Characterizing Data Deliverability of Greedy Routing in Wireless Sensor Networks

Jinwei Liu, *Student Member, IEEE*, Haiying Shen, *Senior Member, IEEE*, Lei Yu, Husnu Saner Narman, Jiannan Zhai, Jason O. Hallstrom, *Senior Member, IEEE*, and Yangyang He

Abstract—As a popular routing protocol in wireless sensor networks (WSNs), greedy routing has received great attention. The previous works characterize its data deliverability in WSNs by the probability of all nodes successfully sending their data to the base station. Their analysis, however, neither provides the information of the quantitative relation between successful data delivery ratio and transmission power of sensor nodes nor considers the impact of the network congestion or link collision on the data deliverability. To address these problems, in this paper, we characterize the data deliverability of greedy routing by the ratio of successful data transmissions from sensors to the base station. We introduce η-guaranteed delivery which means that the ratio of successful data deliveries is not less than η, and study the relationship between the transmission power of sensors and the probability of achieving η-guaranteed delivery. Furthermore, with considering the effect of network congestion, link collision, and holes (e.g., those caused by physical obstacles such as a lake), we provide a more precise and full characterization for the deliverability of greedy routing. Extensive simulation and real-world experimental results show the correctness and tightness of the upper bound of the smallest transmission power for achieving η-guaranteed delivery.

Index Terms—Wireless sensor networks, greedy routing, data deliverability, energy-efficiency

1 Introduction

Wireless sensor networks (WSNs) have been increasingly deployed for environment monitoring [1], [2]. Usually sensor nodes (sensors in short) are distributed over a geographic region of interest and transmit the sensed data to a remote base station using multi-hop routing. Thus, data delivery, as a fundamental function of WSNs, has received great attention. Considerable research efforts have been devoted to studying the reliability [3], timeliness [4] and energy-efficiency [5], [6] of data delivery.

High delivery ratio with low energy consumption is a challenging issue of data delivery in WSNs. Many routing protocols have been proposed to address this challenge, including data-centric [7], hierarchical [8] and location-based [9], [10] design. Among these protocols, the location-based greedy routing (greedy routing in short) protocol [9], [10] is particularly attractive for large-scale sensor networks due to its simplicity, efficiency and scalability, and thus has been widely exploited. In this protocol, each node makes routing decision with only local knowledge and forwards the packet to its neighbor that has the smallest distance to the destination until the packet reaches the destination.

A well-known problem with greedy routing is that it fails at a node called *void node* that has no neighbor closer to the destination. To handle this problem, many previous works [11], [12], [13] theoretically analyzed the relationship between the transmission radius and the deliverability of greedy routing. Specifically, Wan et al. [11] studied the critical transmission radius (i.e., smallest transmission radius) for greedy routing to ensure that packets can be delivered between any source-destination pairs in randomly deployed wireless ad hoc networks. Wang et al. [12] further derived higher accurate asymptotic bounds on the critical transmission radius. Yang et al. [13] studied the relationship between the critical transmission power (i.e., smallest transmission power) and the probability of guaranteed data delivery from all sensors to the central base station (referred to as many-to-one).

These works have studied the deliverability of greedy routing in terms of probability of guaranteeing all deliveries (i.e., probability of guaranteed delivery) and the transmission condition (e.g., critical transmission power/radius) to eliminate void nodes in the network. However, no previous works have studied the relationship between the transmission power and the packet delivery ratio of greedy routing, which is the ratio of the nodes that successfully deliver their data to the base station. We call these nodes *delivery-success nodes*, otherwise, *delivery-failure nodes*. The work in [14] demonstrates that data delivery in WSNs is inherently faulty and unpredictable, and thus the fault tolerant protocols are necessary for sensor applications and the protocols should ensure reliable data delivery while minimizing energy consumption [15]. Therefore, the

- *J. Liu is with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634. E-mail: jinweil@clemson.edu.*
- *H. Shen is with the Department of Computer Science, University of Virginia, Charlottesville, VA 22904. E-mail: hs6ms@virginia.edu.*
- *L. Yu is with the School of Computer Science, Georgia Institute of Technology, Atlanta, GA 30332. E-mail: leiyu@gatech.edu.*
- *H.S. Narman is with the Department of Computer Science, Marshall University, Huntington, WV 25755. E-mail: narman@marshall.edu.*
- *J. Zhai and J.O. Hallstrom are with the Institute for Sensing and Embedded Network Systems Engineering, Florida Atlantic University, Boca Raton, FL 33431. E-mail: {jzhai, jhallstrom}@fau.edu.*
- *Y. He is with the School of Computing, Clemson University, Clemson, SC 29634. E-mail: yyhe@clemson.edu.*

Manuscript received 23 Mar. 2017; revised 7 June 2017; accepted 26 July 2017. Date of publication 9 Aug. 2017; date of current version 2 Feb. 2018. (Corresponding author: Haiying Shen.)
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TMC.2017.2737005

relationship between transmission power and packet delivery ratio of greedy routing is of great interest for WSN designers in practice. It helps to infer the number of delivery-failure nodes with a given transmission power, and provides insights on the impact of void nodes on the number of delivery-failure nodes. Accordingly, the designers can determine whether it is acceptable to use a relatively lower transmission power for sensors by estimating the number of *delivery-failure nodes*, since a limited number of delivery-failure nodes may be acceptable for possible reasons like redundant node deployment. Thus, η-guaranteed delivery is not trivial [16], [17].

Another limitation of these previous works is that they neglect the impact of network congestion and link collision on the deliverability of greedy routing in theoretical analysis, though these two factors are also well-known causes for packet delivery failure in WSNs [18], [19], [20]. Since greedy forwarding decisions are made based on location information without the knowledge of traffic flows in the WSN, it could generate spatial congestion and collision, which may reduce packet delivery ratio. The impact of network congestion and collision on data deliverability poses a challenge to the characterization of data deliverability.

In this paper, we analyze the greedy routing deliverability for many-to-one data delivery in WSNs. Unlike the previous work [13] that considers the deliverability in terms of the probability of guaranteeing all sensors to successfully send their data to the base station, we consider the deliverability in terms of the ratio of delivery-success nodes. In particular, we study the critical transmission power required to ensure that the ratio of delivery-failure nodes does not exceed a threshold with a given probability. We also consider the impact of network congestion and link collision on the deliverability in the study. Compared with the previous work [13], our results characterize the deliverability in general sense and is much more practical with the additional consideration of the two factors. The main contributions of this paper are as follows:

- We introduce the concept of η-guaranteed delivery, which guarantees that the ratio of delivery-failure nodes is at most $1-\eta$. Based on this concept, we study the relationship between the critical transmission power and the ratio of delivery-failure nodes, which provides a more general characterization of the many-to-one deliverability of greedy routing compared to the previous works.
- We derive analytical upper bounds on critical transmission power for the η-guaranteed delivery under Signal-to-Interference-plus-Noise-Ratio (SINR in short) [21] model. Simulation and real-world experimental results are provided to validate our analysis results.
- We further conduct our analysis considering the effects of network congestion, link collision and holes on data deliverability, and provide a more accurate characterization of the deliverability of greedy routing.

The remainder of this paper is organized as follows. Section 2 reviews the related work. Section 3 describes the problem definition and the system model used in this paper. In Sections 4 and 5, we derive the upper bounds on critical transmission power without and with network congestion and link collision considerations. Section 6 additionally considers holes and analyzes the effects of holes on the data deliverability of greedy routing. Section 7 presents the numerical solution of upper bounds on critical transmission power. Section 8 describes the numerical analysis, simulation results and real-world experimental results. Section 9 concludes our work with remarks on our future work.

2 Related Work

Greedy forwarding with geographical locations in a WSN may fail at void nodes. The most well-known method to handle the problem is face routing [9], [22], which requires planarization. Face routing planarizes the network graph and forwards a message along one or a sequence of adjacent faces, which provides progress towards the destination node. However, face routing can perform poorly comparing to optimum route and can be impractical to maintain information of the extremely large planar faces. Therefore, adaptive face routing and various types of greedy-face-greedy routing methods are investigated in [22]. Another method is using virtual coordinates. Sarkar et al. [23] proposed to compute a new embedding of the sensors in the plane such that greedy forwarding with the virtual coordinates guarantees delivery.

To handle this "void node" problem, many works [11], [12], [13], [24], [25] theoretically analyze the deliverability of geographic greedy routing in WSNs or wireless ad hoc networks. The works in [11], [12], [24], [25] focus on the deliverability between any pair of source-destination nodes by greedy routing. However, these works assume packet transmission with no interference, which makes them impossible to accurately characterize the data deliverability in practical scenarios. Yang et al. [13] modeled the relationship between the critical transmission power and the probability of guaranteed delivery in the many-to-one delivery in a 2-D WSN. They showed that the critical transmission radius for many-to-one deliverability can be much smaller than that for any-to-any deliverability. However, they studied the routing deliverability of all nodes in terms of the probability of guaranteed delivery instead of the packet delivery ratio, as indicated in Section 1. Also, their analysis neglects the network congestion and link collision, which are main causes that affect deliverability. Considering the importance of many-to-one data collection for sensor networks, our work targets at many-to-one deliverability of greedy routing and studies the relationship between the critical transmission power and the probability of η-guaranteed delivery. Further, our work is the first to analyze the effect of network congestion and link collision on the deliverability of greedy routing in the physically realistic SINR model [26], which makes our work substantially different from previous works and enables our work to accurately characterize the data deliverability in practical scenarios. Thus, our work is a notable extension compared to previous works.

