IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 3, 2019, accepted May 21, 2019, date of publication May 31, 2019, date of current version June 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920248

Long-Term Routing Stability of Wireless Sensor Networks in a Real-World Environment

CHENG LEONG LIM[1], CINDY GOH[1], AND YUN LI[2,3], (Senior Member, IEEE)
[1]School of Engineering, University of Glasgow, Glasgow G12 8LT, U.K.
[2]Industry 4.0 Artificial Intelligence Laboratory, Dongguan University of Technology, Dongguan 523808, China
[3]Design, Manufacturing and Engineering Management, University of Strathclyde, Glasgow G1 1XJ, U.K.

Corresponding authors: Cindy Goh (cindy.goh@glasgow.ac.uk) and Yun Li (yun.li@ieee.org)

This work was supported by the Economic Development Board (EDB) Singapore under Grant COY-15-IPP-130006.

ABSTRACT The reliability of a wireless sensor network (WSN) is often assessed on node-to-node communication performance through link characterization. Long-term routing stability is an aspect of a WSN that is often overlooked in routing protocol implementations. In this paper, we investigate the routing stability of ZigBee PRO implemented WSN nodes that are deployed in a real-world environment. Frequent changes in next hops along routing paths between source and destination nodes can result in an increase in undesired energy consumption of the WSN. Hence, the relative routing path usage count, usage rate of unique next hop and switching frequency count are proposed as routing stability indicators. Our findings show that routing stability is subjected to not only the quality of a link but also to the implemented routing protocols, deployed environment and routing options available. More importantly, next hops with low usage rates are shown to experience a higher probability of disconnection from the Neighbor Table of respective source nodes, causing them to be short-lived. The need to avoid these links shows the importance of evaluating routing stability and identifying network bottlenecks.

INDEX TERMS Wireless sensor networks, ZigBee, AODV, routing protocol, indoor radio communication, quality of service.

I. INTRODUCTION

The demand for large-scale sensing capabilities and scalable communication networks to monitor and control entities within smart buildings have fuelled the exponential growth in wireless sensor networks (WSNs). A WSN consists of spatially distributed autonomous sensor nodes designed to measure the physical or environmental conditions, and to forward recorded data to a centralized device. A WSN proves to be an attractive enabler for accurate sensing in terms of associated installation costs and flexibility in sensor placement [1, 2]. While a WSN offers a number of benefits, it has yet to realize its full potential due to its susceptibility to network challenges when deployed. Under persistent influence of network challenges, failure to identify the network bottlenecks may lead to undesirable poor packet delivery and frequent route changes, leading to higher energy consumption and even early death of battery-powered devices.

The reliability of a WSN is often assessed on node-to-node communication performance through link characterization. For example, the quality of node-to-node communication is measured with packet delivery and environmental noise factors [3], [4], spatial and temporal characteristics of packet losses [5], [6], and temporal consecutive link failures [7]. So far, however, little work has systematically evaluated WSN communication performance by investigating the long-term routing stability, particularly under real-world environment settings.

A network topology is made up of interconnected routing paths across the network, and a routing path is made up of intermediate routers forming node-to-node connections. Any node-to-node failure along the routing path translates into routing path failure. To improve end-to-end reliability, the implemented routing protocol has to respond to these failures and make appropriate changes along the routing path. Furthermore, the selection of routing paths has to be robust to the dynamics within the deployed environment such as human activities, changes in the physical environment (i.e. opening and closing of doors), and radio channel interference from third-party wireless devices.

Link failures are not uncommon in a WSN [4]–[6], [10], [11]. However, not every link is used for packet routing,

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

in particular a sink-based application (i.e. environmental sensing) where nodes forward packets to a single destination. Given a routing protocol that re-routes upon link failures, monitoring the historical variations along routing paths could provide potentially useful information about the key nodes of these routing paths and the quality of the network. An unstable network suggests frequent failures along the routing paths and initiation of re-routing, hence increasing energy consumptions. Avoiding excessive and unnecessary routing path variation is therefore critical to improving the lifespan of the WSN.

This paper investigates the long-term routing stability of ZigBee PRO implemented wireless sensor nodes deployed in a real-world environment by monitoring relative routing path usage count, usage rate of unique next hop and switching frequency counts (SFC). Unlike typical link quality estimation techniques that are designed for instantaneous evaluation of link quality, these parameters are sampled periodically every 25 minutes, reused from existing information in the ZigBee stack and do not require additional overhead or network probing. Relative routing path usage count detects key routing intersection points in the network. Usage rate of unique next hop relative to individual source node identifies dominant next hop from minority (less dominant) ones. Lastly, SFC determines the consistency of the dominant next hop used relative to a source node.

The remainder of this paper is organized as follows. Section II discusses the differences between link stability and routing stability in distributed wireless networks. Existing link quality estimation techniques provide instantaneous assessment of link quality. However, since the assessment routing stability in a WSN requires long-term monitoring, it is often overlooked. Section III describes the experimental setup developed to evaluate the routing stability of a WSN testbed deployed in a single level administrative office. Section IV introduces the three key measures to evaluate long-term routing stability and to identify possible network bottlenecks. Section V discusses the impact of routing instability on WSN reliability and the importance of monitoring long-term routing stability. Finally, Section VI concludes the paper with key findings and proposes future works.

II. WIRELESS SENSOR NETWORK LINK STABILITY AND ROUTING STABILITY

A. LINK STABILITY AND ITS IMPACT ON LINK QUALITY ESTIMATION

The stability of low-power wireless communication in a WSN is highly influenced by the deployed environment settings. These settings include for example, line-of-sight (LOS) and non-LOS conditions, distance between communicating nodes, the number of human bodies in the environment [8], changes in the physical environment (i.e. opening and closing of doors), noise floor [9], radio channel interference from third party wireless devices and so on.

Link instability in a WSN is often regarded to have temporal characteristics. This means that the quality of transmitted signals between two nodes varies and link failure, if any, may not be constant. As such, temporal solutions are suggested to minimize network protocol compensation and avoid drastic routing changes [7], [11], [13]. For instance, upon identifying a bursty link with temporal failure, Srinivasan *et al.* [7] employed aggressive back-off technique to defer immediate retransmission. Since disconnection of a bursty link is short-lived, by delaying retransmission, the chances of a successful packet delivery improved. Bursty links are identified with a β factor, calculated using conditional probability distribution functions. The β factor determines the probability that the next packet will be received after n consecutive successes or failures. In another work [12], short-term link estimator (STLE) is developed to identify bursty links and suggest using them when they are stable. Doing so avoids the need for re-routing and reduces the total overheads by 19% as compared to traditional routing. STLE measures the link stability of its neighbor's communication by listening to their packets sent. The probability of successful delivery is derived from on the packet sequence number and failed acknowledgment.

