics into MANET routing protocols. Taha et al. [16] proposed an energy-efficient multipath routing protocol that adopted a fitness function as an optimization method to select the best route based on two criteria: the number of intermediate nodes and their remaining energy level. Although this scheme can prolong the network lifetime, the power consumption rate alone appeared relatively insufficient when considering aggressive scenarios with more factors affecting the connection links between network nodes. For instance, when an arbitrary node is in an isolated area, it is certainly not an ideal next hop for the entire route although it might have sufficient energy supply. Therefore, more measures are being exploited to design routing protocols.

For example, Chen et al. [30] proposed a topological change adaptive ad hoc on-demand multipath distance vector (TA-AOMDV) routing protocol that can adapt to the aggressively dynamic nature of mobile networks. Through the combination of individual node information (i.e., residual energy, queue length, and current bandwidth) as route selection metrics with the probability of link stability between nodes, the proposed scheme exhibited better performance in many notable metrics such as packet delivery ratio and

end-to-end delay. However, while the protocol is a prospective choice for applications in high-speed MANETs with quality-of-service (QoS) constraints, it may not be suitable for life-critical systems as its packet delivery rate performance is not consistently satisfactory as the network nodes move chaotically fast (e.g., 30 m/s and higher).

In a similar manner, Dhananjayan and Subbiah [31] proposed a trust-aware ad hoc routing protocol using stability factors such as energy level, mobility, and RSSI-based distance measurement from each node's accumulated logging information to select the optimal next hop from surrounding neighbors. Simulation results showed that this reputation-based protocol achieved high throughput, improved packet delivery rate, and low end-to-end delay. However, the log collection and examination process performed by each node might demand enormous computational costs and subsequently high-power consumption, which is normally limited for resource-constrained MANETs.

More recently, Sirmollo and Bitew [32] proposed a mobility-aware routing scheme for MANETs. This protocol takes multiple factors into consideration, such as the speed of the nodes, the relative distance between them, and their residual energy level, to choose the best nodes to forward the packets to during the route request and route discovery phases. Simulation results also demonstrated the superior performance over other routing protocols. However, the proposed scheme mainly relies on the calculation of the node distance, which requires an accurate positioning system. In reality, this might not always be possible, especially when it comes to indoor contexts.

C. FAULT-TOLERANT ROUTING PROTOCOLS

Regarding fault tolerance in MANETs, Nsaif et al. [33] introduced an approach referred to as seamless routing for wireless ad hoc networks (SRAD). Here, each pair of nodes had two link-disjointed paths, which were used to transmit two redundant frame copies to the destination such that zero-recovery time was achieved in the case where one of the operating paths fails. Instead of using the shortest paths, the path selection is based on its bit error rate (BER) measurement. However, the process to calculate the BER for the links is unclear and the proposed protocol has been evaluated for a benign scenario only (e.g., the network containing only 21 nodes moving at 10 m/s).

Song et al. [34] proposed several topology control algorithms employing the Kalman filter, which can anticipate the movement tendency of other surrounding nodes and consequently adjust its movement to maintain wireless links with other nodes. In addition, they are localized algorithms wherein no more than two hops' information is required. Simulation results against node velocity and the number of cluster members showed that one of the proposed schemes can effectively restore connectivity while maintaining a minimal deviation from the original task-based direction. However, these proposed algorithms require the network nodes to change their movement patterns, which may not always be plausible owing to the highly unpredictable MANET mobility [35].

TABLE 1. Commonly used notation.

Notation	Definition
v	an arbitrary node
p_{ij}	a path between nodes v_i and v_j
$N^{(v)}$	the set of neighbor nodes of node v
$\Phi^{(v_i)}$	the node routing measure of node v
Φ_m	the mobility indicator metric
Φ_s	the neighboring signal strength metric
Φ_e	the energy level metric
$\Theta^{(p)}$	the path routing measure for path p
l	the path length
ζ	the safety threshold of battery level

Recently, Srilakshmi et al. [36] proposed a secure optimization routing protocol that simultaneously addresses the energy and communication issues of MANETs. In detail, there are certain cluster heads in the network that are in charge of routing the packets, and they are chosen based on their calculated trust values. However, the trust values are mainly derived from the transmission duration, which is partially susceptible to the dynamic nature of MANETs. Interestingly, Pattnaik et al. [37] presented a multipath routing scheme for MANETs, which makes use of De Casteljau's algorithm with the Bezier curve for the mobility awareness of multiple speed levels. The optimal routing path for data transmission is then selected based on various factors. Routing in obstacle-ridden environments is certainly a promising research topic. However, it is outside of the scope of this work and can be of great potential for our future research directions.

In addition, Naseem et al. [38] proposed a novel energy-efficient routing protocol for MANETs that also employs manifold routing criteria, such as the number of hops, the round-trip time, and the remaining energy level, to discover the optimal data transmission path. Additionally, it is also a multipath-enabled routing scheme that aims to offload the data transmission among various paths for load balancing. In contrast, in our work, the discovered paths are used to simultaneously send data packets to the desired destination node. As a result, we can guarantee the maximization of fault tolerance for MANETs. Likewise, Sarhan and Sarhan [39] employed the elephant herding optimization algorithm to choose the routing paths with optimal residual energy in an on-demand multipath routing protocol called EHO-AOMDV. Then, various paths are also used for the data transmission's load balancing between the source and destination nodes. The actual number of packets assigned to a path will be determined using the minimum energy level of its intermediate nodes, which ensures that the path with higher residual energy will be responsible for relaying more data packets.

III. PROBLEM STATEMENT

In this section, we describe the general system model, formulate the routing problem, and introduce our proposed routing

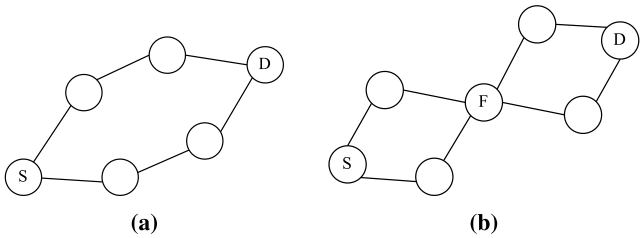


FIGURE 1. Comparison between (a) node-disjointed and (b) link-disjointed paths.

metrics as part of the routing protocol. The commonly used notation in this paper is shown in Table 1.

A. SYSTEM MODEL AND PROBLEM FORMULATION

- A *path* p_{ij} consisting of l nodes is denoted as $p_{ij} = [v_i, \ldots, v_j]$, where $\|p_{ij}\| = l$ with $\|\cdot\|$ being the cardinality of a set;
- For two adjacent nodes, e.g., nodes v_i and v_{i+1}, a bidirectional link is denoted as $(v_i, v_{i+1}) \in E$;
- There should be k possible paths between v_i and v_j, they collectively form a *route* $r_{ij} = \left[p_{ij}^{(1)}, p_{ij}^{(2)}, \ldots, p_{ij}^{(k)}\right]$, where $\|r_{ij}\| = k$.

To provide reliability for in-network data communication, a node should maintain information on alternative paths in addition to the main path [40]. Therefore, in this work, we aim to develop a multipath routing protocol that discovers more than one path (i.e., $k > 1$) from the source to the destination node. This design strategy can cope with potential link breakages due to network mobility and unstable wireless medium. Thus, $k = 2$ being set to a larger value may cause excessive protocol overhead but show no significant improvement [41].

Next, to maximize the fault-tolerant capability, discovered paths should be node-disjointed [42], [43] instead of simply link-disjointed. This is because, for two node-disjointed paths, there is no common node, whereas link-disjointed paths can share one or more intermediate nodes, as depicted in Fig. 1. In this example, following the node-disjointed design scheme, the routing protocol can avoid the situation where a single point of failure occurs at the single common node of two paths, which is denoted as node F in Fig. 1b. In the proposed system model, this implies that $(p_{ij}^{(1)}, p_{ij}^{(2)}) \in r_{ij} : p_{ij}^{(1)} \cap p_{ij}^{(2)} = \{v_i, v_j\}$ as $\|r_{ij}\| = k = 2$ for every pair of source v_i and destination node v_j.