3 System Model and Problem Definition

3.1 System Model

For analytical tractability, we assume that a WSN with N nodes is deployed in a 2-D disk region with radius R. The base station X_{bs} is located at the center of the region. The disk region is denoted by $D(X_{bs}, R)$. The distribution of the sensors over the region follows a homogeneous Poisson point process with constant density λ [11]. Each sensor, denoted by X_i, has the same transmission power [11]. We model the WSN as a graph $G(V, E)$, in which V represents

the set of nodes in the network, and E stands for the links of the network.

3.2 Channel Model

In this paper, we use the SINR model to capture channel characteristics in WSNs. Many previous works [27], [28] on data deliverability assume Unit Disk Graph (UDG) model for communication. The UDG model, which assumes that two nodes within certain distance can communicate directly, oversimplifies the channel model [29], because it does not consider interference from other on-going transmissions. In SINR, the successful reception of a transmission depends not only on the received signal strength but also the interference caused by simultaneously transmitting nodes and the ambient noise level. Thus, based on SINR, we are able to provide more realistic and accurate analysis on the data deliverability of greedy routing in WSNs.

We use v_s and v_r to denote a source transmitter and a receiver. Let P_{rec} be the received signal power at the receiver v_r from the transmitter v_s. Denote I_r as the amount of interference generated by other nodes in the network. Let N_n be the ambient noise power level. Then, in the SINR model, receiver v_r receives a transmission iff

$$P_{rec}/(N_n + I_r) \geq \beta, \tag{1}$$

where β is a small constant (depending on the hardware) and it denotes the minimum signal to interference ratio required for a message to be successfully received. The value of the received signal power P_{rec} is a decreasing function of the euclidean distance d_{sr} between the transmitter v_s and the receiver v_r, represented by

$$P_{rec}(d_{sr}) = P_t/d_{sr}^{\alpha}, \tag{2}$$

where P_t is the transmission power of the transmitter, and the so-called path-loss exponent α is a constant between 2 and 6. α indicates the rate at which the received signal power decreases with the distance between the transmitter and the receiver. Based on (1), the transmission radius r for successful delivery can be represented as

$$r = \sup\{d | P_{rec}(d) \geq \beta(N_n + I_r), 0 < d < +\infty\}, \tag{3}$$

where sup represents the least upper bound. In WSNs on 2-D plane, I_r can be represented by

$$I_r = \sum_{v_i \in V \setminus \{v_s\}} \frac{P_t}{{d_{ir}}^{\alpha}}, \tag{4}$$

where $V \subset \mathbb{R}^2$ is the set of nodes in the 2-D plane.

3.3 Problem Definition

Definition 1 (Delivery-failure node). *X_i is a delivery-failure node if it cannot directly communicate with the base station X_{bs}, and also cannot communicate with X_{bs} via multi-hop.*

Definition 2 (η-guaranteed delivery). *Given a WSN G with N sensors, and a minimum delivery ratio requirement (η), a data gathering of G achieves η-guaranteed delivery if $N_s/N \geq \eta$, where N_s is the number of delivery-success nodes in the data gathering.*

η-guaranteed delivery with $\eta < 100\%$ is usually desired in the applications that can tolerate a limited number of delivery-failure nodes, such as statistical inference to the population with sensed data samples. The determination of η depends on the number of delivery-failure nodes that can be tolerated. When $\eta < 100\%$, the transmission power of sensors to achieve η-guaranteed delivery is much lower than that required by 100%-guaranteed delivery. Based on η-guaranteed delivery, we define the critical transmission power and radius and present our problems below.

Definition 3 (Critical transmission power). *The critical transmission power $P_t^{cri}(\eta, Pr^{th})$ denotes the minimal transmission power, which ensures that the probability of achieving η-guaranteed delivery is no less than a threshold $Prth$ ($0 < Pr^{th} < 1$), i.e.,*

$$\Pr\{N_s/N \geq \eta\} \geq Pr^{th}. \tag{5}$$

Definition 4 (Critical transmission radius). *The critical transmission radius $r^{cri}(\eta, Pr^{th})$, corresponding to the critical transmission power $P_t^{cri}(\eta, Pr^{th})$, denotes the minimal transmission radius which ensures that the probability of achieving η-guaranteed delivery is no less than $Prth$.*

According to the definition, critical transmission power $P_t^{cri}(\eta, Pr^{th})$ is determined by the delivery ratio η and threshold Prth. It ensures that the probability of achieving η-guaranteed delivery for a WSN is no less than a threshold with minimal energy consumption. To ensure η-guaranteed delivery with a certain probability, we need to find the critical transmission power $P_t^{cri}(\eta, Pr^{th})$. Obviously, a sensor using the critical transmission power $P_t^{cri}(\eta, Pr^{th})$ has a corresponding critical transmission radius $r^{cri}(\eta, Pr^{th})$. Based on the above definitions, we can formulate our problems as follows:

Problem 1. *Given a desired ratio of delivery-success nodes η and a probability threshold Pr^{th}, what is the critical transmission power $P_t^{cri}(\eta, Pr^{th})$ to achieve η-guaranteed delivery?*

From the above, we can see the previous work [13] is a special case of our problem with $\eta = 100\%$. Our problem provides a more in-depth and precise characterization on the data deliverability of greedy routing. The study of our problem is also very useful to WSN applications that use approximate data collection that collects incomplete data from WSNs, which has been widely studied due to its energy-efficiency [30], [31].

Because network congestion and link collision affect greedy routing deliverability, we further study Problem 1 with the consideration of these factors. We present this new problem as Problem 2 in the following. We consider a continuous data gathering scenario, in which all sensors periodically send sensed data to the base station, and the data is collected round by round. In one round of data gathering, the ratio of delivery-success nodes is affected by the current status of network congestion and link collision.

Problem 2. *Given a desired ratio of delivery-success nodes η for each round of a continuous data gathering and a probability threshold Pr^{th}, what is the critical transmission power $P_t^{cri}(\eta, Pr^{th})$ to achieve η-guaranteed delivery with the consideration of the impact of network congestion and link collision on the ratio of delivery-success nodes?*

Problem 3. *Given a desired ratio of delivery-success nodes η for each round of a continuous data gathering and a probability*

threshold Prth, what is the critical transmission power $P_t^{cri}(\eta, Pr^{th})$ to achieve η-guaranteed delivery with the consideration of the impact of network congestion, link collision and holes on the ratio of delivery-success nodes?

4 Critical Transmission Power

In this section, we address Problem 1 and derive the upper bounds on critical transmission power for the problem solution with the assumption of Poisson distribution of node deployment and delivery-failure nodes [13], [32], [33], [34] in the SINR model. We first establish the relationship between the probability of η-guaranteed delivery and the probability of a node being a delivery-failure node. Then, we formulate the relationship between the probability of a node being a delivery-failure node and the transmission power. As a result, we can find the upper bounds on critical transmission power.

4.1 The Relationship between η-Guaranteed Delivery and Delivery Failure Probability

For a sensor X_i, $C(X_i)$ denotes a Bernoulli random variable that equals one iff X_i is a delivery-failure node. For all nodes $V = \{X_1, \ldots, X_{|V|}\}$ in the network, $C(X_1), \ldots, C(X_n)$ are identically distributed random variables, where $|V|$ is the cardinality of V. As the work in [35], we assume the distribution of the delivery-failure nodes is statistically independent. Let Z be the number of delivery-failure nodes in the network, and we have

$$Z = \sum_{x_i \in V} C(X_i). \tag{6}$$

According to Definition 3, for critical transmission power, we have

$$\Pr\{Z \leq (1-\eta)N\} \geq Pr^{th}, \tag{7}$$

where N is the number of nodes in the network.

According to Markov's inequality, we have

$$\begin{aligned} Pr(Z \leq (1-\eta)N) &= 1 - Pr(Z \geq ((1-\eta)N + 1)) \\ &\geq 1 - E(Z)/((1-\eta)N + 1). \end{aligned} \tag{8}$$

Suppose that $C(X_i)$ $(1 \leq i \leq N)$ are identically distributed random variables. Then, the expectation of random variable Z can be computed by

$$\begin{aligned} E[Z] &= \sum_{N=0}^{+\infty} E\left[\sum_{i=1}^{N} C(X_i)\right] Pr(|V| = N) \\ &= \sum_{N=0}^{+\infty} (NE[C(X_i)] Pr(|V| = N)) \\ &= E[C(X_i)] \sum_{N=0}^{+\infty} N(\lambda\pi R^2)^N exp(-\lambda\pi R^2)/(N!) \\ &= \lambda\pi R^2 E[C(X_i)] = \lambda\pi R^2 Pr(C(X_i) = 1), \end{aligned} \tag{9}$$

where the distribution of the delivery-failure sensors over the region follows a homogeneous Poisson point process with constant density $\lambda\pi R^2$ [13], [34].

Combining Formulas (7), (8), and (9), we have

$$Pr(C(X_i) = 1) \leq (1 - Pr^{th})((1-\eta)N + 1)/(\lambda\pi R^2). \tag{10}$$

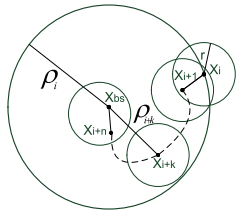


Fig. 1. Routing.

In order to achieve η-guaranteed delivery, the critical transmission power should be chosen to make the delivery failure probability of any node satisfy (10).