Link instability has different impacts on different link quality metrics. Srinivasan *et al.* [10] discovered that when measuring the quality of received packets between two nodes relative to packet reception rate (PRR), link quality indicator (LQI) metric varies more than received signal strength indication (RSSI). The difference is due to the additional indicator of received signals' chip error rate in LQI measurement, while RSSI with a smaller operating range is less sensitive to PRR variation. In particular, when nodes communicate near the receiver's sensitivity edge (i.e. less than -87 decibel-milliwatt (dBm)), it enters a transition region where PRR ranges radically between 0 and 100%. The local noise level is explained to have contributed to poor signal reception in the transition region, leading to temporal communication disconnection and connection. A similar observation is made in [11], where the temporal effect of link stability is found to have both constructive and destructive impacts on a node's packet delivery performance. This results in a communication link of poor quality fluctuating between transitional and disconnected zones. Zuniga and Krishnamachari [11] then concluded that the PRR variance is caused by the severity of multi-path effect of the environment, rather than modulation, encoding, output power, and frame size. To better determine link quality stability, a transitional coefficient is introduced to estimate the size of transitional region (amount of poor links) for different environments. The smaller the coefficient, the better the metric can estimate PRR.

Miranda *et al.* [15] conducted a series of LOS path loss estimation experiments in an indoor environment and found that the measured signal strength fluctuates from 11 to 14 dB between static nodes depending on the communication channels used. This range increases further to between 14 to 18 dB when the experiment was repeated in an indoor industrial environment. The variations in RSSI are due to noise floor, interference and physical obstructions within the environment, leading to multipath effects. Larger obstacles found in industrial settings introduce higher signal attenuation and deeper deviation. Particularly in an indoor environment, every physical entity in the environment is a potential reflector for the transmitted signals. As a result, a node receives multiple copies of the same signal that are reflected from the environment [16], [17]. As the transmission distances of these reflected paths are longer than the direct LOS/non-LOS path, signals arriving at the receiver are weaker due to path loss, and delayed by several nanoseconds. This reception delay is referred to as short-term fading or fast fading [16], [17]. It produces a finer variance of channel impulse within the reception symbol duration due to the small coherence time of the channel relative to application requirement.

The fading phenomenon is evaluated under the presence of human activities in [14], [19]. It is shown that fading exhibits a linear dependence with increasing human density, while long-term fading is a direct consequence of human presence. Horvat *et al.* [8] measured the fading levels of communicating nodes under human presence and concluded that human bodies obstruction has a greater impact on non-LOS propagation than LOS communication. Under non-LOS condition, fading levels range from 15 to 25 dB, while in LOS conditions, fading levels reduced from 4 to 11 dB. Higher fading levels can be explained with the rarely completely shadowed dominant ray of LOS signal propagation. Similar temporal effect is also experienced differently in different channels [16], [17], [20]. This leads to inconsistency in link quality assessment on different channels, where the upper layer protocol has to take into account signal power deviation from fading effects and constant changes in the environment. Distance estimation can vary up to 20 m between the best and the worst single channel, in particular long-distance communication [20]. In order to minimize the influence of fading levels on signal power, measuring signal quality on multiple channels [20] or simply changing the communication channel [16] is suggested.

Existing link quality estimation techniques are often instantaneous, performed at the expense of decoding received packets, probing of network using additional overheads, over-listening of channel for neighboring nodes' transmissions or noise floor, and so on. As long as these estimations reflect the link quality accurately at the moment of transmission, they are assumed to be reliable. However, existing link quality estimation techniques are not effective in distinguishing stable and unstable links because the characteristics of unstable links are often not persistent and may not be detectable over a short period [14]. A node is typically unaware of the impact of an unstable link until a link failure occurs. In addition, the temporal effect of link instability cannot be deterministically calculated unless the local positions of the communicating nodes, the geometry of the deployed environment, and the movements of mobile attenuators are known at all times. In reality, accounting for all these factors is not practical. As such, link stability is often defined as a varying probability during modeling [10]. For example, variations in received signal strength between communicating nodes are accounted as a Gaussian variable in the lognormal shadowing technique [21].

B. ROUTING STABILITY

Link instability can lead to routing instability in a WSN [27]. Routing instability is the phenomenon of frequent changes along routing paths between source and destination nodes. Similar to link stability, routing paths also vary depending on the harshness of the deployed environment. However, routing stability also accounts for the adaptability and robustness of generated routing paths to overcome the long-term impact of the deployed environment.

Ishibashi and Yamaoka [27] evaluated the routing stability of 802.11 a/b/g mesh technology networks in real-world environments in terms of routing path prevalence, persistence and oscillation. Wireless local area network (WLAN) connectivity between a source and destination pair is found to be seldom static with most pairs using the same route for more than 40% of the time. In addition, 57.7% of them have a dominant route usage of less than one minute with routing path oscillation approximately 5000 times over four days. The WLAN routers are statically deployed. Since there are a limited number of routers within the reception range, their routing options are constrained. Unlike in a WSN, network is usually designed for wide deployment of nodes that forms a dense interconnected mesh network.

A *Competence* metric is introduced in [14] to differentiate good and long-term stable links for routing, while dropping the unstable ones (even if they are good). To characterize long-term link stability, *Competence* incorporates exponential weighted moving average with link quality history as the weight of the smoothing filter. Furthermore, *Competence* compensates the variability of wireless communication by specifying two upper and lower packet delivery rate (PDR) bounds, which accounts for short-term variation in delivery performance. PDR is the rate in which transmitted packets from a sender node are successfully delivered to its recipient. It is found that the end-to-end (E2E) PDR varies significantly during the daytime. E2E PDR is the rate in which transmitted packets from a sender node are successfully delivered to the destination node. E2E PDR measures approximately 55% between the hours of 8 AM and 8 PM, dropping from 90% in the evening hours. *Competence* level is measured poor during the day, indicating long-term link instability. In addition, the drop in quality of links during the day introduces the number of count in which parent nodes switch between nodes pairs. This phenomenon triggers further packet losses from network maintenance packets leading to greater energy consumption and route changes. However, a stable route enforced by a *Competence* implemented protocol may potentially increases traffic loads on affected nodes. In our work, we have shown that the most dominant next hop may also operate on links with failures and not all routers have "good" routing options. The choice of routing path is largely dependent on the resources available and the type of routing mechanism. Failing to take these into account may be costly in the long run.

Long-range link characterization of a WSN operating at 868 MHz is conducted in [23]. A node constructs a list of its neighbors within reception range in its Neighbor Table (NT). It is observed from the variations within NT that the number of nodes within reception changes constantly with uncommon periods of stability. A proactive approach (i.e. instantaneous link quality estimation) is said to be ineffective at selecting reliable nodes, since a "reliable" next hop may be redundant in the next moment. Although the list of connected nodes in NT changes frequently, a group of stable neighbors still exists. Long-term stable connection with these nodes is discovered to have either less than -75 dBm in RSSI value or within one-fifth of the radio range at about 70 m. This suggests that for a connection to withstand the dynamics in the deployed environment, sufficient link budget must be considered.