In addition, as this study considered $k = 2$ paths to be used to transmit the data packets between the source and destination nodes, an algorithm to select two paths from many possibly discovered paths is required. Therefore, a *routing measure* was introduced for each operating node in the network. In particular, the routing measure for node v at time t is defined as $\Phi^{(v)}(t)$. Recall that as a path p is formed between nodes v_i and v_j, it consists of l intermediate nodes. Thus, the routing measure $\Theta^{(p)}$ for the entire path p is expressed as

$$\Theta^{(p)} = \frac{1}{l} \sum_{v_i \in p} \Phi^{(v_i)}. \tag{1}$$

Definition 1: From many possible paths between nodes v_i and v_j, path p is the optimal path if its routing measure $\Theta^{(p)}$ is the largest one.

Therefore, in the proposed study, the act of selecting the two optimal paths was equal to selecting the two paths with the **two largest routing measures** Θ. In the subsequent sections, we will provide details for the computation process of the routing measure value for nodes and paths, i.e., Φ and Θ respectively.

B. NODE ROUTING MEASURE

In the proposed scheme, when the network nodes are operating, each one computes its own node routing measure Φ at every selected interval. This Φ value is calculated from the information of the current state of the node and its surrounding environment. A node routing measure is composed of three *routing metrics*.

1) Mobility indicator Φ_m;
2) Neighboring signal strength Φ_s;
3) Energy level Φ_e.

The proposed routing metrics can be easily obtained from commercially available wireless products without any additional designated sensors or peripherals. In particular, the mobility indicator suggests the tendency of a node to change its neighbors, neighboring signal strength indicates if a node is within an area of strong wireless signal coverage, and energy level reveals the current energy level of a node and its power consumption rate. Finally, the routing measure Φ of node v is expressed as

$$\Phi^{(v)} = \Phi_m + \Phi_s + \Phi_e. \tag{2}$$

1) MOBILITY INDICATOR

Mobility indicator metric was first proposed in [44] to incorporate the mobility pattern of a node considering changes in its neighboring nodes. A node is deemed more reliable to be part of a transmission link if it tends to stay with a higher number of other surrounding nodes. The mobility indicator $\Phi_m(t)$ for a node v at time t is calculated using

$$\Phi_m(t) = \begin{cases} 0, & \text{if } \|N_t^{(v)}\| = \|N_{t-\Delta t}^{(v)}\| = 0, \\ \sqrt{\dfrac{\|N_t^{(v)} \cap N_{t-\Delta t}^{(v)}\|}{\|N_t^{(v)} \cup N_{t-\Delta t}^{(v)}\|}}, & \text{otherwise,} \end{cases} \tag{3}$$

where $N_t^{(v)}$ (resp. $N_{t-\Delta t}^{(v)}$) denotes the set of neighboring nodes of node v at time t (resp. $t - \Delta t$), and Δt is a sufficiently large sampling period.

Lemma 1: $0 \leq \Phi_m \leq 1$.

Proof: First, it is evident from (3) that, in the case of $\|N_t^{(v)}\| = \|N_{t-\Delta t}^{(v)}\| = 0$, $\Phi_m = 0$. In addition, Φ_m is a square root and therefore, $\Phi_m > 0$. Next, it is apparent that $\|N_t^{(v)} \cap N_{t-\Delta t}^{(v)}\| \leq \|N_t^{(v)} \cup N_{t-\Delta t}^{(v)}\|$ or $\|N_t^{(v)} \cap N_{t-\Delta t}^{(v)}\| / \|N_t^{(v)} \cup N_{t-\Delta t}^{(v)}\| \leq 1$, and the equality holds when $N_t^{(v)} = N_{t-\Delta t}^{(v)}$. Hence, the lemma is proven. □

From Lemma 1, it is apparent that the fewer the changes in the neighbor set at the two different time instances, the larger the value of Φ_m, implying a more reliable node. In other studies, e.g., [45], global positioning system (GPS) devices may be used to compute the mobility of a node based on the relative distance between nodes. However, the GPS fix process may result in large power consumption [46], which is not suitable for mobile nodes powered by on-board batteries.

2) NEIGHBORING SIGNAL STRENGTH

Mobility indicator suggests the change rate in the number of neighboring nodes within a certain amount of time. However, this information alone does not indicate whether the node is currently within a sufficiently close distance to properly receive the radio signal from other transmitting nodes. Therefore, this study introduced the neighboring signal strength metric that employs the received signal strength indicator (RSSI) to show the proximity of a node within the transmission ranges of its neighbors.

As a node receives a packet from one surrounding node, it can retrieve information on the strength level of the signal, from which it successfully receives that packet. In particular, for $\Gamma(v, v_i) < 0$ in dBm as the RSSI value of node v_i's signal measured by the node v, it is known that the closer to 0 the value of Γ, the better the signal. Subsequently, node v builds up a collection of the measured signal levels of its neighbors at time t, denoted as $\alpha = \{(\Gamma(v, v_i)) \mid v_i \in N_t^{(v)}\}$ with $N_t^{(v)} \neq \varnothing$. Then a set β of *RSSI coefficients* is computed using

$$\beta = \left\{ \frac{(\Gamma(v, v_i))^{-1}}{\sum_{v_i \in N_t^{(v)}} (\Gamma(v, v_i))^{-1}} \mid v_i \in N_t^{(v)} \right\} = \left\{ \gamma_{v_i} \mid v_i \in N_t^{(v)} \right\}, \tag{4}$$

where $\gamma_{v_i} = \frac{(\Gamma(v, v_i))^{-1}}{\sum_{v_i \in N_t^{(v)}} (\Gamma(v, v_i))^{-1}}$. Because of the computation of γ_{v_i}, we obtain

$$0 < \gamma_{v_i} \leq 1, \tag{5}$$

and

$$\sum_{v_i \in N^{(v)}} \gamma_{v_i} = 1. \tag{6}$$

Then, the neighboring signal strength metric Φ_s at time t is expressed as

$$\Phi_s(t) = \begin{cases} 0, & \text{if } \|N^{(v)}\| = 0, \\ -\dfrac{\sum_{v_i \in N^{(v)}} \gamma_{v_i} \ln \gamma_{v_i}}{\ln(|\bar{\alpha}| + \|N^{(v)}\|)}, & \text{otherwise}, \end{cases} \tag{7}$$

where $\bar{\alpha}$ is the mean value of set α and $|\cdot|$ denotes the absolute value.

Lemma 2: $0 \leq \Phi_s \leq 1$.

Proof: From (7), for $\|N^{(v)}\| = 0$, $\Phi_s = 0$. Then, from (5), it is clear that $\ln \gamma_{v_i} < 0$ or $-\ln \gamma_{v_i} > 0$. In addition, the denominator given in (7) is always positive for $\|N^{(v)}\| \geq 1$. Owing to these conditions and (5), we obtain $\Phi_s \geq 0$. Next, by applying the *log sum inequality* [47] for the set β of $\|N^{(v)}\|$ positive numbers given in (4) and a set $\{1, 1, \ldots, 1\}$ of the same size, we obtain

$$\begin{aligned} \sum_{v_i \in N^{(v)}} \gamma_{v_i} \ln(\gamma_{v_i}) &= \sum_{v_i \in N^{(v)}} \gamma_{v_i} \ln\left(\frac{\gamma_{v_i}}{1}\right) \\ &\geq \left(\sum_{v_i \in N^{(v)}} \gamma_{v_i} \right) \ln \frac{\sum_{v_i \in N^{(v)}} \gamma_{v_i}}{\sum_{v_i \in N^{(v)}} 1} \\ &= -\ln \|N^{(v)}\|, \end{aligned} \tag{8}$$

for $\sum_{v_i \in N^{(v)}} \gamma_{v_i} = 1$ according to (6). Therefore, it is obvious that $\Phi_s \leq \frac{\ln \|N^{(v)}\|}{\ln(|\bar{\alpha}| + \|N^{(v)}\|)} \leq 1$ and the proof is completed. □

In particular, this study exploited the characteristics of the *entropy* concept [48] to compute the routing metric Φ_s. According to the entropy concept, given a set $X = \{x_1, x_2, \ldots, x_n\}$ satisfying $0 \leq x_i \leq 1$ and $\sum x_i = 1$, the entropy of this set can be computed using $H(X) = -\sum x_i \log x_i$. Regarding the computation of the proposed routing metric, a node obtains a set β of RSSI coefficients from its neighbors' RSSI values, as given in (4). Thus, from conditions (5) and (6), it is obvious that the entropy of β can be calculated, as provided in the numerator of (7).