4.2 Upper Bound on Critical Transmission Power

Recall that a node is a void node if it cannot directly communicate with the central base station X_{bs} and it is closer to X_{bs} than all its neighbors. To compute the probability of X_i being a delivery-failure node, we first consider the probability of X_i being a delivery-success node. Suppose that the distance between X_i and X_{bs} is ρ and the transmission radius is r, X_i is a delivery-success node only if it falls into either of the following two cases:

Case 1. ρ is less than or equal to r, that is, X_i can directly communicate with X_{bs}.

Case 2. ρ is greater than r, and there exists a multi-hop greedy routing path to X_{bs} with no delivery-failure nodes.

Suppose $X_{i+1}, \ldots, X_{i+k}, \ldots, X_{i+n}$ are intermediate nodes from X_i to the base station, as shown in Fig. 1. ρ_{i+k} is the distance between the node X_{i+k} $(k = 0, 1, \ldots, n)$ and the base station X_{bs}. $n = 0$ if X_i can directly communicate with X_{bs}. The solution for Case 1 is intuitive, and in most cases the delivery success-node (say, X_i) falls into Case 2. Here we focus on analyzing the probability that a packet can be successfully sent from a node X_i to X_{bs} via multiple hops (Case 2). Case 2 is satisfied iff X_i satisfies both of the following two conditions:

- Condition E_1: There exists at least one node located in X_i's transmission range which is closer to the base station than X_i.
- Condition E_2: The next forwarding node X_{i+1}, one of X_i's neighbors who has the smallest distance to the base station among X_i and all its neighbors, can successfully forward the packet to the base station.

Next, we first consider the probability of E_1, then derive the probability of X_i being a delivery-success node which is equal to the probability that both E_1 and E_2 are satisfied.

4.2.1 Probability of Condition E_1

We call the area where the potential next forwarding node X_{i+1} can be located as *the feasible region of node* X_i. Because X_{i+1} must be in the transmission range of X_i and also must have smaller distance to the base station than X_i, the feasible area of X_i is the intersection area of the two circles of radius r and ρ centered at X_i and the base station, respectively.

We use random variable U to denote the distance between the base station (X_{bs}) and the next forwarding node chosen by the greedy routing algorithm. Consider the feasible region of X_i, where potential next forwarding nodes can be located at some distance u or less from the base station (shaded region in Fig. 2). The area of the feasible region is denoted by $S_\rho(u)$. According to [36], because when ρ is greater than r, the probability of no next forwarding nodes existing in the feasible

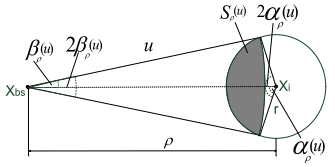


Fig. 2. Feasible region of nodes.

region of area is equivalent to the probability that U is strictly greater than u. The complement of this probability yields the distribution of U [36] which varies with u

$$F(u) = \begin{cases} 1 - exp(-\lambda S_\rho(u)), & \rho - r \le u < \rho \\ 1, & u \ge \rho \\ 0, & u < \rho - r \end{cases}. \quad (11)$$

We can obtain the following probability density function by differentiating the distribution $F(u)$ which is absolutely continuous

$$f(u) = \lambda S_\rho^{'}(u) exp(-\lambda S_\rho(u)), \ \rho - r \le u < \rho, \quad (12)$$

where $S_\rho^{'}(u)$ is the derivative of $S_\rho(u)$ with respect to u.

We define the angles of the two intersecting sectors as $2\alpha_\rho$, $2\beta_\rho$, as shown in Fig. 2. By the Law of Cosines, we have

$$\alpha_\rho(u) = \arccos\left(\frac{r^2 + \rho^2 - u^2}{2r\rho}\right) \quad (13)$$

$$\beta_\rho(u) = \arccos\left(\frac{u^2 + \rho^2 - r^2}{2u\rho}\right). \quad (14)$$

Then, we have

$$S_\rho(u) = r^2\alpha_\rho(u) + u^2\beta_\rho(u) - u\rho\sin\beta_\rho(u), \ \rho - r \le u < \rho. \quad (15)$$

Based on (13), (14), and (15), we have

$$S_\rho^{'}(u) \approx 2u\beta_\rho(u). \quad (16)$$

4.2.2 Probability of Being a Delivery-Success Node

Considering that the sensors are uniformly distributed on 2-D plan, the nodes which has the same distance to the base station are equal on the network deliverability for their packets. Thus, for a given node X_i which has distance ρ to the base station, we let the probability of X_i being a delivery-success node be a function of the distance ρ, denoted by $P(\rho)$.

The distance U has probability density function $f(u)$ given by (12). When $U = u$, the probability of X_{i+1} being a delivery-success node is $P(u)$. Because X_i can successfully send a packet to X_{bs} via multiple hops only if it satisfies both Condition E_1 and Condition E_2, we have

$$P(\rho) = \int_{\rho - r}^{\rho} P(u) f(u) du. \quad (17)$$

We take the derivative of this equation with respect to ρ first, and get a differential equation. After computing this differential equation using Mathematica, we get the following analytic solution:

$$\begin{aligned} P(\rho) = exp\Bigg(-\int_1^r -2exp\Bigg(-\lambda\Big(r^2\arccos\left(\frac{r}{2t}\right) + \arccos\left(\frac{-r^2+2t^2}{2t^2}\right)t^2 \\ - \frac{1}{2}t^2\sqrt{\frac{r^2(-r^2+4t^2)}{t^4}}\Big)\Bigg)\lambda\arccos\left(\frac{-r^2+2t^2}{2t^2}\right)tdt \\ + \int_1^\rho -2exp\Bigg(-\lambda\Big(r^2\arccos\left(\frac{r}{2t}\right) + \arccos\left(\frac{-r^2+2t^2}{2t^2}\right)t^2 \\ - \frac{1}{2}t^2\sqrt{\frac{r^2(-r^2+4t^2)}{t^4}}\Big)\Bigg)\lambda\arccos\left(\frac{-r^2+2t^2}{2t^2}\right)tdt\Bigg). \end{aligned} \quad (18)$$

Accordingly, the probability of the node X_i being a delivery-failure node is

$$(P(\rho))^c = 1 - P(\rho), \quad (19)$$

where superscript c means the complement of $P(\rho)$.

4.2.3 Upper Bound on Critical Transmission Power

Considering all the possible locations of X_i, the probability of a node being a delivery-failure node is

$$P^c = \int_0^{2\pi}\int_r^R \frac{(P(\rho))^c}{\pi R^2}\rho d\rho d\theta = \frac{2}{R^2}\int_r^R \rho(P(\rho))^c d\rho = \frac{2g(r)}{R^2}, \quad (20)$$

where

$$g(r) = \int_r^R \rho(1 - P(\rho))d\rho. \quad (21)$$

Hence

$$Pr(C(X_i) = 1) = (2g(r))/R^2. \quad (22)$$

Theorem 4.1. *Assume a WSN $G(V, E)$ with N nodes is deployed in a 2-D disk region $D(X_{bs}, R)$. Given a designed probability threshold $Prth$ and a desired delivery ratio η, the critical transmission radius $r^{cri}(\eta, Pr^{th})$ satisfies*

$$r^{cri}(\eta, Pr^{th}) \le \widetilde{r} = \inf\{r | g(r) \le \frac{(1 - Pr^{th})(x+1)}{2\lambda\pi}\}, \quad (23)$$

where inf represents the greatest lower bound, $g(r)$ is defined in Formula (21), $x = (1-\eta)N$ is the maximum number of delivery-failure nodes.

Proof. Recall that critical transmission radius $r^{cri}(\eta, Pr^{th})$ is the minimum transmission radius that can ensure the probability of η-guaranteed delivery $\Pr\{N_s/N \ge \eta\} \ge Pr$th (Formula (5)), that is, $\Pr\{Z \le (1-\eta)N\} \ge Pr$th (Formula (7)). Let $x = (1-\eta)N$. Based on (8), (9), and (22), we have

$$Pr(Z \le x) \ge 1 - (\lambda\pi R^2(2g(r))/R^2)/(x+1). \quad (24)$$

To ensure that $Pr(Z \le x) \ge Pr^{th}$, we only need to make

$$g(r) \le (1 - Pr^{th})(x+1)/(2\lambda\pi). \quad (25)$$

Based on Lemma 2 in the Appendix, which can be found on the Computer Society Digital Library at http://doi.ieeecomputersociety.org/TMC.2017.2737005, $g(r)$ is strictly decreasing for r. Hence, we can ensure $Pr(Z \le x) \ge Pr^{th}$ as long as the critical transmission radius $r^{cri}(\eta, Pr^{th})$ satisfies Formula (23). Hence Theorem 4.1 holds. □

Corollary 4.1. *Based on Theorem 4.1, the critical transmission power $P_t^{cri}(\eta, Pr^{th})$ corresponding to $r^{cri}(\eta, Pr^{th})$ satisfies*

$$P_t^{cri}(\eta, Pr^{th}) \leq \widetilde{P}_t = \beta(N_n + I_r)\widetilde{r}^{\alpha}, \tag{26}$$

where $\widetilde{P}_t$ is the upper bound on critical transmission power, N_n is the ambient noise power level, I_r is the amount of interference generated by other nodes in the network, α is the path-loss exponent.