A distributed wireless network involves many uncertainties [14]. For WSN nodes to operate on a single reference value yet expecting a stable network is not practical. Changes along routing paths are expected. The choice in routing path selection is largely subjected to the implemented routing protocol. However, persistent changes in routing paths are undesirable. Re-routing requires the use of network broadcast mechanism, which has shown to trigger further changes in next hop due to increasing packet collisions [14], [24]. An unstable routing path suggests frequent link failures, leading to the need for additional network maintenance overheads such as retransmission and re-routing. Given a routing mechanism that re-routes upon failure, the most utilized routing path may be seen as the most dominant and robust one.

Link instability affects the performance of a WSN at the network layer, which is reflected on the stability of generated routing paths. For instance, when experiencing link instability, duty cycling protocol failing to allocate transmission periods or a multi-radio network failing to re-assign radio channels between nodes can lead to frequent changes in routing connectivity. Therefore, the ability to measure routing path stability can provide useful insights not only on the adaptability and robustness of network layer protocol, but also the quality of links between wireless sensor nodes. To our best knowledge, there is limited work that realistically investigates the long-term WSN routing stability in real-world indoor environments.

III. TESTS OF THE WIRELESS SENSOR NETWORK IN A REAL-WORLD ENVIRONMENT

A. ZIGBEE PRO HOME AUTOMATION

In this work, the wireless sensor nodes are equipped with ZigBee PRO home automation standard [26]. ZigBee PRO is a wireless communication specification based on IEEE 802.15.4 standard designed for low-data rate, low-power, and low-latency applications. The wireless sensor nodes are configured to operate in the 2.4 GHz industrial, scientific and medical (ISM) radio bands with data rates up to 250 Kbit/s and transmit power of 0 dBm.

A mesh topology is used where nodes can communicate directly, indirectly and non-hierarchically, minimizing the reliance on a particular node. In addition, ZigBee PRO utilizes a reactive routing protocol, ad hoc on-demand distance vector (AODV) mechanism where routing paths between source and destination nodes are formed only upon request, managed by the coordinator and routers of the network. A routing path with the least path cost (summation of link costs of nodes that forms the routing path) will be selected. In wireless microcontroller JN5168 [25], link cost is measured with the link quality indicator (LQI). The LQI shown in (1) is a characterization of the received signal strength performed for every received packet as an integer ranging from 0x00 to 0xff. LQI values of 0x00 and 0xff are associated with the lowest and highest quality signals respectively, in which the LQI value is uniformly distributed between these limits.

$$cost\{P\} = cost\left\{\sum_{i=1}^{L} LQI_{D_i D_{i+1}}\right\} \tag{1}$$

where P is the path cost, $L$is the number of hops along the routing path, and LQI is the link cost between device i (D_i) and its next hop towards destination node (D_{i+1}).

B. WIRELESS SENSOR NETWORK TESTBEDS IN A BUILDING

A WSN testbed is deployed in a single level administrative office within a building (WSN@Solaris) approximately 900 m^2. Fig. 1 illustrates the floor plan of WSN@Solaris and also the deployment locations of 20 routers and a coordinator. The office is divided into two parts. Firstly, the centralized open-concept administrative area consists of chest height desk partitions and was occupied by approximately 24 employees. Secondly, the dense partitioned rooms occupying the south and west sections of office meeting rooms, laboratories, and pantry. The office is furnished with carpet floor and false ceilings.

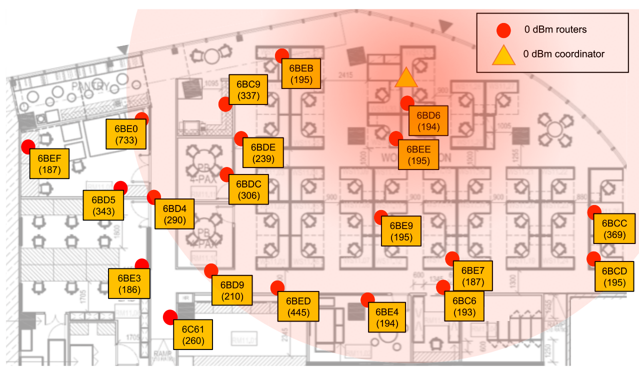


FIGURE 1. Wireless sensor network testbed deployed in a 900 square meter, single level administrative office in Solaris Building, Singapore. The testbed consists of 20 routers and a coordinator deployed in a scattered manner along the walls at the height of 0.5 m and among occupied workstations.

Routers, denoted as red circles in Fig. 1, are deployed in a scattered manner within WSN@Solaris. They are either located among the workstations and along the walls of rooms and corridors, at a height of approximately 0.5 m. The coordinator, denoted as a yellow triangle in Fig. 1, is deployed where nodes located further away are subjected to greater signal attenuation of partitioned rooms, while nodes closer to the coordinator are subjected to human activities (open-concept administrative area).

C. EXTRACTION OF ROUTING PATH INFORMATION FROM WIRELESS SENSOR NODES

As opposed to adopting the use of external sniffers within WSN testbeds to obtain link quality information, Neighbor Table (NT) and Routing Table (RT) information are extracted from WSN routers periodically. The use of sniffers is not practical due to two factors. Firstly, the resources needed are significant and grow exponentially with increasing network size. Secondly, the information collected on the sniffers may not be representative, as sniffers are subjected to packet distortion from interference. For instance, external devices operating in the same spectrum may transmit at the same time, resulting in the sniffer receiving a distorted packet.

A router's NT contains information about its neighboring nodes, consisting of their network address and respective RSSI value, depth, relationship to the router, and device type. If node *A* is found in node *B*'s NT, nodes *A* and *B* have established communication in the last 60 sec. Vice versa, if a previously existing node *A*is no longer found in node *B*'s NT, communication between them has failed. A router also holds information about the state of established routing paths relative to itself and desired destination nodes. This information is stored as entries in the RT, consisting of the destination and next hop addresses.

NT and RT information are sampled from routers in the WSN@Solaris at an approximately 25 minutes interval continuously for 6 consecutive days. Routing paths towards the coordinator are computed from collected routers' NT and RT. Table 1 presents the pseudo-code (Algorithm 1) developed for collating nodes that form the individual link along the routing paths. In Algorithm 1, the source node first checks for the destination node in its RT (the destination node is always the coordinator). If a coordinator is found, the source node will forward the message to the next hop, assuming it has direct/indirect connection with the coordinator. This process is repeated until the coordinator is not found. Subsequently, the latest next hop will check its NT for a coordinator. If a coordinator is found, the routing path between the original source node and coordinator is collated. Otherwise, the collation of routing path is considered unsuccessful, meaning no routing path is available between source router and the coordinator at the moment of data query.