Remark 1: The entropy value of a set has the following relevant properties, which can be used to describe the relationship between the RSSI values γ_{v_i} collected by a node and its metric Φ_s.

- *Φ_s should be proportional to γ_{v_i}, implying that a small increase or decrease in γ_{v_i} values result in a small increase or decrease in Φ_s, respectively. According to this property, a node obtaining higher RSSI values exhibits a higher Φ_s value, thus, it is more likely to be chosen to be part of a routing path;*
- *Φ_s should be maximal if γ_{v_i} values are equally likely. This implies that if all RSSI values are equally high, the node is in an area with strong signal coverage and therefore becomes an optimal candidate to be included in a routing path. However, there is a case when γ_{v_i} values are equally low and Φ_s still has its maximum value. To overcome this, the denominator $\ln(|\bar{\alpha}| + \|N\|)$ as given in (7) was introduced. With $|\bar{\alpha}|$ being the absolute value of the mean of the RSSI set, this implies that if all the RSSI values are equally small, the Φ_s of the node will be divided by a large value as the absolute value of a non-positive RSSI value is being used. In contrast, if all the RSSI values are equally high, Φ_s will be larger.*

3) ENERGY LEVEL

Assume that a node is able to acquire its battery level at time t, denoted by $E_t^{(v)}$ in Joule (J). The energy level metric is computed as

$$\Phi_e(t) = \begin{cases} 0, & \text{if } E_t^{(v)} < \zeta, \\ \dfrac{E_t^{(v)}}{E_{t-\Delta t}^{(v)}}, & \text{otherwise}, \end{cases} \tag{9}$$

where ζ is a sufficiently small safety threshold to indicate that this node is no longer suited to be involved in the network activity owing to a shortage in power storage.

Lemma 3: $0 \leq \Phi_e \leq 1$.

Proof: First, because the battery level is always non-negative, $\Phi_e \geq 0$ and the equality holds when E_t value is below the given ζ threshold. Then, as it is clear that the battery level at a particular time will always be less than or equal to the previous time, $E_t^{(v)} \leq E_{t-\Delta t}^{(v)}$ or $E_t^{(v)}/E_{t-\Delta t}^{(v)} \leq 1$. The equality holds when the node consumes minimal power, resulting in relatively no change between the two acquisition attempts of battery level, or $E_t^{(v)} = E_{t-\Delta t}^{(v)}$. □

Through the introduction of this metric, this study aimed to calculate the power consumption rate of a node and make decisions accordingly. For example, if the node is quickly drawing power from its battery for network activities such as packet transmission or reception (i.e., $E_t^{(v)} \ll E_{t-\Delta t}^{(v)}$), Φ_e will have a smaller value and this node stands a small chance of being an intermediate hop in a path. Moreover, from (9), if the battery level is less than ζ, this node will be certainly excluded from the path formation, thereby preventing later possible link interruptions owing to power outages.

C. PATH ROUTING MEASURE

Now, recall that path p between two nodes v_1 and v_l comprising l nodes is denoted as $p = [v_1, v_2, \ldots, v_l]$, where $\|p\| = l$. The routing measure for node v_i and path p is given by $\Phi^{(v_i)}$ and $\Theta^{(p)}$, respectively, and by substituting (2) into (1), the following is obtained

$$\Theta^{(p)} = \frac{1}{l}\sum_{v_i \in p} \Phi^{(v_i)} = \frac{1}{l}\sum_{v_i \in p}\left(\Phi_m^{(v_i)} + \Phi_s^{(v_i)} + \Phi_e^{(v_i)}\right). \quad (10)$$

Lemma 4: $0 \leq \Theta^{(p)} \leq 3$.

Proof: First, from Lemmas 1 to 3, it is clear that for every $v_i \in p$, $\Phi^{(v_i)} \geq 0$, thus $\Theta^{(p)} = \frac{1}{l}\sum_{v_i \in p} \Phi^{(v_i)} \geq 0$ because l is also positive. Then,

$$\begin{aligned}
\max \Theta^{(p)} &= \max \frac{1}{l}\sum_{v_i \in p}\left(\Phi_m^{(v_i)} + \Phi_s^{(v_i)} + \Phi_e^{(v_i)}\right) \\
&\leq \frac{1}{l}\sum_{v_i \in p} \max\left(\Phi_m^{(v_i)} + \Phi_s^{(v_i)} + \Phi_e^{(v_i)}\right) \\
&leq \frac{1}{l}\sum_{v_i \in p}\left(\max \Phi_m^{(v_i)} + \max \Phi_s^{(v_i)} + \max \Phi_e^{(v_i)}\right) \\
&= \frac{1}{l}\sum_{v_i \in p}(1+1+1) \\
&= \frac{3\|p\|}{l} \\
&= 3, \qquad (11)
\end{aligned}$$

also from Lemmas 1 to 3 and for $\|p\| = l \neq 0$. Hence, the lemma is proven. □

From Definition 1, the act of selecting the best path is equal to selecting the route with the maximum path measure Θ, i.e., maximizing the constituent routing metrics (i.e., Φ_m, Φ_s, and Φ_e) of each node. Based on this maximization, the chosen path will be the optimal one and have the following characteristics.

Theorem 1: For a path with the maximum Θ value, its intermediate nodes are less likely to change their neighbors.

Proof: From Lemmas 1 and 4, it is evident that one of the conditions for achieving the maximum value of path measure $\Theta^{(p)}$ is that nodes in the path p appear to have few changes in the set of their neighboring nodes. Consequently, the selected path will remain stable over time and there should be a reduction in the number of intermediate link breaks as nodes do not tend to flee from one another. □

Theorem 2: For a path with the maximum Θ value, its intermediate nodes tend to stay in a region with equally distributed strong signal coverage from the neighbor nodes.

Proof: From Lemmas 2 and 4, it can be observed that one of the conditions for achieving the maximum value of path measure $\Theta^{(p)}$ is that nodes in the path p can obtain equally high RSSI values of the radio signal from all the neighbor nodes. This is thoroughly justified in Remark 1. □

Theorem 3: For a path with the maximum Θ value, its intermediate nodes are higher in their current energy level and have slower rates of power consumption.

Proof: From Lemmas 3 and 4, it can be observed that one of the conditions for achieving the maximum value of path measure $\Theta^{(p)}$ is that nodes in the path p appear to be maximized in the battery level. In addition, if nodes appear as consuming energy quickly (i.e., $E_t \ll E_{t-\Delta t}$), it results in reduced Φ_e and subsequently Θ value. □

From (10), it is observed that the routing measure for a path is the summation of the routing metrics of all the nodes in that path, including the source and the destination nodes. However, a node is not required to know the entire network topology to calculate the routing measure for every possible path between itself and the desired destination node. In fact, this computation is distributedly performed by each intermediate hop during the route discovery procedure, which is addressed in the next section.

IV. PROPOSED ROUTING PROTOCOL

In this section, a fault-tolerant ad hoc on-demand routing protocol (FT-AORP) is presented. First, the manner in which the conduction of the route discovery procedure as a source node requires the transmission of a data packet to a specific destination (route information is not yet available) is discussed. Next, after the source node acquires the route information of the destination node inside its routing table, a fault-tolerance scheme of data packet transmission was proposed, wherein two duplicates of the original data packet were sent over the network to guarantee reliable transmission for critical data packets.

A. ROUTE DISCOVERY

The route discovery strategy of FT-AORP is partially based on the well-known ad hoc on-demand distance vector (AODV) routing protocol [27] with certain modifications for

Type (8 bits)	U (1 bit)	Hop Count (8 bits)	RREQ ID (8 bits)
Destination IP Address (32 bits)			
Destination Sequence Number (32 bits)			
Originator IP Address (32 bits)			
Originator Sequence Number (32 bits)			
Routing Measure (32 bits)			

FIGURE 2. Structure of the RREQ packet with the newly added "Routing Measure" field.

the multipath routing purpose. Similar to the AODV protocol, there are two phases from the point the source node initiates the route discovery until it is responded to with the requested route: route request (RREQ) and route reply (RREP). In general, the route request process floods the RREQ packets into the network and as they reach the desired destination node, it sends back the RREP packets to the source node via unicast.