Proof. According to (1), we have $P_{rec} \geq (N_n + I_r)\beta$. Letting d_{sr} in (2) be $\widetilde{r}$, with $P_{rec}(d_{sr}) \geq (N_n + I_r)\beta$ we can obtain the upper bound of the critical transmission power $P_t^{cri}(\eta, Pr^{th})$, that is, $P_t^{cri}(\eta, Pr^{th}) \leq \widetilde{P}_t = \beta(N_n + I_r)\widetilde{r}^{\alpha}$, where I_r can be computed based on Formula (4). □

5 Effects of Network Congestion and Link Collision

In this section, we derive the upper bound on the critical transmission power for η-guaranteed delivery with consideration of the effects of congestion and collision. The congestion at the receiver node introduces packet loss due to buffer overflow. Also, when multiple active sensor nodes try to access the channel simultaneously, collisions could occur and corrupt the packet in transmission. A sensor fails in delivering data to its next hop when the transmission experiences a collision or the buffer of its next hop is full. Since the congestion and collision are well-identified causes of packet loss in WSNs [18], [37] and they are important in analyzing the deliverability for many-to-one data delivery in WSNs [38], [39], we investigate their effects on the deliverability of greedy routing to provide realistic analysis results. Here, we assume each sensor in the WSN has a buffer size of m packets.

To compute the probability that a given node X_i delivers data to X_{bs}, we assume the data delivery path from X_i to X_{bs} is $X_i \rightarrow X_{i+1} \rightarrow, \ldots, \rightarrow X_{i+n} \rightarrow X_{bs}$. $n = 0$ if X_i can directly communicate with X_{bs}. We first consider the probability of successful data transmission at one hop in the path.

5.1 Probability of Delivery Success in One Hop

For a successful one-hop data transmission, say $X_j \rightarrow X_{j+1}$, the following two conditions must be satisfied.

- Condition E_A: X_j is not a void node, i.e., X_j has a neighbor whose distance to X_{bs} is smaller than X_j's.
- Condition E_B: No link collision occurs during the packet transmission from X_j to X_{j+1}, and when the packet arrives at X_{j+1} the buffer queue of X_{j+1} is not full, i.e., no congestion occurs to the packet.

Hence, we have

$$Pr(X_j \rightarrow X_{j+1}) = Pr(E_A)Pr(E_B). \tag{27}$$

5.1.1 Probability of Condition E_A

The probability that X_j is a void node is the probability that no nodes exist in X_j's feasible region. The area of X_j's feasible region where any node has smaller distance from the base station than X_j, denoted by $S(\rho_j, r)$, can be computed by (15) with $u = \rho_j$ where ρ_j, is the distance between X_j and X_{bs}, i.e.,

$$S(\rho_j, r) = 2\rho_j^2 arcsin\frac{r}{2\rho_j} + r^2 \arccos\frac{r}{2\rho_j} - r\sqrt{\rho_j^2 - \frac{r^2}{4}}. \tag{28}$$

According to spatial Poisson point process distribution of nodes, we have

$$Pr(E_A) = 1 - \exp(-\lambda S(\rho_j, r)). \tag{29}$$

5.1.2 Probability of Condition E_B

Next, to compute $Pr(E_B)$, we first derive the probability of packet loss caused by network congestion and link collision respectively, and then obtain $Pr(E_B)$.

Network Congestion. Let P_{nc} be the probability that a node fails to deliver a packet to its next hop due to buffer overflow. We derive P_{nc} based on $M/M/1/k$ model. The $M/M/1/k$ model describes a stochastic process whose state space is the set $I = \{0, 1, 2, \ldots, k\}$ where the value corresponds to the number of packets in the node's buffer. According to [40], steady state probabilities of the system, denoted by $P_j (j = 0, 1, 2, \ldots, k)$, are

$$P_0 = \begin{cases} \frac{1-\varrho}{1-\varrho^{k+1}}, & \varrho \neq 1 \\ \frac{1}{k+1}, & \varrho = 1 \end{cases} \tag{30}$$

$$P_j = \begin{cases} \frac{\varrho^j(1-\varrho)}{1-\varrho^{k+1}}, & \varrho \neq 1 \\ \frac{1}{k+1}, & \varrho = 1. \end{cases} \tag{31}$$

Here $\varrho = \lambda_{ARR}/\mu$ in which μ is the packet transmission rate and λ_{ARR} is packet arrival rate. Since it is a many-to-one model (i.e., all packets go to sink), the arrival rate of the sensor in the center (closer to the sink) should be higher (more contending nodes) than that of the sensor away from the sink, and thus we consider the arrival rate as a function (inverse proportion to the receiver's distance to the base station) of the receiver's distance to the base station so that it can better reflect the case in real system [41]. The arrival rate of node X_{j+1} is as follows:

$$\lambda_{ARR}(\rho_{j+1}) = (R/2)/\rho_{j+1} \cdot \overline{\lambda}, \tag{32}$$

where R is the radius of the 2-D disk region, ρ_{j+1} is the distance between X_{j+1} and X_{bs}, and $\overline{\lambda}$ is an expected arrival rate.

Each sensor has a buffer size of m packets. With $k = m$, the steady state probability P_m is the probability of a buffer being full which causes packet drop. Obviously,

$$P_{nc} = P_m. \tag{33}$$

Hence, the probability that node X_j fails to deliver a packet to its next hop X_{j+1} due to buffer overflow is P_m with $\varrho = \lambda_{ARR}(\rho_{j+1})/\mu$ (denoted by $P_m(\rho_{j+1})$).

Link Collision. Since in WSNs wireless channels are shared by several nodes using CSMA-like (Carrier Sense Multiple Access) protocols, we derive the probability of packet loss due to link collision based on modeling of CSMA/CA in [42]. The binary exponential backoff procedure is modeled as a Markov chain with the assumption of constant and independent collision probability of a packet transmitted by each node. We consider a fix number l of contending nodes, each always having a packet available for transmission after the completion of each successful transmission. Based on [42], we can get the probability of a packet encountering collision P_{lc} as

$$P_{lc} = 1 - (1-\tau)^l, \tag{34}$$

where τ is the probability that a node transmits in a randomly chosen slot time

$$\tau = \frac{2(1-2P_{lc})}{(1-2P_{lc})(W+1) + P_{lc}W(1-(2P_{lc})^v)}, \tag{35}$$

where W is the minimum contention window size $W = CW_{min}$, and the maximum contention window size is $CW_{max} = 2^v W$. v is the maximum backoff stage. In particular, when $v = 0$, i.e., no exponential backoff is considered, the probability τ results to be independent of P_{lc}. Formula (35) thus simply becomes

$$\tau = 2/(W+1). \tag{36}$$

Computation of $Pr(E_B)$. Based on (33) and (34), the probability of Condition E_B, can be found by simply multiplying probability of not having link collision $(1 - P_{lc})$ and probability of not encountering full buffer $(1 - P_{nc})$ as follows:

$$Pr(E_B) = (1-P_{nc})(1-P_{lc}) = (1-P_m)(1-\tau)^l. \tag{37}$$

5.2 Probability of Delivery Success to the Base Station

For simplicity, we use the average number of hops that a packet can traverse from a node to the base station to approximately estimate the probability of successful data delivery from node X_i to base station X_{bs}.

5.2.1 Average Number of Hops

If a packet travels from a node with distance ρ_i to the base station to another node with distance ρ_{i+1} to the base station, the *distance it advances* equals $\rho_i - \rho_{i+1}$. Previous work [43] shows that the probability density function of progress in one hop from X_i towards the base station X_{bs} is

$$\begin{aligned} &f_c(c|||X_i, X_{bs}|| = \rho) \\ &= \sigma\left(\frac{2}{\pi r^2}\right)^{\sigma} 2(\rho - c)\left(\frac{\pi}{2} - \arcsin\left(1 + \frac{c^2 - r^2}{2\rho(\rho - c)}\right)\right)\left(\left(\rho - c\right)^2\right. \\ &\quad \left.\arcsin\left(1 + \frac{c^2 - r^2}{2\rho(\rho - c)}\right) + \frac{1}{2}\sqrt{4r^2\rho^2 - (c^2 - r^2 - 2\rho c)^2}\right. \\ &\quad \left. - r^2 \arcsin\left(\frac{c^2 - r^2 - 2\rho c}{2\rho r}\right) - \frac{\pi(\rho - c)^2}{2}\right)^{\sigma - 1}, 0 \le c \le r, \end{aligned} \tag{38}$$

where ρ is the distance between X_i and X_{bs}, c is the maximum forward progress in one hop towards the base station X_{bs}, and σ is the number of nodes (a function of r) located in the semi-circle with radius r, computed by $\sigma = \lambda\frac{\pi r^2}{2}$ where λ is the constant density.

Based on (38), we can get the average progress per hop towards the base station $\bar{c}$ for X_i with distance ρ to X_{bs} as follows:

$$\bar{c}(\rho) = \int_0^r v f_c(v) dv. \tag{39}$$

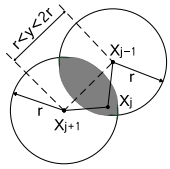


Fig. 3. Geometry of a two-hop connection.