In ZigBee PRO, keep-alive pings are broadcasted by routers every 15 seconds to inform the network that it is alive. An existing link between two routers is considered missing if four consecutive pings are not received (i.e. 60 sec). If so, all information associated with the neighbor is erased from the NT and RT. For example, if four consecutive keep-alive pings

TABLE 1. Algorithm 1–Pseudo code used to trace and collate node-to-node routing paths from sampled neighbor table and routing table.

```
Input variables:
S: Source node
C: Destination node (coordinator)
H: Next hop
R: Relay node
RT: Routing Table
NT: Neighbor Table
P: Routing Path
Method:
(1) P = {S} % Initiating the routing path with source node address
(2) Given a list of NT and RT of 10 minutes window period
(3) R = S % Replace source node as relay node
(4) While C is found in RT of R
(5)          P = {P, H} % Insert next hop address into the routing path
(6)          R = H % Replace next hop as relay node
(7)          % Repeat while loop until C is not found in RT of R
(8) If C is found in NT of R
(9)          P = {P, C} % Routing path towards C is found
(10) Else % C is not found in both NT and RT of R
(11)         P = {P, "failed"} % Routing path is not found
```

from node *A* are unheard, node *B* then proceeds to remove all of node $A's$ related information from its NT and RT. This removal is reflected as changes or failures in the computed routing paths in Algorithm 1.

IV. ROUTING STABILITY IN A BUILDING

In this section, the usage and stability of routing paths in WSN@Solaris are analyzed. Instead of monitoring E2E performance of routing paths, the next hops along the routing paths relative to individual source nodes are monitored. The relative routing path usage count, unique next hop's usage rate and SFC between unique next hops are proposed as indicators of routing stability.

A. ROUTERS' RELATIVE USAGE COUNTS IN ROUTING PATHS

1) THE IMPACT OF LEAST HOP COUNTS ON USAGE OF ROUTERS IN ROUTING PATHS

The number of times a router is used as part of routing paths is marked in orange in Fig. 1. An estimated 190 unique routes were expected from individual routers over six days (values may vary depending on the query latency). Abnormally high routing path usage count can be observed on certain routers as compared to others in similar regions. For example, routers *6BCC*, *6BE0* and *6BED* have 369, 733 and 445 routing path usage counts respectively.

For illustration purposes, the pink circle in Fig. 1 denotes the approximate reception range of the coordinator (based on the routers' reception of coordinator observed in NTs). It is observed that nodes deployed closer to the end of the reception range of coordinator were utilized more often than those deployed nearer to the coordinator. The route with the lowest depth (least hop) from the coordinator will be selected if the path costs of all possible routing options are the same [26]. When constructing a routing path, as long as the destination node is within reception range, a router will opt for direct communication. Similarly, nodes that are not within the reception range of the coordinator will connect to routers that are at the edge of the coordinator's reception range. This is done to minimize the total hop count. As such, routers at the edge of the coordinator's reception range were often used as a relay for other nodes deployed further away.

2) USAGE RATE AND THE IMPACT OF DOMINANT NEXT HOPS

To better understand the phenomenon of abnormally high routing path usage count, we took a look closer at the unique next hops of individual source routers. Unique next hops are referred to as the routers observed over a period, which were chosen by the routing protocol as the first hop relay nodes between a source node and the coordinator. The usage counts and NT failure counts of unique next hops in Table 2 are computed from the routing paths collected over six days, using Algorithm 1 from Table 1. For example, a total of 192 routing paths were generated from source node *6BC6*. Among the 190 of the paths, coordinator *6209* was used as the next hop. In five of the 190 paths, coordinator *6209* was not found in the source node *6BC6*'s NT. Evidently, a source node shows multiple unique next hops. Their usage rates vary, ranging from 0.5% to 100%. A unique next hop with 100% usage rate signifies that the respective source router only has one connection towards the coordinator, as seen on source nodes *6BD6*, *6BE4*, *6BE7*, *6BE9* and *6BEE* in Table 2.

Routers *6BD4* and *6BCD* from Table 2 are used as examples to illustrate the differences in dominating next hops. Router *6BD4* has five unique next hops over the period of six days, while router *6BCD* has three. The usage rate of router *6BD4*'s unique next hops – routers *6C61*, *6BE0*, *6BDC*, *6BC9 and*coordinator 6209 – ranged from 0.6% to 36% of its total collected routing paths. In comparison, the usage rates of router *6BCD*'s unique next hops – routers *6BCC*, *6BE7*, and coordinator *6209*–ranges from 1% to 89.7%. Referring to Table 2, router *6BCD* was connected directly to router *6BCC* for 89.7% of its total E2E routing paths. In contrast, the most connected next hop of router *6BD4* accounts for only 36%. The greater usage rate of dominant next hop signifies a more stable and robust connection as compared to non-dominant ones (minority next hop(s)).

The greater usage of dominant next hop explains why certain routers have higher routing path usage counts. Fig. 2 illustrates three routing paths taken from router *6BCD* to the coordinator *6209* initiated by three different next hops. As shown in Fig. 2a, despite the obstructions of workstations, chest height partitions and a building pillar, a direct communication between router *6BCD* and the coordinator is possible. However, router *6BCD* was dominantly connected to intermediate router *6BCC* with a usage rate of 89.7%. Since a routing path only re-constructs when there is a link failure, router *6BCD's* consistent connection with router *6BCC* showed a greater long-term stability than the direct connection to the coordinator. This dominant next hop connection with router *6BCC* leads to the abnormally high routing path usages count of router *6BCC* at 369 (refer to Fig. 1). Similar observations were found for router *6BE0* and *6BED* with 733 and 445 routing path usage counts respectively.

TABLE 2. The usage counts and rates of unique next hops that connect respective source routers to the coordinator in WSN@Solaris.