1) ROUTE REQUEST

RREQ is a broadcast packet that is sent by a source node if it does not know a route to a destination. Thus, the source node wants to send a data packet to a certain node and it searches its routing table for an entry that contains relevant information regarding the destination node. As the node finds nothing, it starts the route request process by broadcasting the RREQ packet. The format of the RREQ packet is shown in Fig. 2. It should be noted that all the packet structures proposed in this paper are for illustrative purposes only and are not byte aligned.

As evident from Fig. 2, the RREQ packet defines the following fields:

- *Type* is the type of FT-AORP control packets and RREQ packet is type number 1;
- *U* is the unknown sequence number flag, indicating that the destination sequence number is unknown;
- *Hop Count* is the number of intermediate hops from the originator node of an RREQ packet to the node currently handling it. This value is incremented for every node that the RREQ packet passes;
- *RREQ ID* is a monotonically increasing number that, coupled with the originator IP address, uniquely identifies an RREQ packet. *RREQ ID* number is incremented by one whenever an RREQ packet is created;
- *Destination IP Address* is the IP address of the destination node of the route that is being discovered;
- *Destination Sequence Number* is the most recently received sequence number by the originator for any route to the destination;
- *Originator IP Address* is the IP address of the node that started the route discovery and initiated the route request;
- *Originator Sequence Number* is the current sequence number to be used for the route entry to the initiator of the route request;
- *Routing Measure* is the accumulated routing measure value Φ of all the nodes from the originator node to the current node. The routing measure of a node is computed using (2).

Before eventually sending the RREQ packet, the source node must encapsulate its RREQ-identifying information inside. Thus, it increments its own *RREQ ID* number by one and embeds this value inside the *RREQ ID* field of the packet. Later, as other nodes receive this broadcasted RREQ packet, they can check whether it has received the earlier copy before by examining both the *RREQ ID* and *Originator IP Address* fields. In addition, each node maintains a sequence number such that other nodes can check for this information by examining the *Originator Sequence Number* field to ensure that it is updated with the originator node regarding the routing control packets. The route request process performed by the source node is described in Fig. 3.

If a node receives an RREQ packet, it (with the exception of the destination node), determines whether it has received an earlier RREQ packet with the same *RREQ ID* and *Originator IP Address* or not. If it has, the node simply discards the newly arrived RREQ packet to avoid unnecessary dissemination of the RREQ packet all over the network. However, if the node cannot find the RREQ packet's identity inside its record, it increases the *Hop Count* field by one, adds its own routing measure value to the accumulated *Routing Measure*, and rebroadcasts the RREQ packet. In contrast to the original AODV protocol, if the destination node receives RREQ packets, it does not check for any duplications. Instead, it maintains a record of every arrived RREQ packet inside its routing table to enable multipath routing. Subsequently, the destination node responds to each RREQ packet with an RREP packet, which begins the route reply phase.

2) ROUTE REPLY

As the destination node receives an RREQ packet, it immediately generates an RREP packet; thus, the number of the RREQ packets possibly reaching the destination is equal to the number of paths between the source and destination nodes. In contrast to the broadcasted RREQs, the RREP responses are performed via unicast as the destination and intermediate nodes already learn the reverse route from the destination back to the source node during the route request period. The format of the RREP packet is shown in Fig. 4.

Specifically, the RREP packet defines the following fields:

- *Type* is the type of FT-AORP control packets and RREP is type number 2;
- *Hop Count* is similar to that defined in the RREQ packet's structure;
- *Destination IP Address* is the IP address of the destination node of the route. As the RREP packet is always created by the destination node, this field should contain the IP address of the destination itself;
- *Destination Sequence Number* is similar to that defined in the RREQ packet, and its purpose is to ensure that other nodes are up-to-date regarding its routing activities;

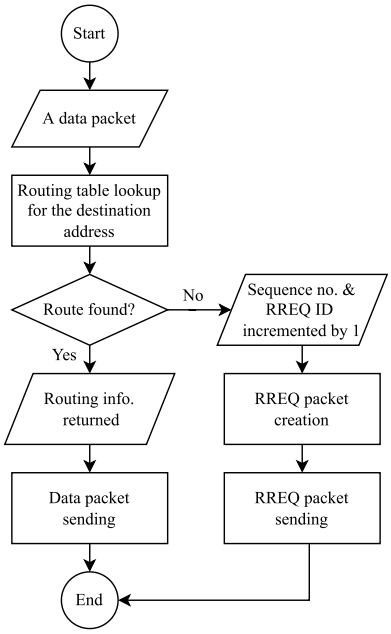


FIGURE 3. Flowchart of creating and sending an RREQ packet.

Type (8 bits)	Hop Count (8 bits)
Destination IP Address (32 bits)	
Destination Sequence Number (32 bits)	
Originator IP Address (32 bits)	
Routing Measure (32 bits)	

FIGURE 4. Structure of the RREP packet with the newly added "Routing Measure" field.

- *Originator IP Address* is the IP address of the node that started the route discovery and initiated the route request;
- *Routing Measure* is similar to that defined in the RREQ packet's structure, except that it is added up from the destination back to the source node. This is because the nodes should have the latest possible information regarding routing measure values of the path.

Analogous to the creation of RREQ packets, the destination node also attaches the necessary information to the RREP packet. In fact, the RREP packet's structure has fewer fields as it does not need to carry any identifiable information, such as the *RREQ ID* field, as required in the case of the RREQ packet. However, the RREP packets still must contain their latest sequence number to facilitate other nodes in determining the freshness level of the received RREP packets via the *Destination Sequence Number* field. Thus, the destination node increments its own sequence number by one every time it sends an RREP packet. In addition, the RREP packet defines the new *Routing Measure* compared to the conventional AODV protocol, which is initialized with the destination node's routing measure Φ as it prepares the RREP packet.

Because the RREP packets are sent via unicast, an intermediate hop need not check if it has received the same packet earlier or not. Instead, it increments the *Hop Count* value by one, adds its own routing measure to the *Routing Measure* field, and simply forwards the RREP packet to the next hop according to its routing table. However, as the source node receives the RREP packets through which it has requested the route, it updates its routing table with the obtained route information from such RREP packets and becomes ready to transmit the data packet to the desired destination.

An example of the entire route request and route reply procedures is shown in Fig. 5. In this scenario, first, the source node S broadcasts an RREQ packet as it desires to find paths to the destination node D. The solid red arrows are the first copies of the RREQ packet that unprecedentedly reach the neighbor nodes. As the later arrived RREQ packets (illustrated by the dotted black arrows) are discarded, there is only one single red arrow towards a node except for the destination node D because it accepts multiple arriving RREQ packets. In addition, as the destination D receives an RREQ packet, it immediately responds with an RREP packet via unicast, which is illustrated by the solid blue arrows. Following the entire route request and reply process, there are two discovered paths between nodes S and D, namely $p^{(1)} = [S, I_1, I_4, I_5, I_8, D]$ and $p^{(2)} = [S, I_2, I_7, I_{10}, I_9, D]$. Given the found paths $p^{(1)}$ and $p^{(2)}$, the S node is ready to transmit the data packet using them.

B. DATA PACKET TRANSMISSION

After a successful route discovery, the source node can finally utilize the paths found to send the data packets. However, as now there can be more than two possible paths to the destination (there is no limit to the number of RREQ packets that the destination node can reply to), the source node is required the decision on which paths to use. As introduced earlier in Definition 1, the optimal path has the largest calculated routing measure Θ given in (10). Based on this, the source can select the best two paths to the destination from its routing table. The implementation of the path selection strategy is described in Algorithm 1.

From Algorithm 1, it is evident that if there is no path available even after the route discovery scheme, the source is still unable to transmit the data packet. In the case of only one path being found, the two output paths p_1 and p_2 are identical and the data packet is duplicated and transmitted using this single path. However, if there are two or more paths, the source simply selects the two paths with the largest routing measure computed using (10). In this case, each path carries a duplicate of the original data packet.