Consider all the possible locations of X_i, we have,

$$\bar{c} = \int_0^{2\pi}\int_0^R \frac{\bar{c}(\rho)}{\pi R^2}\rho d\rho d\theta = \frac{2}{R^2}\int_0^R\int_0^r v f_c(v|||X_i, X_{bs}|| = \rho) dv \rho d\rho. \tag{40}$$

Since the radius of the geographic region $D(X_{bs}, R)$ is R, we estimate the maximum number of hops for delivering a packet to the base station X_{bs} by

$$\hat{H}_{max} = \lceil R/\bar{c} \rceil. \tag{41}$$

According to [44], the average number of hops a packet traverses in the network equals

$$E(H) = \sum_{k=1}^{\hat{H}_{max}} \left\{ k\left(e^{-(k-1)^2\lambda\pi r^2} - e^{-k^2\lambda\pi r^2}\right)\left(1 - e^{-\lambda A}\right)^{k-1}\right\}, \tag{42}$$

where A is the intersection area between two transmission ranges, illustrated by the shaded area in Fig. 3, and can be computed by

$$A = r^2\left(2\arccos\left(\frac{y}{2r}\right) - sin\left(2\arccos\left(\frac{y}{2r}\right)\right)\right). \tag{43}$$

5.2.2 The Probability of Delivery Success

A node succeeds in delivering a packet to the base station if every hop on the routing path achieves successful delivery of the packet. For simplicity, we assume that the delivery of each hop transmission is independent of other hop transmissions along the path [45]. Then, given the probability of delivery success in one hop $Pr(E_A)Pr(E_B)$ and the average number of hops for delivering a packet to the base station $E(H)$, the probability that a node X_i succeeds in delivering a packet to the base station can be derived by combining (29), (37) and (42) (Assume the base station can always receive packets from its neighbors [46].)

$$\begin{aligned} &Pr(C(X_i) = 0|||X_i, X_{bs}|| = \rho_i) = (Pr(E_A)Pr(E_B))^{E(H)} \\ &= \Pi_{j=i}^{i+E(H)-2} Pr(E_A)Pr(E_B) \\ &= \Pi_{j=i}^{i+E(H)-2}(1 - \exp(-\lambda S(\rho_i, r)))(1 - P_m(\rho_{j+1}))(1-\tau)^l. \end{aligned} \tag{44}$$

5.3 Upper Bound on Critical Transmission Power

Based on (20), (21) and (44), we can obtain the probability of a node being a delivery-failure node

$$\begin{aligned} &Pr(C(X_i) = 1|||X_i, X_{bs}|| = \rho_i) = 1 - Pr(C(X_i) = 0|||X_i, X_{bs}|| = \rho_i) \\ &= 1 - \Pi_{j=i}^{i+E(H)-2}(1 - \exp(-\lambda S(\rho_i, r)))(1 - P_m(\rho_{j+1}))(1-\tau)^l. \end{aligned} \tag{45}$$

Considering all the possible locations of X_i, the probability of a node being a delivery-failure node ($Pr(C(X_i)=1)$) can be obtained as follows:

$$\begin{aligned} &Pr(C(X_i)=1)\\ &=\int_0^{2\pi}\int_r^R (\rho_i(1-\Pi_{j=i}^{i+E(H)-2}Pr(E_A)Pr(E_B)))/(\pi R^2)d\rho_i d\theta\\ &=\frac{2}{R^2}\int_r^R \rho_i(1-\Pi_{j=i}^{i+E(H)-2}(1-\exp(-\lambda S(\rho_i,r)))\\ &\quad(1-P_m(\rho_{j+1}))(1-\tau)^l)d\rho_i. \end{aligned} \tag{46}$$

Because the complexity of computing $Pr(C(X_i)=1)$, and P^c is the probability of a node being a delivery-failure node caused by void nodes, and $Pr(E_A)$ is the probability that a node X_j is not a void node, we use

$Pr(C(X_i)=1)=1-\Pi_{j=i}^{i+E(H)-2}(1-P^c)Pr(E_B)$ to approximately compute $Pr(C(X_i)=1)$. For simplicity, we use $h(r)$ to denote $Pr(C(X_i)=1)$

$$\begin{aligned} h(r)&=Pr(C(X_i)=1)=1-\Pi_{j=i}^{i+E(H)-2}(1-P^c)Pr(E_B)\\ &=1-\left(\frac{R^2-2g(r)}{R^2}\right)^{(E(H)-1)}\Pi_{j=i}^{i+E(H)-2}(1-P_m(\rho_{j+1}))(1-\tau)^l. \end{aligned} \tag{47}$$

Theorem 5.1. *Assume a WSN $G(V,E)$ with N nodes is deployed in a 2-D disk region $D(X_{bs},R)$. Given a designed probability threshold Prth and a desired delivery ratio η, the critical transmission radius $r^{cri}(\eta,Pr^{th})$ under network congestion and link collision satisfies*

$$r^{cri}(\eta,Pr^{th})\le\widetilde{r}=\inf\{r|h(r)\le\tfrac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}\}, \tag{48}$$

where $h(r)$ is defined in Formula (47), $x=(1-\eta)N$ is the maximum number of delivery-failure nodes.

Proof. Note that critical transmission radius $r^{cri}(\eta,Pr^{th})$ is the minimum transmission radius that can ensure the probability of η-guaranteed delivery $\Pr\{Z\le(1-\eta)N\}\ge Pr$th. Let $x=(1-\eta)N$. Based on (8), (9) and (47), we have

$$Pr(Z\le x)\ge 1-(\lambda\pi R^2h(r))/(x+1). \tag{49}$$

To ensure that $Pr(Z\le x)\ge Pr^{th}$, we only need to ensure

$$h(r)\le(1-Pr^{th})(x+1)/(\lambda\pi R^2). \tag{50}$$

By Lemma 3 in the Appendix, available in the online supplemental material, $h(r)$ strictly decreases with r. Hence, we can ensure $Pr(Z\le x)\ge Pr^{th}$ as long as the critical transmission radius $r^{cri}(\eta,Pr^{th})$ satisfies Formula (48). Hence Theorem 5.1 holds. □

Corollary 5.1. *Based on Theorem 5.1, the critical transmission power $P_t^{cri}(\eta,Pr^{th})$ corresponding to $r^{cri}(\eta,Pr^{th})$ satisfies*

$$P_t^{cri}(\eta,Pr^{th})\le\widetilde{P}_t=\beta(N_n+I_r)\widetilde{r}^{\alpha}. \tag{51}$$

Proof. Based on (1), we have $P_{rec}\ge(N_n+I_r)\beta$. Letting d_{sr} in (2) be $\widetilde{r}$, with $P_{rec}(d_{sr})\ge(N_n+I_r)\beta$ we can obtain the upper bound of the critical transmission power $P_t^{cri}(\eta,Pr^{th})$, that is, $P_t^{cri}(\eta,Pr^{th})\le\widetilde{P}_t=\beta(N_n+I_r)\widetilde{r}^{\alpha}$. □

6 Effects of Holes on Data Deliverability

Considering that holes (e.g., those caused by physical obstacles such as a lake) in practical scenarios can also cause delivery failure and hence affect data deliverability, we model the effects of holes on data deliverability in this section.

Suppose there are O holes in the network. The distribution of the holes follows a Poisson point process with constant density λ_O [47], [48]. The areas of the holes (hole sizes) are $S_1,\ldots,S_O$, and they follow a normal distribution $\mathcal{N}(\mu_S,\sigma_S^2)$, with mean $\mu_S=\sum_{i=1}^O S_i/O$ and variance σ_S^2 [49], [50], [51].

6.1 Probability of Delivery Success in One Hop

For a successful one-hop data transmission with the consideration of holes, say $X_j\to X_{j+1}$, the following conditions must be satisfied.

- Condition E_B: No link collision occurs during the packet transmission from X_j to X_{j+1}, and when the packet arrives at X_{j+1}, and the buffer queue of X_{j+1} is not full, i.e., no congestion occurs to the packet.
- Condition E_C: X_{j+1} is in X_j's forward region (greedy forwarding area), and it is not in a hole. If X_{j+1} in a hole, X_{j+1} is not in any forwarding regions of any nodes.

Hence, the probability of a node X_j successfully delivering data to its next hop node X_{j+1} can be computed as follows:

$$Pr(X_j\to X_{j+1})=Pr(E_B)Pr(E_C). \tag{52}$$

6.1.1 Probability of Condition E_C

To compute the probability that a given node X_j successfully delivers data to X_{j+1}, we need to calculate the probability of Condition E_C. According to spatial Poisson process distribution of holes, the probability of hole(s) being in X_j's feasible region, denoted by E_d, is

$$Pr(E_d)=1-\exp(-\lambda_O S(\rho_j,r)). \tag{53}$$

The expected area size of the hole(s) existing in X_j's feasible region, denoted by $\bar{S}_H$, is around

$$\bar{S}_H=\sum_{k=1}^{O}\frac{\exp(-\lambda S(\rho_j,r))(\lambda_O S(\rho_j,r))^k}{k!}\cdot k\cdot\mu_S. \tag{54}$$

Based on Formula (29), the probability that the node X_j is not a void node is $1-\exp(-\lambda S(\rho_j,r))$. According to Formula (53), the probability of hole(s) being in X_j's feasible region is $1-\exp(-\lambda_O S(\rho_j,r))$, and $\bar{S}_H/S(\rho_j,r)$ is the probability that X_{j+1} is in the hole within the feasible region given that X_j is not a void node and X_j's feasible region contains hole(s). Hence, the probability that the next hop node X_{j+1} (located in X_{j+1}'s feasible region) is not in a hole of the network is

$$Pr(E_C)=1-(1-\exp(-\lambda_O S(\rho_j,r)))\frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r))). \tag{55}$$