Source node	Unique next hop towards the coordinator	Usage counts of unique next hop (%)	Counts of unique next hop with NT failure
Router *6BC6*	Coordinator *6209*	190 (~98.9%)	5
	Router *6BCC*	1 (~0.5%)	1
	Router *6BE7*	1 (~0.5%)	0
Router *6BD4*	Coordinator *6209*	21 (12%)	5
	Router *6BC9*	1 (~0.6%)	1
	Router *6BDC*	63 (~36%)	18
	Router *6BE0*	46 (~26.2%)	5
	Router *6C61*	44 (~25.1%)	15
Router *6BC9*	Coordinator *6209*	187 (~99.5%)	26
	Router *6BEB*	1 (~0.5%)	0
Router *6BCC*	Coordinator *6209*	192 (~99.5%)	13
	Router *6BC6*	1 (~0.5%)	0
Router *6BCD*	Coordinator *6209*	18 (~9.23%)	11
	Router *6BCC*	175 (~89.7%)	7
	Router *6BE7*	2 (~1%)	1
Router *6C61*	Router *6BD4*	20 (~10.2%)	1
	Router *6BD9*	4 (~2.1%)	0
	Router *6BED*	171 (~87.7%)	1
Router *6BD5*	Router *6BD4*	13 (~7%)	2
	Router *6BDC*	1 (~0.5%)	0
	Router *6BE0*	170 (~91.4%)	1
	Router *6BE3*	2 (~1.1%)	2
Router *6BD6*	Coordinator *6209*	194(100%)	0
Router *6BD9*	Coordinator *6209*	167 (~85.6%)	30
	Router *6BDC*	5 (~2.6%)	0
	Router *6BED*	17 (~8.7%)	0
	Router *6BEE*	6 (~3.1%)	0
Router *6BDC*	Coordinator *6209*	155 (~81.1%)	12
	Router *6BC9*	1 (~0.5%)	0
	Router *6BD4*	10 (~5.2%)	3
	Router *6BD9*	6 (~3.1%)	3
	Router *6BED*	1 (~0.5%)	1
	Router *6BEE*	18 (~9.4%)	3
Router *6BDE*	Coordinator *6209*	194 (~99.5%)	0
	Router *6BC9*	1 (~0.5%)	0
Router *6BE0*	Coordinator *6209*	135 (~70.7%)	8
	Router *6BD4*	56 (~29.3%)	0
	Router *6BDC*	1 (~0.5%)	1
Router *6BE3*	Router *6BD5*	156 (~85.2%)	0
	Router *6BD9*	3 (~1.6%)	1
	Router *6BDC*	21 (~11.5%)	4
	Router *6BED*	3 (~1.6%)	2
Router *6BE4*	Coordinator *6209*	194 (100%)	9
Router *6BE7*	Coordinator *6209*	174 (100%)	7
Router *6BE9*	Coordinator *6209*	195 (100%)	0
Router *6BEB*	Coordinator *6209*	5 (~2.6%)	2
	Router *6BC9*	145 (~74.7%)	14
	Router *6BDE*	44 (~22.7%)	4
Router *6BED*	Coordinator *6209*	189 (~99%)	13
	Router *6BD9*	2 (~1%)	1
Router *6BEE*	Coordinator *6209*	194 (100%)	21
Router *6BEF*	Router *6BDC*	3 (~1.6%)	3
	Router *6BE0*	184 (~98.4%)	1

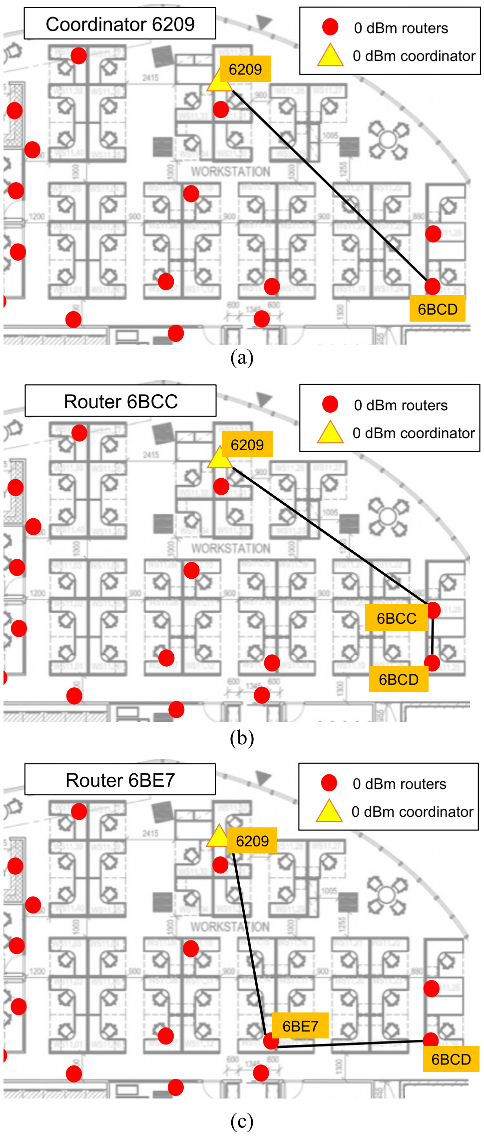


FIGURE 2. **a, b and c. Three routing paths generated from source router *6BCD* to coordinator *6209*. These routing paths illustrate the use of three different unique next hops of router *6BCD*. They are (a) coordinator *6209*, (b) router *6BCC* and (c) router *6BE7*.**

B. PROBABILITY OF LINK FAILURE BASED ON UNIQUE NEXT HOP'S USAGE RATE

The number of failures found in unique next hop(s) in WSN@Solaris is also shown in Table 2. These failures account for the periods in which a particular next hop was missing in the respective source node's NT. Similar to [23], the number of neighboring nodes vary constantly throughout its deployment lifetime. Fig. 3 illustrates the combined next hop failure rate based on routers' unique next hop usage rate in WSN@Solaris. It is observed that 17 of the 20 routers operate with a dominant unique next hop at a usage rate of at least 81.1%. This suggests that routing paths are rather consistent and are used as long-term routing solutions.

Of the 1116 times where next hops with over 90% usage rate were utilized, 96 of them (8.6%) experienced periods in which the particular next hop was missing from the source

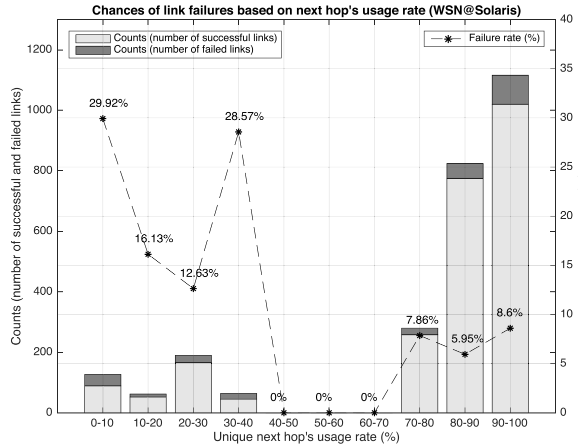


FIGURE 3. **Probability of link failures based on unique next hops' usage counts in WSN@Solaris.**

router's NT. On the other hand, NT failure rate increased to 29.92% when the usage rate of unique next hop dropped to less than 10%. In other words, as the unique next hop's usage rate decreases, the probability of experiencing NT failure increases. Decreasing usage rate suggests that nodes are utilized only briefly before switching back to a dominant next hop. Increasing NT failure with decreasing usage rate implies that the affected next hops are short-lived and unsustainable, likely due to poor node-to-node connectivity. Since a router may be used as a relay for nodes deployed further in the network, a less dominant next hop poses potential network bottlenecks. Therefore, it is critical to identify them so that appropriate measures can be put in place to minimize their usage.