Finally, as the copies of the data packet reach the destination node, the sequence number attached to a packet is checked to determine whether it has received the same one earlier. If the sequence number of the packet is not in the destination node's record, it accepts the packet and processes the encapsulated payload. In contrast, if this packet has been already received, the destination node silently ignores

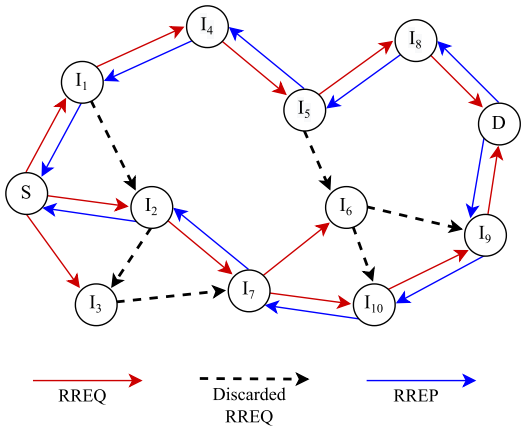


FIGURE 5. Example of route request and reply procedures.

Algorithm 1 Path Selection Algorithm

Input: List r of found paths to the destination, $\|r\| \geq 0$
Output: Two selected paths p_1 and p_2

```
if ||r|| = 0 then
    p1 ← p2 ← ∅
else if ||r|| = 1 then
    p1 ← p2 ← p ∈ r
else
    p1 ← p ∈ r | ∀pi ∈ r : Θ(p) ≥ Θ(pi)
    p2 ← p ∈ r | ∀pi ∈ r, pi ≠ p1 : Θ(p) ≥ Θ(pi)
end if
```

it. Thus, by using multipath routing, the reliability of packet transmission is maximized even if one path is not operational.

C. NODE DISCOVERY AND ROUTING TABLE

Along with the route discovery scheme and data packet transmission, the network activities also include node discovery. A node's discovery of its neighbors enables it to beware of the existence of the other surrounding nodes. Hence, it should be able to compute its own routing measures Φ_m and Φ_s using this information coupled with the measured RSSI values. Moreover, node discovery also allows a node to update its routing table with direct paths to the nearby nodes, thereby avoiding the route discovery overhead if the destination is already within a direct communication range with the source node itself. To realize the node discovery scheme, each node in the network broadcasts a HELLO packet at every predefined interval.

Another important component of the routing protocol is the routing table maintained by every node in the network. More specifically, Table 2 presents an example of the routing table with two entries. The routing table has the following fields:

- *Destination* is the IP address of the destination node;
- *Next hop* is the IP address of the next hop that also contains the path information towards the destination node;
- *Routing measure* is the associated cost of the path and is used to determine the optimal path to the destination;
- *Hop count* is the number of intermediate hops that this path includes;
- *Lifetime* is the point of time at which a path in the routing table is considered obsolete. Here, the entry associated with this path is removed from the routing table.

At predefined intervals, a node checks for expired entries in its routing table. If the node needs to send data packets to the destination via this outdated path, it must initiate a route discovery scheme again and waits for at least one available path before being eventually able to transmit any data packets.

D. COMPLEXITY ANALYSIS

Because the route discovery process of the proposed FT-AORP is mainly based on the original AODV protocol, the complexity analysis of FT-AORP can be straightforwardly inferred from the AODV protocol [49], [50]. We describe two classes of complexity that can be used to characterize the proposed algorithm: time complexity and communication complexity.

In detail, time complexity is defined as the amount of time that is required for the entire network to perform a complete protocol operation (in this case, we consider a successful route discovery). Meanwhile, communication complexity denotes the number of protocol messages that are used to do the same task. Without a loss of generality, we assume that the whole network operates in a synchronous manner. This means that all the nodes collectively execute at fixed time instants; in other words, both the processing and propagation delays of packets are negligible for all nodes. Subsequently, FT-AORP has the time complexity of $\mathcal{O}(2d)$, where d is the diameter of the network. In the worst case, where the source and destination nodes are on two opposite sides of the network, recalling that l is the number of intermediate nodes between two nodes, we obtain $l = d$. It is then intuitively obvious that a route discovery process must traverse $2l$ or $2d$ nodes, including both the route request from the source to the destination node and vice versa (i.e., the route reply phase).

Similarly, the communication complexity of FT-AORP is $\mathcal{O}(2n)$, where n is the number of nodes in the network. This is due to the fact that the operation of FT-AORP is mainly based on the broadcasting mechanism, which means that all network nodes are able to send and receive the protocol's control packets in both the route request and route reply phase. Consequently, FT-AORP has a reasonably acceptable convergence rate of the route discovery process given small to medium-sized networks.

V. PERFORMANCE EVALUATION

In this section, the proposed routing protocol is implemented in the OMNeT++ discrete event simulator [22] and thus evaluated by conducting various extensive simulation experiments. The performance was assessed in terms of packet delivery ratio, end-to-end delay, and path energy

TABLE 2. Example of the routing table.

Destination	Next hop	Routing measure	Hop count	Lifetime
192.168.0.1	192.168.0.12	8.45	3	14.54
192.168.0.6	192.168.0.3	11.23	4	15.69

level. In addition, for each evaluation metric above, three network configurations were altered to observe their impact on the overall performance, including the node density or the number of network nodes, the node speed, and the data packet sending rate as follows.

- For the node density scenario, node speeds were fixed at 15 m/s and the source node's sending rate was fixed at 0.5 Mbps;
- Regarding the node speed scenario, there were a total of 20 nodes and the source node's sending rate was also 0.5 Mbps;
- For the sending rate scenario, 20 nodes were used, while the node speed was fixed at 15 m/s.

In addition, to obtain reliable results, 10 simulation runs were conducted for each configuration with different random seed numbers. Ultimately the mean results were computed.

For comparative analysis, four representative routing protocols, namely ad hoc on-demand distance vector (AODV) [27], ad hoc on-demand multipath distance vector (AOMDV) [51], AOMDV with the fitness function (FF-AOMDV) [16], and load-balanced multi-path routing protocol with energy constraints (EE-LB-AOMDV) [38] were employed. It is noted that for the EE-LB-AOMDV protocol, we did not implement the load balancing function and we instead use the discovered paths to transmit multiple copies of the same packet to enable fault tolerance. These protocols were re-implemented in the simulation environment and were provided with the exact same configurations for each simulation run in all scenarios.

A. SIMULATION MODEL

In the simulation testbed, every simulation run shared the following configurations. First, various numbers of nodes were initially randomly scattered within a 1000×1000 (m^2) obstacle-free area. The simulation model employed the random waypoint mobility model [52], implying every node moved to a uniformly distributed position with a varied number of speeds and a zero-pause time. During the simulation time, the source node generated fixed-size data packets with different rates. In addition, the ratio medium of the simulation environment had a background noise power of -110 dBm. Each node was equipped with a wireless interface with the following settings:

- transmitter power: 1.2 mW;
- receiver sensitivity: -87 dBm;
- signal-to-noise-plus-interference ratio (SNIR) threshold: 3 dB.

Regarding the MAC protocol, the wireless interfaces used IEEE 802.11n standard with the ad hoc management mode and operated at 2.4 GHz. In addition, each node was powered by energy storage with a nominal capacity of 5328 J. During the start phase of the simulation, the battery capacity of each node was initialized with a random value between 70% and 100% of the nominal capacity. Moreover, when a node's energy storage is below a threshold ζ of 5%, it was considered energy-depleted. Finally, each entry in the routing table had an active route timeout of 1.5 s and unless it was updated; this entry was unusable and removed. The key simulation parameters are summarized in Table 3.

B. PACKET DELIVERY RATIO

Packet delivery ratio (PDR) is computed as the ratio of the number of successfully delivered packets from the source to the destination to the number of generated packets by the source node in a simulation run. This metric is crucial to data-critical packet transmissions because it demonstrates the reliability and fault-tolerant capability of a protocol. Therefore, given n_g and n_d being the number of generated and successfully delivered packets, respectively, the PDR is calculated using

$$\text{PDR} = \frac{n_d}{n_g}. \tag{12}$$

Fig. 6 shows the evaluation of the PDR performance of five protocols under three different scenarios. First, it was measured as the number of nodes increased from 10 to 80, as shown in Fig. 6a. It is evident that, with only 10 nodes, all the protocols succeeded in delivering more than 90% of the data packets to the destination node. However, as the number of nodes increased to 80, the other four protocols, except for FT-AORP, failed to provide reliable transmission and their PDRs were as low as 0.8. In contrast, FT-AORP guaranteed a PDR of more than 80%, even in the most aggressive scenario of the network density. This may be justified by the fact that FT-AORP employs various relevant routing metrics to avoid the occurrence of potential link failures on one path.