6.2 Probability of Delivery Success to the Base Station

Based on Formulas (37), (52), and (55), the probability of a node X_j successfully delivering data to its next hop node X_{j+1} with the consideration of holes is

$$Pr(X_j \to X_{j+1}) = (1-P_m)(1-\tau)^l(1-(1-\exp(-\lambda_O S(\rho_j,r)))\frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r)))). \tag{56}$$

6.2.1 The Probability of Delivery Success

As in Section 5.2.2, we assume the delivery of each hop transmission is independent of each other hop transmissions along the path. Then, given the probability of delivery success in one hop $Pr(E_B)Pr(E_C)$ and the average number of hops for delivering a packet to the base station $E(H)$ (based on Formula (42)), the probability that a node X_i succeeds in delivering a packet to the base station can be derived using Formulas (42), (52), and (56)

$$\begin{aligned} &Pr(C(X_i)=0|\|X_i,X_{bs}\|=\rho_i) = (Pr(E_B)Pr(E_C))^{E(H)} \\ &= \Pi_{j=i}^{i+E(H)-2} Pr(E_B)Pr(E_C) \\ &= \Pi_{j=i}^{i+E(H)-2}(1-P_m(\rho_{j+1}))(1-\tau)^l(1-(1-\exp(-\lambda_O S(\rho_j,r))) \\ &\quad \frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r)))). \end{aligned} \tag{57}$$

Based on Formulas (20), (21), and (57), we can obtain the probability of a node being a delivery-failure node

$$\begin{aligned} &Pr(C(X_i)=1|\|X_i,X_{bs}\|=\rho_i) = 1 - Pr(C(X_i)=0|\|X_i,X_{bs}\|=\rho_i) \\ &= 1-\Pi_{j=i}^{i+E(H)-2}(1-P_m(\rho_{j+1}))(1-\tau)^l(1-(1-\exp(-\lambda_O S(\rho_j,r))) \\ &\quad \frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r)))). \end{aligned} \tag{58}$$

Considering all the possible locations of X_i, we have

$$\begin{aligned} &Pr(C(X_i)=1) \\ &= \int_0^{2\pi}\int_r^R (\rho_i(1-\Pi_{j=i}^{i+E(H)-2}Pr(E_B)Pr(E_C)))/(\pi R^2)d\rho_i d\theta \\ &= \frac{2}{R^2}\int_r^R \rho_i(1-\Pi_{j=i}^{i+E(H)-2}(1-P_m(\rho_{j+1}))(1-\tau)^l(1-(1 \\ &\quad -\exp(-\lambda_O S(\rho_j,r)))\frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r))))d\rho_i. \end{aligned} \tag{59}$$

For simplicity, we use $f(r)$ to denote $Pr(C(X_i)=1)$. Formula (59) has a high computing complexity. As in Section 5.3, based on Equation (46), with the additional consideration of the hole effect ($Pr(E_C)$), we can approximately get

$$\begin{aligned} f(r) &= Pr(C(X_i)=1) = 1-\Pi_{j=i}^{i+E(H)-2}(1-P^c)Pr(E_B)Pr(E_C) \\ &= 1-\left(\frac{R^2-2g(r)}{R^2}\right)^{(E(H)-1)}\Pi_{j=i}^{i+E(H)-2}(1-P_m(\rho_{j+1}))(1-\tau)^l \\ &\quad (1-(1-\exp(-\lambda_O S(\rho_j,r)))\frac{\bar{S}_H}{S(\rho_j,r)}(1-\exp(-\lambda S(\rho_j,r)))). \end{aligned} \tag{60}$$

Theorem 6.1. *Assume a WSN $G(V,E)$ with N nodes is deployed in a 2-D disk region $D(X_{bs},R)$. Given a designed probability threshold Prth and a desired delivery ratio η, the critical transmission radius $r^{cri}(\eta,Pr^{th})$ under network congestion, link collision and holes satisfies*

$$r^{cri}(\eta,Pr^{th}) \le \widetilde{r} = \inf\left\{r|f(r) \le \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}\right\}, \tag{61}$$

where $f(r)$ is defined in Formula (60), $x=(1-\eta)N$ is the maximum number of delivery-failure nodes.

Proof. Recall that critical transmission radius $r^{cri}(\eta,Pr^{th})$ is the minimum transmission radius that can ensure the probability of η-guaranteed delivery $\Pr\{Z \le (1-\eta)N\} \ge Pr$th. Let $x=(1-\eta)N$. Based on (8), (9) and (60), we have

$$Pr(Z \le x) \ge 1-(\lambda\pi R^2 f(r))/(x+1). \tag{62}$$

To ensure that $Pr(Z \le x) \ge Pr^{th}$, we only need to make

$$f(r) \le (1-Pr^{th})(x+1)/(\lambda\pi R^2). \tag{63}$$

Based on Lemma 4 in the Appendix, available in the online supplemental material, $f(r)$ strictly decreases with r. Hence, we can ensure $Pr(Z \le x) \ge Pr^{th}$ as long as the critical transmission radius $r^{cri}(\eta,Pr^{th})$ satisfies Formula (61). Hence Theorem 6.1 holds. □

Corollary 6.1. *Based on Theorem 6.1, the critical transmission power $P_t^{cri}(\eta,Pr^{th})$ corresponding to $r^{cri}(\eta,Pr^{th})$ satisfies*

$$P_t^{cri}(\eta,Pr^{th}) \le \widetilde{P}_t = \beta(N_n+I_r)\widetilde{r}^{\alpha}. \tag{64}$$

Proof. Letting d_{sr} in (2) be $\widetilde{r}$, with $P_{rec}(d_{sr}) \ge (N_n+I_r)\beta$ we can obtain the upper bound of the critical transmission power $P_t^{cri}(\eta,Pr^{th})$, that is, $P_t^{cri}(\eta,Pr^{th}) \le \widetilde{P}_t = \beta(N_n+I_r)\widetilde{r}^{\alpha}$. □

7 Numerical Solution of Upper Bounds on Critical Transmission Power

Recall that Formulas (23), (26), (48), (51), (61) and (64) show the result for the case without considering the effects of network congestion and link collision and holes, without considering the effects of holes, and with considering the effects of network congestion and link collision and holes, respectively. In practical application, we can constrain the delivery ratio η to be no less than a threshold (e.g., 80 percent), that is, $x \le 0.2 \cdot N$ in Formulas (23), (48), and (61) [52]. According to Formulas (23), (26), (48), (51), (61) and (64), to obtain an exact value of upper bound on critical transmission power, we need to compute critical transmission radius $\widetilde{r}$ based on the function $g(r)$, $h(r)$, or $f(r)$. Due to the complexity of $g(r)$ in (21), $h(r)$ in (47) and $f(r)$ in (60), we alternatively provide a numerical solution to obtain $\widetilde{r}$ by following [13] in this section.

Since the upper bounds on critical transmission power can be directly mapped to the upper bounds on critical transmission radius in (26), (51) and (64), respectively, we focus on computing the upper bounds on critical transmission radii in this section.

Theorem 7.1. *Let* $\phi(r) = g(r) - \frac{(1-Pr^{th})(x+1)}{2\lambda\pi}$, *then* $\phi(r)$ *is strictly monotonically decreasing and there exists a unique root equaling* $\tilde{r}$ *in the domain* $(0, R]$ *such that equation* $\phi(r) = 0$ *is satisfied.*

Proof. By Lemma 2 in the Appendix, available in the online supplemental material, $g(r)$ is strictly decreasing for $r \in (0, R]$, and given a particular and arbitrary x, $\frac{(1-Pr^{th})(x+1)}{2\lambda\pi}$ is a constant, hence $\phi(r)$ is strictly monotonically decreasing and there exists at most one root in the domain $(0, R]$ such that $\phi(r) = 0$ is satisfied. Moreover, the single root exists iff $\phi(0^+) \cdot \phi(R) < 0$ is satisfied, where $\phi(0^+) = lim_{r\to 0^+}\phi(r)$ is the limitation of $\phi(r)$ when r goes to 0^+.

Based on Formula (21), we have

$$\phi(0^+) = lim_{r\to 0^+} \int_r^R \rho(1 - P(\rho))d\rho - \frac{(1 - Pr^{th})(x + 1)}{2\lambda\pi}. \tag{65}$$

Based on Formula (17), the probability of a node being a delivery-success node is 0 if $r = 0$. Thus, we have

$$\phi(0^+) = \frac{R^2}{2} - \frac{(1 - Pr^{th})(x + 1)}{2\lambda\pi}. \tag{66}$$

Since $\lambda\pi R^2$ is the expected number of sensor nodes in the network and x is the maximum number of delivery-failure nodes with η-guaranteed delivery, it is reasonable that $\lambda\pi R^2 > (x + 1) > (1 - Pr^{th})(x + 1)$ is always satisfied. Thus we have

$$\frac{R^2}{2} > \frac{(1 - Pr^{th})(x + 1)}{2\lambda\pi}. \tag{67}$$

Hence, $\phi(0^+) > 0$. Based on Formula (21), we have

$$\phi(R) = \int_R^R \rho(1 - P(\rho))d\rho - \frac{(1 - Pr^{th})(x + 1)}{2\lambda\pi} = -\frac{(1 - Pr^{th})(x + 1)}{2\lambda\pi}. \tag{68}$$

Hence, $\phi(0^+) \cdot \phi(R) < 0$ is satisfied if $r \in (0, R]$. Thus, equation $\phi(r) = 0$ has one root in the domain $(0, R]$. Since $\phi(r)$ is strictly monotonically decreasing in the domain $(0, R]$, equation $\phi(r) = 0$ has at most one root in the domain $(0, R]$. Therefore equation $\phi(r) = 0$ has a unique root equaling $\widetilde{r} = inf\{r|g(r) \le \frac{(1-Pr^{th})(x+1)}{2\lambda\pi}\}$ in the domain $(0, R]$. Hence Theorem 7.1 holds. □

Theorem 7.2. *Let* $\phi(r) = h(r) - \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}$, *then* $\phi(r)$ *is strictly monotonically decreasing and there exists a unique root equaling* $\tilde{r}$ *in the domain* $(0, R]$ *such that equation* $\phi(r) = 0$ *is satisfied.*

Proof. By Lemma 3 in the Appendix, available in the online supplemental material, $h(r)$ is strictly decreasing for $r \in (0, R]$, and given a particular and arbitrary x, $\frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}$ is a constant, hence $\phi(r)$ is strictly monotonically decreasing and there exists at most one root in the domain $(0, R]$ such that $\phi(r) = 0$ is satisfied.