C. ROBUSTNESS OF DOMINANT NEXT HOPS

Fig. 4 - 8 show the switching frequency count (SFC) for five source routers in WSN@Solaris. SFC measures the number of times the next hops relative to a source node changes. An increase in SFC signifies frequent link failures and re-routing between affected source nodes. Fig. 4 - 8 also illustrate the connection periods of respective source routers between dominant next hop and minority ones. The peak(s) indicates the period(s) when minority next hop(s) was used. Each period represents approximately 25 minutes, where the greater the peaks, the longer it takes for the source router to revert back to its dominant next hop.

In Fig. 4, source router *6BE9* with 0 *SFC* was connected to coordinator *6209* (dominant next hop) throughout its deployment cycle. In Fig. 5, source router *6BED* with 2 *SFC* had switched to a minority source next hop momentarily before switching back to the dominant one. In these examples, source routers with relatively low *SFC* have consistent connections with their dominant next hops. In cases where the route failed, the minority next hops took over as routing redundancies, but were only utilized for a brief period before returning to the dominant next hop. These dominant next hops can be seen to provide long-term routing options compared to minority ones.

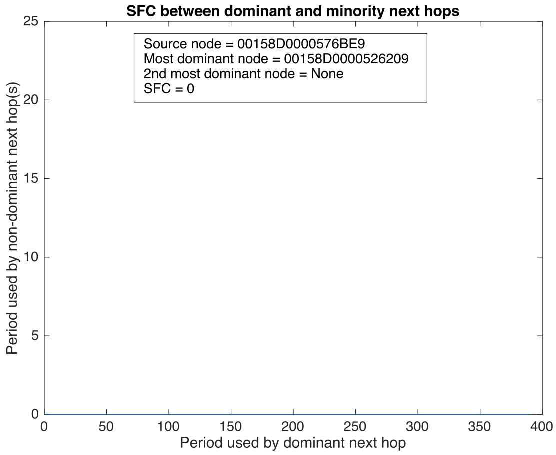


FIGURE 4. Switching Frequency Count between source router *6BE9* and its dominant next hop coordinator *6209*.

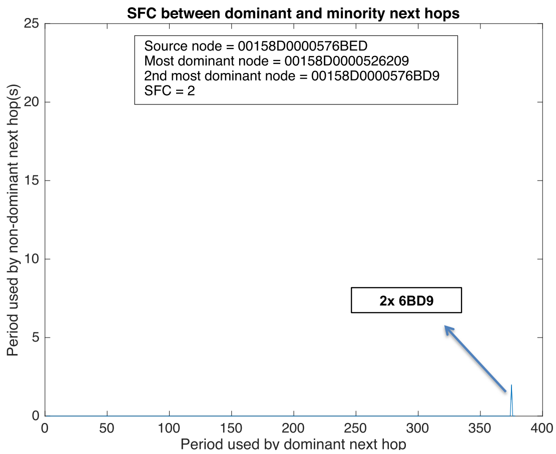


FIGURE 5. Switching Frequency Count between source router *6BED* and its dominant next hop coordinator *6209*.

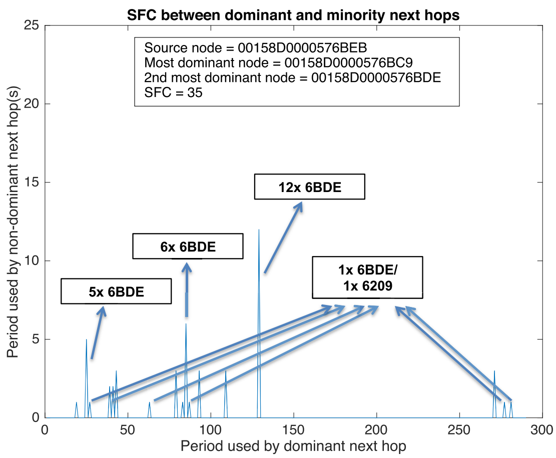


FIGURE 6. Switching Frequency Count between source router *6BEB* and its dominant next hop router *6BC9*.

In Fig. 6, router *6BEB* is observed to switch between its dominant next hop and minority ones for over 35 times. Similarly, router *6BD4* in Fig. 7 has a *SFC* of 42 during the same period. Referring to Table 2, the dominant next

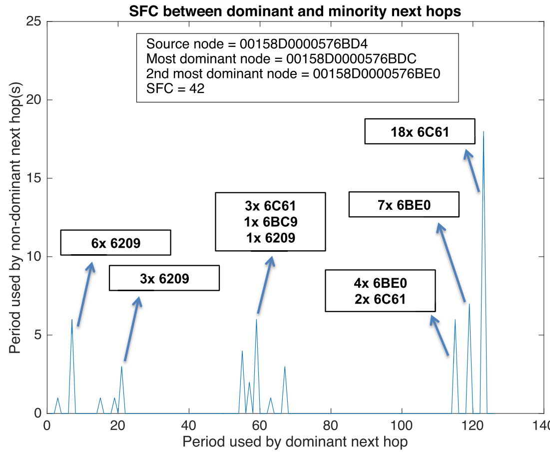


FIGURE 7. Switching Frequency Count between source router *6BD4* and its dominant next hop router *6BDC*.

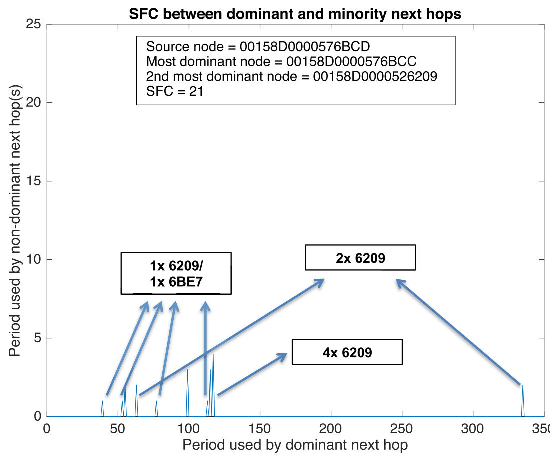


FIGURE 8. Switching Frequency Count between source router *6BCD* and its dominant next hop router *6BCC*.

hop usage rates of routers *6BEB* and *6BD4* are 74.7% and 36% respectively. This difference in usage rate highlighted that a dominant next hop may also be subjected to frequent disconnections and poor reception quality. Router *6BEB's* high usage of dominant next hop was segmented into multiple periods. It took minority next hops longer periods to fail before switching back to the dominant next hop. On the other hand, router *6BD4* experiences undesirable constant switching between next hops. Bezahaf *et al.* [22] highlighted that in a WLAN testbed (IEEE 802.11 a/b/g), routing paths with higher dominance rate are found to have higher routing stability and lesser oscillations. This work has shown that such observations are not present in low-power WSNs. Despite having dominant routes, frequent switching of next hops was observed.