In addition, Fig. 6b shows the PDR performance against various node speeds, from 5 to 60 m/s. It can be observed that as node speed increases, PDR decreases owing to the high likelihood of link breaks as the nodes constantly change their positions. However, EE-LB-AOMDV and FT-AORP outperformed the other three baseline protocols in nearly every scenario. Even at a very high speed of 60 m/s, the two protocols were still able to deliver 70% of the data packets to the destination, whereas the recorded numbers of the remaining protocols were all 10% lower. Because FT-AORP considers the node mobility and its location with respect to other nodes when selecting the optimal paths, its results were marginally better than EE-LB-AOMDV in general.

TABLE 3. Key simulation parameters.

Parameter	Value	Unit
Simulation area	1000×1000	m^2
Number of nodes	$\{10, 20, 40, 60, 80\}$	nodes
Mobility model	Random waypoint	
Node speed	$\{5, 15, 30, 45, 60\}$	m/s
Packet sending rate	$\{0.1, 0.5, 1, 2, 5\}$	Mbps
Packet size	500	bytes
Noise power	-110	dBm
Transmitter power	1.2	mW
Receiver sensitivity	-87	dBm
SNIR threshold	3	dB
MAC	IEEE 802.11n	
Center frequency	2.4	GHz
Initial energy level	$[70\%, 100\%]$	
ζ threshold	5%	
Active route timeout	1.5	seconds

Fig. 6c further demonstrates the fault tolerance of FT-AORP against different packet sending rates between 0.1 and 5 Mbps. In general, the PDR performance of the three protocols was less materially affected by this factor than by the network density and node speed. At 0.1 Mbps, the reduced packet delivery efficiency is possibly due to the low data rate compared to the predetermined node speed and density. To be more specific, a certain number of packets might be undelivered due to the fast changes in the network topology. In the scenario that required the largest throughput (i.e., 5 Mbps), FT-AORP successfully transmitted nearly 85% of the data packets, which was just 3% fewer compared to the other less throughput-demanding scenarios of 0.1, 0.5, and 1 Mbps. Meanwhile, EE-LB-AOMDV had a very comparable simulation result, and AODV did not provide such a satisfactory performance. Thus, FT-AORP is also an ideal routing protocol for bandwidth-demanding applications, such as voice and video calls.

C. END-TO-END DELAY

End-to-end delay is the elapsed time from when a data packet is generated by the source node to when it is successfully received by the destination node. This latency includes all potential delays such as queuing at the wireless interface and re-transmission attempts by the Medium Access Control. For this metric, the average delay of all the successfully transmitted packets in a simulation run was calculated as

$$\text{End-to-end delay} = \frac{\sum_{i=1}^{n_d} \left(\tau_i^d - \tau_i^g\right)}{n_d}, \tag{13}$$

where τ_i^g (resp. τ_i^d), $\tau_i^d > \tau_i^g$, is the time instant where the i-th packet is generated by the source node (resp. successfully received by the destination node).

Fig. 7 shows the end-to-end delay performance under three different simulation parameters. In particular, Fig. 7a compares end-to-end latency with different levels of the network density measured in the number of nodes. In most cases, the latency increased as the network grew larger because there were possibly more nodes involved in a transmission path. However, the FT-AORP protocol exhibited smaller delays overall than the other four protocols for all network sizes. This may be because the intermediate nodes move away from one another and potentially cause link breaks, while the four protocols mainly transmit packets using the path with the smallest number of hop counts

Fig. 7b depicts the delay performance with regard to various node speed values. It is evident that as the nodes sped up, the network topology kept changing, possibly causing the nodes to lose their current established links. At 5 and 15 m/s, all the protocols showed approximately the same delay in packet transmission of 0.013 and 0.008 s, respectively. As the speed increased to 30 m/s and higher, FF-AOMDV and EE-LB-AOMDV exhibited the best delay results, while the performance of FT-AORP was also very similar. This is because they could choose more stable paths compared to AODV and AOMDV.

Regarding the end-to-end delay results against various sending rates, as shown in Fig. 7c, as the data packets being injected into the network in a time instant increased, the transmission delay increased. This may be attributed to lower-layer channel conflicts, as the nodes compete for channel access. On the whole, the four multipath protocols outperformed AODV in all scenarios because they could transmit the packets using two paths and thus avoid conflicts happening on one path. In fact, EE-LB-AOMDV performed slightly better than FT-AORP because it considered round-trip time as a routing metric. Overall, the applicability of FT-AORP to time-critical systems where the packet's transmission time should be stably minimal in a variety of contexts is proven.

D. PATH ENERGY

With this metric, the average energy level of the immediate nodes in a path that is used to transmit a data packet was computed. It indicates that the FT-AORP protocol prefers to choose the path with high-energy intermediate nodes. Because there may be two discovered paths for data transmission between the source and the destination, the path that delivers the data packet to the destination first, was considered. The path energy level for a simulation run is computed as

$$\text{Path energy} = \frac{1}{n_d} \sum_{i=1}^{n_d} \left(\frac{1}{\|p^{(i)}\|} \sum_{v_j \in p^{(i)}} E^{(v_j)} \right), \tag{14}$$

where n_d is the number of successfully transmitted packets, $p^{(i)}$ is the path used to transmit i-th packet, v_j is the j-th node in the path, and $E^{(v_j)}$ is the energy level (percent) of node v_j.

Fig. 8 presents the average energy level of the transmitting paths with three different simulation parameters. First, the performance of the protocols was compared in the testbed including from 10 to 80 nodes, as shown in Fig. 8a. It is evident that both AODV and AOMDV shared very similar simulation results, as there was not much discrepancy in their operating principles. Regarding FF-AOMDV, EE-LB-AOMDV, and FT-AORP, because these protocols can

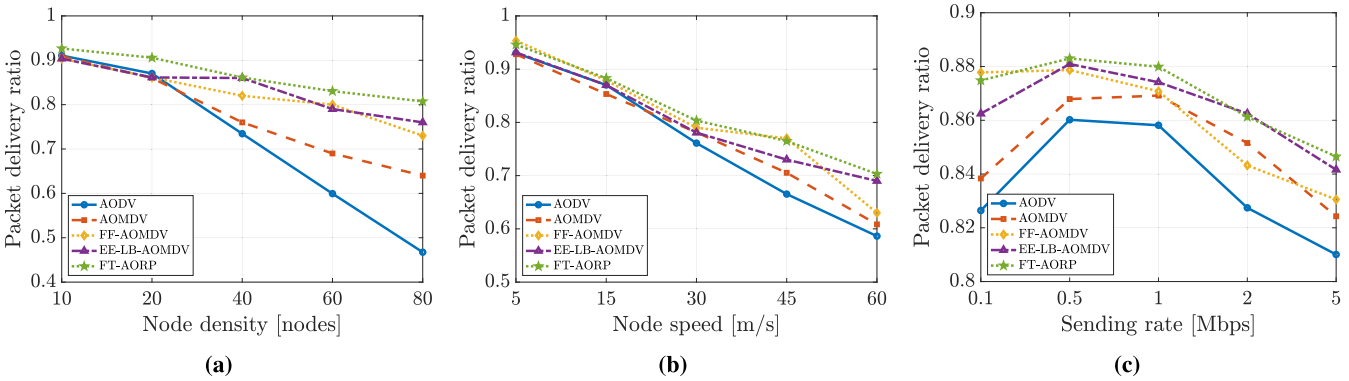


FIGURE 6. Packet delivery ratio performance against (a) node density, (b) node speed, and (c) sending rate.