Based on Formula (47), we have

$$\begin{aligned}\phi(0^+) &= lim_{r\to 0^+}(h(r) - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}) \\ &= lim_{r\to 0^+}(1 - (R^2 - 2g(r))^{(E(H)-1)}\Pi_{j=i}^{i+E(H)-2} \\ &(1 - P_\phi(\rho_{j+1}))(1 - \tau)^l/R^{(2E(H)-2)} - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}).\end{aligned} \tag{69}$$

Based on Formula (17), the probability of a node being a delivery-success node is 0 if $r = 0$, and according to Formula (21), $lim_{r\to 0^+} 2g(r) = R^2$. Thus, we have

$$\phi(0^+) = 1 - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}. \tag{70}$$

According to Formula (67), $\phi(0^+) > 0$. Based on Formulas (46) and (47), we have

$$\phi(R) = h(R) - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2} = 0 - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2} < 0. \tag{71}$$

Hence, $\phi(0^+) \cdot \phi(R) < 0$ is satisfied if $r \in (0, R]$. Similar to the proof of Theorem 7.1, equation $\phi(r) = 0$ has a unique root equaling $\widetilde{r} = inf\{r|h(r) \le \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}\}$ in the domain $(0, R]$. Hence Theorem 7.2 holds. □

Theorem 7.3. *Let* $\phi(r) = f(r) - \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}$, *then* $\phi(r)$ *is strictly monotonically decreasing and there exists a unique root equaling* $\tilde{r}$ *in the domain* $(0, R]$ *such that equation* $\phi(r) = 0$ *is satisfied.*

Proof. By Lemma 4 in the Appendix, available in the online supplemental material, $f(r)$ is strictly decreasing for $r \in (0, R]$, and given a particular and arbitrary x, $\frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}$ is a constant, hence $\phi(r)$ is strictly monotonically decreasing and there exists at most one root in the domain $(0, R]$ such that $\phi(r) = 0$ is satisfied.

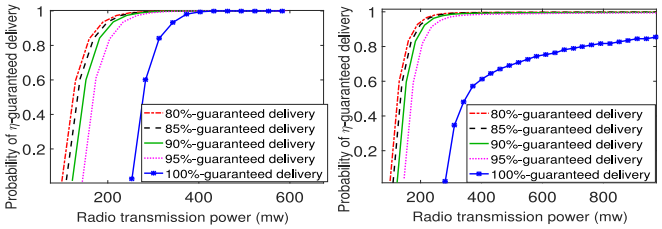
Based on Formula (60), we have

$$\begin{aligned}\phi(0^+) &= lim_{r\to 0^+}\left(f(r) - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}\right) \\ &= lim_{r\to 0^+}\left(1 - \left(\frac{R^2 - 2g(r)}{R^2}\right)^{(E(H)-1)}\Pi_{j=i}^{i+E(H)-2}\right. \\ &\left.(1 - P_m(\rho_{j+1})\right)(1 - \tau)^l(1 - (1 - \exp(-\lambda_O S(\rho_j, r)))\frac{\bar{S}_H}{S(\rho_j, r)} \\ &\left(1 - \exp(-\lambda S(\rho_j, r)))\right) - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}\right).\end{aligned} \tag{72}$$

Based on Formulas (17) and (21), we have

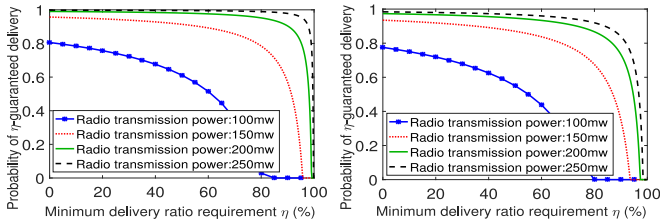
$$\phi(0^+) = 1 - \frac{(1 - Pr^{th})(x + 1)}{\lambda\pi R^2}. \tag{73}$$

According to Formula (67), $\phi(0^+) > 0$. Based on Formulas (59) and (60), we have



(a) W/o congestion & collision (b) W/ congestion & collision

Fig. 4. Relationship between probability of η-guaranteed delivery and transmission power with interference.



(a) W/o congestion & collision (b) W/ congestion & collision

Fig. 5. Relationship between probability of η-guaranteed delivery and the minimum delivery ratio requirement η.

$$\phi(R) = f(R) - \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2} = 0 - \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2} < 0. \tag{74}$$

Hence, $\phi(0^+)\cdot\phi(R) < 0$ is satisfied if $r \in (0, R]$. Similar to the proof of Theorem 7.1, equation $\phi(r) = 0$ has a unique root equaling $\tilde{r} = inf\{r|f(r) \le \frac{(1-Pr^{th})(x+1)}{\lambda\pi R^2}\}$ in the domain $(0, R]$. Hence Theorem 7.3 holds. □

Based on Theorems 7.1, 7.2, and 7.3, $\tilde{r}$ can be obtained by solving $\phi(r) = 0$ using the bisection method.

8 Experimental Results

In this section, we present numerical analysis of our theoretical results to investigate the relationships among the transmission power, probability of η-guaranteed delivery and minimum delivery ratio η. Then, we present simulation results that evaluate the tightness of our upper bounds on the critical transmission powers. Finally, we provide real-world experimental results to validate our model's ability of well approximating real life performance.

8.1 Numerical Analysis

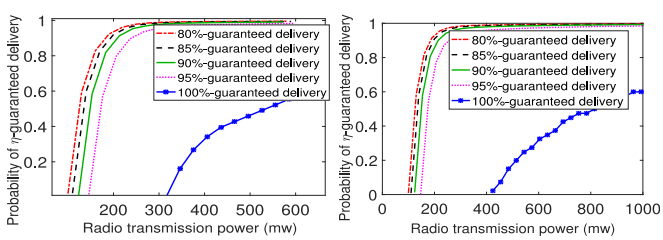
In our numerical analysis, we assume that 500 sensor nodes are distributed over a disk region $D(X_{bs}, 1000\ \mathrm{m})$ following a Poisson distribution. The base station is located at the center of the disk region. All the sensor nodes have the same transmission power. For SINR model, we set path-loss exponent $\alpha = 3$, the minimum signal to interference ratio $\beta = 4$, and ambient noise power level $N_n = 10$ nw [53], [54]. The number of contending nodes l was set to be 10 [42], and the buffer size m was set to be 10. The number of holes was set to be 10. The distribution of the holes follows a Poisson distribution, and the hole size follows a normal distribution with mean $\mu_S = 500\ \mathrm{m}^2$ and variance $\sigma_S^2 = 25$.

The Formulas (23), (24), (25), and (26) in Section 4 show the upper bound on critical transmission power without considering congestion and collision, and Formulas (48), (49), (50), (51) in Section 5 consider congestion and collision. Based on these results, Figs. 4a and 4b show the relationship between the probability of η-guaranteed delivery and transmission power when η = 80%, 85%, 90%, 95%, and 100%, without and with the existence of congestion and collision, respectively. Both figures show that the probability of η-guaranteed delivery increases as the radio transmission power increases. Comparing Figs. 4b to 4a, we see that with the consideration of congestion and collision, greater transmission power is required to achieve the same probability of η-guaranteed delivery. The probability of η-guaranteed delivery in Fig. 4a eventually goes to 1 when the transmission power is large enough. However, in Fig. 4b it approaches 1 but cannot be 1 (though it is not obvious in the figure) due to the existence of congestion and collision. Both figures show that with a smaller η, the transmission power required to achieve the same probability of η-guaranteed delivery is smaller. An interesting observation is that the curve of $\eta = 100\%$ is widely separated from the curves of other η values. This result indicates that with tolerance to a small percentage of delivery-failure nodes, much less transmission power is needed compared to that needed by 100%-guaranteed delivery, thus obtaining significant energy saving.

Fig. 5 shows the relationship between the probability of η-guaranteed delivery and η with different transmission powers. We see that given a transmission power, the probability of η-guaranteed delivery decreases as η increases, and higher transmission power results in higher probability of η-guaranteed delivery. This is because a higher transmission power enables nodes to communicate with nodes further away, decreasing the probability of delivery failure caused by void nodes. Comparing Figs. 5a and 5b, for the same transmission power and the same η, the probability of η-guaranteed delivery in Fig. 5b is lower than that in Fig. 5a because of the congestion and collision effects.