V. MONITORING LONG-TERM ROUTING STABILITY

A. IMPACT OF POOR ROUTING STABILITY ON WSN RELIABILITY

In the previous sections, the routing stability of WSN@ Solaris was evaluated based on their historical connectivity.

Whilst, it is impossible to account for all dynamics of the deployed environment, the routing path usage counts, usage rates of unique next hops and SFC serve as useful indicators about the health of routing paths, taking into account their ability to withstand and adapt to changes in the environment.

Given that AODV protocol re-routes only upon link failure, a dominant next hop with low SFC can be seen as a link that provides a long-term solution relative to minority ones. Ironically, referring to Table 2, dominant next hops may also operate with the possibility of NT failures. This is because routers often opted for longer distance communication to minimize hop counts, even if the link quality may not be optimal. In addition, the choice in next hop also depends on the routing options available. For instance, a constant switching of next hops can be due to the source node lacking a ''good'' routing option rather than poor routing path selection of routing protocol and the influence from harsh environment.

Fig. 6, 7 and 8 are examples of source nodes with relatively high SFCs. Multiple short peaks are observed in these figures, suggesting that increasing SFCs are primarily contributed by the use of minority next hops that are short-lived, lasting for only one period. Regardless of the usage rate of dominant next hop, the usage of a minority one has to fail first before triggering re-routing process for the dominant next hop to be reselected. The need for the minority next hop to fail before switching to a better routing option can be seen as a poor utilization of energy. The route discovery process requires the synchronization of all active nodes in the network to search for the ''best'' possible routing options on behalf of affected nodes. Doing so introduces high overhead and energy consumption. The consistent use of unsustainable minority next hops will have serious implications on the overall lifespan of the WSN.

Furthermore, care needs to be taken for routers with abnormally high routing path usage counts since they play a key role in relaying packets for nodes deployed further in the network. And lastly, a dominant next hop with high usage rate may also experience node-to-node disconnections, suggesting a suboptimal routing choice. The unsustainable characteristics of minority unique next hops and higher probability of finding NT failures demonstrate the importance of evaluating routing stability.

B. IMPORTANCE OF MONITORING LONG-TERM ROUTING STABILITY

Similar to link stability, long-term routing stability is observed to vary in real-world WSN deployment. It should be noted that WSN nodes are often designed with redundancy features for network self-healing and to minimize abrupt changes in a network. These features include retransmissions, consecutive keep-alive messages, network re-routing, which are performed automatically by the ZigBee stack and are transparent to the user [26]. As such, any frequent changes along the routing paths are hidden from the user point of view. Therefore, information about the health of long-term routing stability is critical for the user or routing protocol to identify unstable regions in the network that are subjected to frequent link failures.

Relative routing path usage count, usage rates of unique next hops and SFC are shown to be useful indicators of the health of a routing path and finding network bottlenecks. For instance, a source node with a dominant next hop of low usage rate and high SFC signifies that it has limited stable routing alternatives. In addition, a node can measure its routing stability by monitoring the changes in its next hop without additional overhead. In other words, our proposed approach is applicable to other types of reactive routing protocols without modifications of existing routing mechanisms. These protocols are for example, ad hoc on-demand multipath distance vector (AOMDV) [28] and dynamic source routing (DSR) [29], which react to link failures with route changes.

The assessment of long-term routing stability complements rather than replaces existing instantaneous link quality estimation techniques. Instantaneous assessment is necessary for evaluating the quality of routing options under dynamic environmental settings, while long-term routing instability highlights the potential bottlenecks in the network. For instance, if two routing options are assessed to have the same link quality, the more dominant next hop based on usage rate should be chosen, since the minority next hops are more likely to fail.

VI. CONCLUSION

We have evaluated real-world WSN routing stability using historical routing paths generated from ZigBee PRO implemented nodes deployed. Unlike typical assessments of link stability, routing stability also takes into account the long-term adaptability and robustness of generated routing paths in the face of environmental dynamics. Three parameters — relative routing path usage count, usage rate of unique next hops and SFC — are proposed as indicators of routing stability. Our findings show that routing stability is subjected to not only the quality of a link, but also the implemented routing protocols, deployed environment and routing options available. As a result, certain routers may turn into network bottlenecks if they have relative high usage as relay nodes, frequent switching between next hops, and repeated usage of minority next hops. This work demonstrates the importance of evaluating routing stability and finding network bottlenecks. For instance, it is found that the probability of link failures can be as high as 29.9% when a next hop's usage rate falls below 10%, suggesting that minority next hops are subjected to more link failures and are short-lived. Over dependency on minority next hops can lead to further network instability and energy wastage.

Future work includes implementing a routing mechanism to predict potential network bottlenecks. A router having knowledge about its routing stability will potentially make better decisions on route selection.

REFERENCES

[1] *Internet of Things: Wireless Sensor Network*, Int. Electrotech. Commission, Geneva, Switzerland, 2015.

[2] U. B. Desai, B. N. Jain, and S. N. Merchant, "Wireless sensor networks: Technology roadmap," in *Proc. Workshop Wireless Sensor Netw.*, Dept. Inf. Technol., Ministry Inf. Commun. Technol., New Delhi, India, Tech. Rep., Apr. 2007.

[3] E. Aguirre, P. Lopez-Iturri, L. Azpilicueta, J. J. Astrain, J. Villadangos, and F. Falcone, "Analysis of wireless sensor network topology and estimation of optimal network deployment by deterministic radio channel characterization," in *Proc. 1st Int. Electron. Conf. Sensors Appl.*, vol. 1, Jun. 2014, pp. 3766—3788. doi: 10.3390/s150203766.

[4] K. Srinivasan and P. Levis, "RSSI is under appreciated," in *Proc. 3rd IEEE Workshop Embedded Netw. Sensors (EmNets)*, Cambridge, MA, USA, 2006.

[5] A. Cerpa, N. Busek, and D. Estrin, "SCALE: A tool for simple connectivity assessment in lossy environments," Univ. California, Los Angeles, Los Angeles, CA, USA, CENS Tech. Rep. #21, Sep. 2003.

[6] J. Zhao and R. Govindan, "Understanding packet delivery performance in dense wireless sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst.*, 2003, pp. 1–13.

[7] K. Srinivasan, M. A. Kazandjieva, S. Agarwal, and P. Levis, "The β-factor: Measuring wireless link burstiness," in *Proc. 6th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, New York, USA, 2008, pp. 29–42.

[8] G. Horvat, S. Rimac-Drlje, and D. Žagar, "Fade depth prediction using human presence for real life WSN deployment," *Radioengineering*, vol. 22, pp. 758–768, 2013.