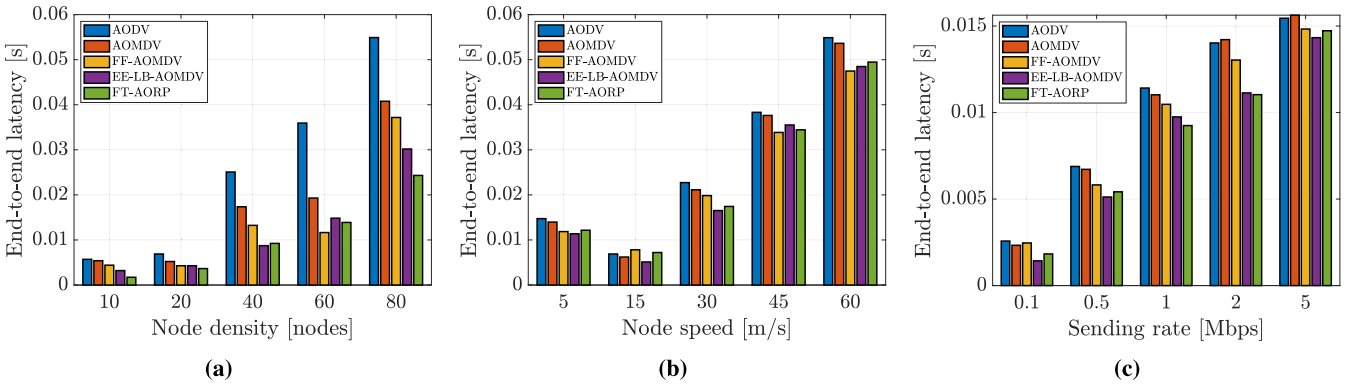


FIGURE 7. End-to-end delay performance against (a) node density, (b) node speed, and (c) sending rate.

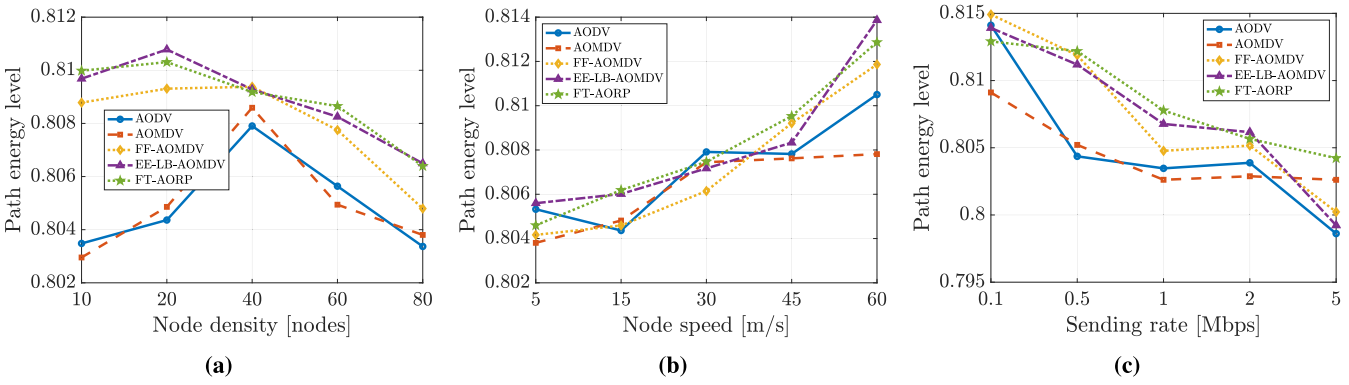


FIGURE 8. Path energy performance against (a) node density, (b) node speed, and (c) sending rate.

learn and select paths of higher in the energy levels, they certainly exhibited better performance regardless of the node density.

Next, Fig. 8b shows the measured path energy against variations in node mobility. It is evident that the overall trend is an increase in the energy level as the node speed increases for all the routing protocols. For certain speed values, specifically 5, 30, and 60 m/s, FT-AORP exhibited slightly lower energy level results compared to the other protocols. However, for the remaining scenarios, FT-AORP was capable of selecting paths with higher energy nodes. Consequently, the network lifetime was significantly improved, as the energy-depleted nodes did not participate in the data transmission activities.

Finally, Fig. 8c depicts the path energy performance with multiple data-sending rates. It is obvious that higher the sending rates result in more power being consumed by the nodes to transmit the data packets. In detail, AODV and AOMDV had the two smallest path energy levels overall because they did not consider energy as a routing metric. Meanwhile, FF-AOMDV, EE-LB-AOMDV, and FT-AORP exhibited the

highest remaining energy levels overall, especially at 5 Mbps, where FT-AORP outperformed all other routing protocols.

VI. CONCLUSION

This study proposed a fault-tolerant ad hoc on-demand routing protocol for MANET systems, referred to as FT-AORP. Considering the mobility tendency of network nodes, the radio signal strength levels they obtain from their neighbors, and their energy consumption rate, the proposed routing protocol can make rational decisions on the prospective paths to be used to transmit the data packets. Simulation results using the OMNeT++ environment indicated that FT-AORP can improve the packet delivery ratio, reduce the end-to-end transmission delay, and select high-energy paths. Consequently, the proposed protocol is helpful for applications where data-critical packets are required to be successfully delivered to the destination with low latency, and a rapid installation of an ad hoc network is strongly favored.

In future work, other routing metrics will be developed to guarantee the quality of service for specific applications where a traffic prioritization scheme is demanded. In addition, the route discovery strategy can be improved to reduce the protocol control overhead. Finally, because radio signal characteristics could not be entirely modeled by simulations conducted, the proposed protocol will be implemented on real-world mobile devices to further experiment and prove the applicability potential of FT-AORP.

REFERENCES

[1] R. Bruzgiene, L. Narbutaite, and T. Adomkus, *MANET Network in Internet of Things System*. Rijeka, Croatia: IntechOpen, May 2017.

[2] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for MANET based on distributed trust and energy management," *Wireless Pers. Commun.*, vol. 81, no. 3, pp. 961–979, Apr. 2015.

[3] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile ad hoc network (MANET) protocols and their applications," in *Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, May 2021, pp. 204–211.

[4] L. Kant, K. Young, O. Younis, D. Shallcross, K. Sinkar, A. Mcauley, K. Manousakis, K. Chang, and C. Graff, "Network science based approaches to design and analyze MANETs for military applications," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 55–61, Nov. 2008.

[5] J. Sandeep and J. S. Kumar, "Efficient packet transmission and energy optimization in military operation scenarios of MANET," *Proc. Comput. Sci.*, vol. 47, pp. 400–407, Jan. 2015.

[6] I.-R. Chen, R. Mitchell, and J.-H. Cho, "On modeling of adversary behavior and defense for survivability of military MANET applications," in *Proc. IEEE Mil. Commun. Conf.*, Oct. 2015, pp. 629–634.

[7] M. H. Hassan, S. A. Mostafa, H. Mahdin, A. Mustapha, A. A. Ramli, M. H. Hassan, and M. A. Jubair, "Mobile ad-hoc network routing protocols of time-critical events for search and rescue missions," *Bull. Electr. Eng. Informat.*, vol. 10, no. 1, pp. 192–199, Feb. 2021.

[8] Y. Jin, X. Tan, W. Feng, J. Lv, A. Tuerxun, and K. Wang, "MANET for disaster relief based on NDN," in *Proc. 1st IEEE Int. Conf. Hot Information-Centric Netw. (HotICN)*, Aug. 2018, pp. 147–153.

[9] P. K. Garg, "Potentials of network-based unmanned aerial vehicles," in *Cloud IoT-Based Vehicular Ad Hoc Networks*. Hoboken, NJ, USA: Wiley, 2021, pp. 369–397.

[10] T. Ohta, M. Nishi, T. Terami, and Y. Kakuda, "Information dissemination using MANET for disaster evacuation support," *IEICE Trans. Commun.*, vol. 102, no. 4, pp. 670–678, 2018.

[11] Y. Jahir, M. Atiquzzaman, H. Refai, A. Paranjothi, and P. G. LoPresti, "Routing protocols and architecture for disaster area network: A survey," *Ad Hoc Netw.*, vol. 82, pp. 1–14, Jan. 2019.

[12] R. A. Nazib and S. Moh, "Reinforcement learning-based routing protocols for vehicular ad hoc networks: A comparative survey," *IEEE Access*, vol. 9, pp. 27552–27587, 2021.

[13] M. Ayyash, Y. Alsbou, and M. Anan, "Introduction to mobile ad-hoc and vehicular networks," in *Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications*, D. Benhaddou and A. Al-Fuqaha, Eds. New York, NY, USA: Springer, 2015, pp. 33–46.

[14] M. Conti and S. Giordano, "Multihop ad hoc networking: The theory," *IEEE Commun. Mag.*, vol. 45, no. 4, pp. 78–86, Apr. 2007.

[15] M. Conti and S. Giordano, "Multihop ad hoc networking: The evolutionary path," in *Mobile Ad Hoc Networking*. Hoboken, NJ, USA: Wiley, 2013, pp. 1–33.