[9] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis, "An empirical study of low-power wireless," *ACM Trans. Sensor Netw.*, vol. 6, no. 2, pp. 16:1–16:49, Mar. 2010.

[10] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis, "Understanding the causes of packet delivery success and failure in dense wireless sensor networks," in *Proc. 4th Int. Conf. Embedded Netw. Sensor Syst., SenSys*, New York, NY, USA, vol. 6, 2006, pp. 419–420.

[11] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," in *Proc. 1st Annu. IEEE Commun. Soc. Conf. Sensor Ad Hoc Commun. Netw. (SECON)*, Oct. 2004, pp. 517–526.

[12] M. H. Alizai, O. Landsiedel, K. Wehrle, and A. Becher, "Challenges in short-term wireless link quality estimation," in *Proc. 7th GI/ITG Fachgespraech Wireless Sensor Netw. (FGSN)*, Berlin, Germany, vol. 8, no. 2, Feb. 2008, pp. 27–30.

[13] A. Cerpa, J. L. Wong, M. Potkonjak, and D. Estrin, "Temporal properties of low power wireless links: Modeling and implications on multi-hop routing," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Champaign, IL, USA, May 2005, pp. 414–425.

[14] S. Lin, G. Zhou, K. Whitehouse, Y. Wu, J. A. Stankovic, and T. He, "Towards stable network performance in wireless sensor network," in *Proc. 30th IEEE Real-Time Syst. Symp.*, Dec. 2009, pp. 227–237.

[15] J. Miranda, R. Abrishambaf, T. Gomes, P. Goncalves, J. Cabral, A. Tavares, and J. Monteiro, "Path loss exponent analysis in wireless sensor networks: Experimental evaluation," in *Proc. IEEE Int. Conf. 11th Ind. Inform. (INDIN)*, Jul. 2013, pp. 54–58.

[16] T. Watteyne, S. Lanzisera, A. Mehta, and K. S. J. Pister, "Mitigating multipath fading through channel hopping in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, May 2010, pp. 1–5.

[17] D. Puccinelli and M. Haenggi, "Multipath fading in wireless sensor networks: Measurements and interpretation," in *Proc. Int. Conf. Wireless Commun. Mobile Comput. (IWCMC)*, New York, NY, USA, 2006, pp. 1039–1044.

[18] S.-Y. Han and N. B. Abu-Ghazaleh, "On the effect of fading on adhoc networks," May 2005, *arXiv:cs/0504002v1*. [Online]. Available: https://arxiv.org/abs/cs/0504002v1

[19] R. Akl, D. Tummala, and X. R. Li, "Indoor propagation modeling at 2.4 GHz for IEEE 802.11 networks," in *Proc. 6th IASTED Int. Multi-Conf. Wireless Opt. Commun.*, Banff, AB, Canada, 2004.

[20] P. Pettinato, N. Wirström, J. Eriksson, and T. Voigt, "Multi-channel two-way time of flight sensor network ranging," in *Proc. 9th Eur. Conf. Wireless Sensor Netw. (EWSN)*, 2011, pp. 163–178.

[21] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[22] M. Bezahaf, L. Iannone, M. D. Amorim, and S. Fdida, "Insights into the routing stability of a multi-hop wireless testbed," in *Ad Hoc Networks*. Berlin, Germany: Springer, 2010, pp. 82–97.

[23] B. Pavkovic, F. Theoleyre, D. Barthel, and A. Duda, "Experimental analysis and characterization of a wireless sensor network environment," in *Proc. 7th ACM Workshop Perform. Eval. Wireless Ad Hoc, Sensor, Ubiquitous Netw.*, Bodrum, Turkey, 2010, pp. 25–32.

[24] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst. (SenSys)*, New York, NY, USA, 2003, pp. 14–27.

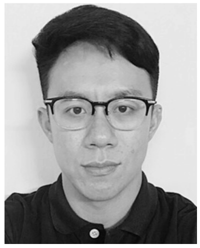
[25] *JN5168-001-Myy Datasheet*, NXP Lab., Glasgow, U.K., 2013.

[26] *ZigBee PRO Stack User Guide*, NXP Lab., Glasgow, U.K., 2014.

[27] K. Ishibashi and K. Yamaoka, "A study of network stability on wireless sensor networks," in *Proc. IEEE 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Cambridge, U.K, Sep. 2015, pp. 96–101.

[28] 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.

[29] 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.



CHENG LEONG LIM received the B.Eng. degree (Hons.) in mechatronics from the University of Glasgow, Glasgow, U.K., in 2013, where he is currently pursuing the Ph.D. degree in electronics and electrical engineering.

His research interests include fuzzy modeling, optimizing communication reliability of wireless sensor networks, and artificial intelligence for Industry 4.0. He was a recipient of the 2014 Professor Wu Dao Quan Outstanding Engineering Student Award from the University of Glasgow.

CINDY GOH received the Ph.D. degree from the University of Glasgow, U.K., in 2004. From 2011 to 2013, she was an Assistant Professor with the University of Glasgow, Singapore (UGS), where she became an Associate Professor and the Director of research programs, in 2013 and she is currently the Director where she has overall responsibility for its strategy and management. Her work has been published in internationally peer-reviewed journals. Her research interests include intelligent optimization and data analytics for optimal decision-making and design to advance the state-of-the-art in complex engineering systems, energy and transport networks, and smart manufacturing. She is a Founding Member of the International Union of Radio Science Committee, Singapore.

YUN LI (S'87–M'90–SM'17) received the B.S. degree in electronics science from Sichuan University, Chengdu, China, in 1984, the M.E. degree in electronic engineering from the Electronic Science and Technology of China, Chengdu, China, in 1987, and the Ph.D. degree in parallel computing and control from the University of Strathclyde, Glasgow, U.K., in 1990.

Since 1989, he has been a Control Engineer with the U.K. National Engineering Laboratory. Since 1990, he has been a Postdoctoral Research Engineer with Industrial Systems and Control Ltd. From 1991 to 2018, he was a Lecturer, a Senior Lecturer, and a Professor with the University of Glasgow and served as the Founding Director of the University of Glasgow Singapore. He is currently a Professor with the Dongguan University of Technology, Dongguan, China, and also with the University of Strathclyde. He has published more than 250 papers, two of which are among the 10 most popular articles in the IEEE TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY and the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS. He has authored the step-by-step interactive evolutionary algorithm (EA) courseware, EA_demo, published online, in 1997. His current research interests include artificial intelligence for Industry 4.0.

Prof. Li is an Associate Editor of the IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION and of the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE. He is a Chartered Engineer in the U.K. and chaired the EPSRC funded first Industrial Systems in the Digital Age conference, Looking Beyond Industry 4.0, Glasgow, in 2017.