[16] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq, and T. Saba, "Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function," *IEEE Access*, vol. 5, pp. 10369–10381, 2017.

[17] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[18] J. Park, S. Moh, and I. Chung, "A multipath AODV routing protocol in mobile ad hoc networks with SINR-based route selection," in *Proc. IEEE Int. Symp. Wireless Commun. Syst.*, Oct. 2008, pp. 682–686.

[19] C. T. Hieu and C.-S. Hong, "A connection entropy-based multi-rate routing protocol for mobile ad hoc networks," *J. Comput. Sci. Eng.*, vol. 4, no. 3, pp. 225–239, Sep. 2010.

[20] S. S. Solapure and H. H. Kenchannavar, "Design and analysis of RPL objective functions using variant routing metrics for IoT applications," *Wireless Netw.*, vol. 26, no. 6, pp. 4637–4656, Aug. 2020.

[21] H. H. El-Sayed, A. Younes, and F. A. Alghamdi, "Multiobjective multicast DSR algorithm for routing in mobile networks with cost, delay, and hop count," *Complexity*, vol. 2021, pp. 1–8, Jun. 2021.

[22] *OMNeT++ Discrete Event Simulator*. Accessed: Oct. 20, 2022. [Online]. Available: https://omnetpp.org/

[23] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc Netw.*, vol. 2, no. 1, pp. 1–22, Jan. 2004.

[24] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. SIGCOMM*, New York, NY, USA, Oct. 1994, pp. 234–244.

[25] T.-W. Chen and M. Gerla, "Global state routing: A new routing scheme for ad-hoc wireless networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 1, Jun. 1998, pp. 171–175.

[26] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proc. IEEE Int. Multi Topic Conf.*, Lahore, Pakistan, Dec. 2001, pp. 62–68.

[27] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl.*, Jan. 1999, pp. 90–100.

[28] D. B. Johnson, D. A. Maltz, and J. Broach, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad Hoc Netw.*, vol. 5, pp. 139–172, Jan. 2001.

[29] V. Park and M. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, vol. 3, Apr. 1997, pp. 1405–1413.

[30] Z. Chen, W. Zhou, S. Wu, and L. Cheng, "An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET," *IEEE Access*, vol. 8, pp. 44760–44773, 2020.

[31] G. Dhananjayan and J. Subbiah, "T2AR: Trust-aware ad-hoc routing protocol for MANET," *SpringerPlus*, vol. 5, no. 1, p. 995, Jul. 2016.

[32] C. Z. Sirmollo and M. A. Bitew, "Mobility-aware routing algorithm for mobile ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–12, May 2021.

[33] S. A. Nsaif, S. Y. Park, and J. M. Rhee, "SRAD: A novel approach to seamless routing for wireless ad hoc networks," in *Proc. 23rd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2021, pp. 172–175.

[34] X. Song, L. Zhou, H. Zhao, X. Hu, and J. Wei, "Localized fault tolerant and connectivity restoration algorithms in mobile wireless ad hoc network," *IEEE Access*, vol. 6, pp. 36469–36478, 2018.

[35] H. Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On minimizing the impact of mobility on topology control in mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1158–1166, Mar. 2012.

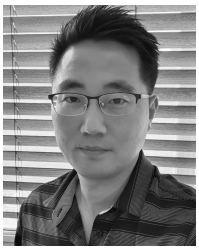
[36] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[37] P. K. Pattnaik, B. K. Panda, and M. Sain, "Design of novel mobility and obstacle-aware algorithm for optimal MANET routing," *IEEE Access*, vol. 9, pp. 110648–110657, 2021.
[38] M. Naseem, G. Ahamad, S. Sharma, and E. Abbasi, "EE-LB-AOMDV: An efficient energy constraints-based load-balanced multipath routing protocol for MANETs," *Int. J. Commun. Syst.*, vol. 34, no. 16, p. e4946, Nov. 2021.
[39] S. Sarhan and S. Sarhan, "Elephant herding optimization ad hoc on-demand multipath distance vector routing protocol for MANET," *IEEE Access*, vol. 9, pp. 39489–39499, 2021.
[40] M. Tarique, K. E. Tepe, S. Adibi, and S. Erfani, "Survey of multipath routing protocols for mobile ad hoc networks," *J. Netw. Comput. Appl.*, vol. 32, no. 6, pp. 1125–1143, 2009.
[41] S. Mao, S. Lin, Y. Wang, S. S. Panwar, and Y. Li, "Multipath video transport over ad hoc networks," *IEEE Wireless Commun.*, vol. 12, no. 4, pp. 42–49, Aug. 2005.
[42] X. Li and L. Cuthbert, "Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks," in *Proc. IEEE Comput. Soc. 12th Annu. Int. Symp. Modeling, Anal., Simulation Comput. Telecommun. Syst.*, Oct. 2004, pp. 184–191.
[43] Y. H. Robinson, E. G. Julie, K. Saravanan, R. Kumar, and L. H. Son, "FD-AOMDV: Fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 11, pp. 4455–4472, Nov. 2019.
[44] C. Wu, K. Kumekawa, and T. Kato, "A MANET protocol considering link stability and bandwidth efficiency," in *Proc. Int. Conf. Ultra Modern Telecommun. Workshops*, Oct. 2009, pp. 1–8.
[45] D. Macone, G. Oddi, and A. Pietrabissa, "MQ-routing: Mobility-, GPS- and energy-aware routing protocol in MANETs for disaster relief scenarios," *Ad Hoc Netw.*, vol. 11, no. 3, pp. 861–878, May 2013.
[46] R. Jurdak, P. Corke, D. Dharman, and G. Salagnac, "Adaptive GPS duty cycling and radio ranging for energy-efficient localization," in *Proc. 8th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, Zürich, Switzerland, 2010, pp. 57–70.
[47] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Hoboken, NJ, USA: Wiley, 2006.
[48] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jan. 1948.
[49] M. Srivastava and P. Yadav, "A performance analysis of routing protocols in mobile ad-hoc networks," *International J. Eng. Res. Technol.*, vol. 1, no. 8, p. 11, Oct. 2012.
[50] A. Lee, I. Ra, and H. Kim, "Performance study of ad hoc routing protocols with gossip-based approach," in *Proc. Simulation Multiconference*, Mar. 2009, pp. 1–8.
[51] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. IEEE 9th Int. Conf. Netw. Protocols (ICNP)*, Nov. 2001, pp. 14–23.
[52] C. Bettstetter, H. Hartenstein, and X. Pérez-Costa, "Stochastic properties of the random waypoint mobility model," *Wireless Netw.*, vol. 10, no. 5, pp. 555–567, 2004.

DUC N. M. HOANG (Graduate Student Member, IEEE) received the B.E. degree in computer engineering from the Ho Chi Minh City University of Technology (HCMUT), VNU—HCM, Vietnam, in 2020. He is currently pursuing the M.S. degree with the Department of Electronics Engineering, Myongji University, South Korea. His research interests include *ad-hoc* networking, wireless networks, fault-tolerant networks, and the Internet of Things.

JONG MYUNG RHEE (Member, IEEE) received the Ph.D. degree from North Carolina State University, USA, in 1987.

After 20 years at the Agency for Defense Development in South Korea, where he made noteworthy contributions to C4I and military satellite communications, he joined DACOM and Hanaro Telecom, in 1997 and 1999, respectively. At Hanaro Telecom, which was the second-largest local carrier in South Korea, he served as the Chief Technology Officer (CTO) with a senior executive vice-president position. His main duty at Hanaro Telecom was a combination of management and new technology development for high-speed Internet, VoIP, and IPTV. In 2006, he joined Myongji University, and currently, he is a Special Mission Professor with the Information and Communications Engineering Department. His current research interests include centered on military communications and smart grids, including *ad-hoc* and fault-tolerant networks.



SANG YOON PARK (Member, IEEE) received the B.S. degree in electrical engineering and the M.S. and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, Republic of Korea, in 2000, 2002, and 2006, respectively. He joined the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, as a Research Fellow, in 2007. From 2008 to 2014, he was a Research Scientist with the Institute for Infocomm Research, Singapore. Since 2014, he has been with the Department of Electronic Engineering, Myongji University, Yongin, Republic of Korea, where he is currently an Associate Professor. His research interests include design of dedicated and reconfigurable architectures for low-power and high-performance digital communication systems.