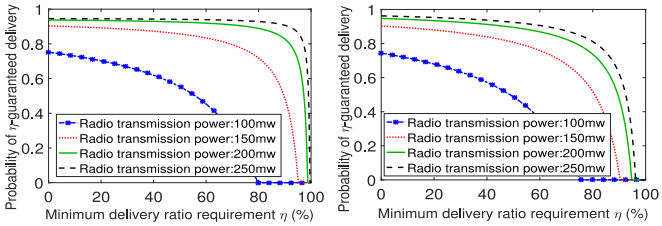
The Formulas (61), (62), (63), and (64) in Section 6 consider the effects of holes on data deliverability. With these results, Fig. 6 shows the relationship between the probability of η-guaranteed delivery and transmission power when η = 80%, 85%, 90%, 95%, and 100% with holes. Fig. 6 mirrors Fig. 4 due to the same reasons explained in Fig. 4. Comparing Figs. 6 and 4, the probability of η-guaranteed delivery in Fig. 6 is lower than that in Fig. 4 because the holes in Fig. 6 can also lead to delivery failure, which increases delivery failure probability.

Fig. 7 shows the relationship between the probability of η-guaranteed delivery and η with holes in different transmission powers. We also see that given a transmission power, the probability of η-guaranteed delivery decreases as η increases, and higher transmission power results in higher probability of η-guaranteed delivery due to the same reasons explained in Fig. 5. For the same transmission power and the



(a) W/o congestion & collision (b) W/ congestion & collision

Fig. 6. Relationship between probability of η-guaranteed delivery and transmission power with interference and holes.



(a) W/o congestion & collision (b) W/ congestion & collision

Fig. 7. Relationship between probability of η-guaranteed delivery and the minimum delivery ratio requirement η with hole consideration.

same η, the probability of η-guaranteed delivery in Fig. 7b is lower than that in Fig. 7a because of the congestion and collision effects. By examining Figs. 7 and 5, we find the probability of η-guaranteed delivery in Fig. 7 is lower than that in Fig. 5 for the same transmission power and the same η because the holes in Fig. 7 can result in delivery failure, which increases the probability of delivery failure and thereby decreases the probability of η-guaranteed delivery.

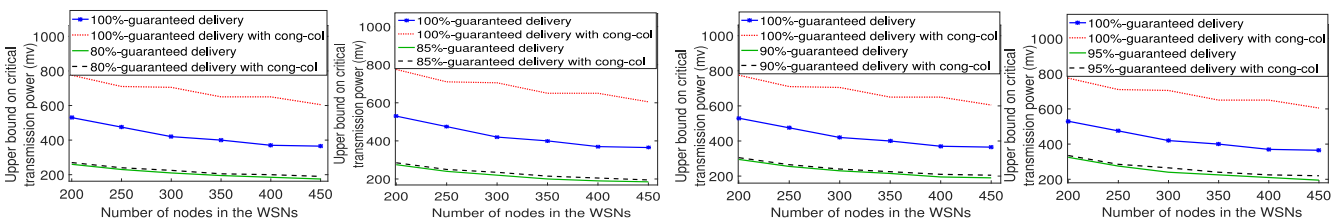
Fig. 8 shows the relationship between the upper bound on critical transmission power and the node density. We changed the node density by varying the number of sensor nodes over the disk region $D(X_{bs}, 1000\text{ m})$. Figs. 8a, 8b, 8c, and 8d show the upper bounds on the critical transmission power for η = 80%, 85%, 90%, and 95% guaranteed delivery, respectively. Each figure shows upper bounds derived with congestion and collision (denoted as "cong-col" in figures) as well as without congestion and collision. The upper bounds for 100%-guaranteed delivery are drawn in every figure for comparison. From these figures, it can be seen that the upper bounds on critical transmission power decrease as the number of nodes in the network (hence node density) increases. This is because a higher node density leads to a smaller average distance between any pair of nodes, which enables each node to use a smaller transmission radius for communication. We also see that the upper bounds on critical transmission power decrease slowly as the node density increases. This is because the increase of node density introduces more interference, offsetting some effect of decreasing average distance of any pairs. All of these figures show that the upper bound derived with the consideration of congestion and collision is larger than that without the consideration. This indicates that higher transmission power is required to counter the effect of congestion and collision. We also find that a smaller η generates a smaller upper bound on critical transmission power. The upper bound for 100%-guaranteed delivery is considerably larger than that for smaller η, which indicates that higher delivery ratio requires higher transmission power regardless of the existence of congestion and collision.

Fig. 9 shows the relationship between the upper bound on critical transmission power and node density with holes in the network. Fig. 9 mirrors Fig. 8 due to the same reasons explained in Fig. 8. Comparing Figs. 9 and 8, the upper bounds in Fig. 9 are larger than that in Fig. 8. This is because the holes in Fig. 9 increase the delivery failure probability and thus increase the upper bounds on critical transmission power.

Figs. 10a, 10b, 10c, and 10d show the relationship between the probability of η-guaranteed delivery and the number of nodes in the network (node density) with transmission powers 300, 350, 400 and 450 mw, respectively. Each figure shows the probabilities of η-guaranteed delivery increase as the node density increases. Also, higher η requires a higher node density to ensure a higher probability of η-guaranteed delivery. 100%-guaranteed delivery requires much higher node density to achieve a high probability of guaranteed delivery than others. Comparing these figures, we also see that the larger the transmission power, the smaller the node density is required for achieving a high probability of η-guaranteed delivery. This is because a larger transmission power enables nodes to communicate with nodes further away.

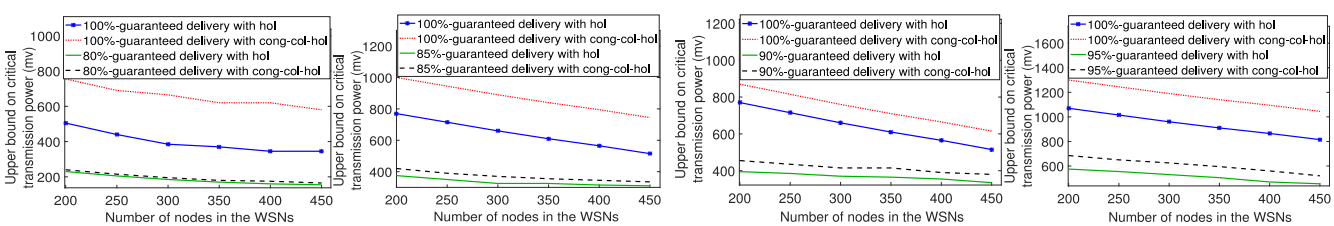
8.2 Simulation Results

We used network simulator NS2 [55] to conduct simulation experiments. Constant Bit Rate (CBR) Traffic generator [55] is used for each sensor to create a fixed size packet for every fixed interval. To validate the correctness and tightness of our upper bound, we compare our theoretical results with simulation results in various scenarios. By default, the number of nodes in the network was set to 200 in the simulation.



(a) 80%-guaranteed delivery (b) 85%-guaranteed delivery (c) 90%-guaranteed delivery (d) 95%-guaranteed delivery

Fig. 8. Relationship between upper bound on critical transmission power and node density with interference.



(a) 80%-guaranteed delivery (b) 85%-guaranteed delivery (c) 90%-guaranteed delivery (d) 95%-guaranteed delivery

Fig. 9. Relationship between upper bound on critical transmission power and node density with interference and holes.

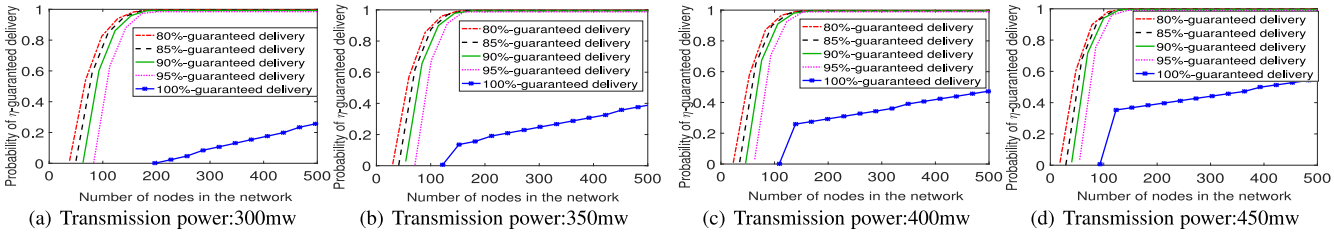


Fig. 10. Probability of η-guaranteed delivery versus node density with interference.

The nodes are distributed over a disk region $D(X_{bs}, 300\ \mathrm{m})$ following a Poisson distribution. The threshold for decoding a signal was set to $P_{th} = -64\ \mathrm{dBm}$. For each setting of transmission power, we generated 200 random network topologies and for each topology we computed the ratio of delivery-success nodes. The probability of η-guaranteed delivery is estimated with the 200 delivery ratio samples. The number of holes was set to be 10. The distribution of holes follows a Poisson distribution, and the hole size follows a normal distribution with mean $\mu_S = 100\ \mathrm{m}^2$ and variance $\sigma_S^2 = 5$.

Figs. 11a and 11b show the theoretical upper bounds on critical transmission power and the simulation results for 85 and 95 percent guaranteed delivery. We see our theoretical upper bounds are very close to the simulation results, and the upper bound on critical transmission power increases as η increases. This is because higher η-guaranteed delivery needs larger transmission power to enable nodes to communicate with nodes further away and thus reduce the delivery failure probability caused by void node, congestion, etc.

To further validate our model, we varied the network density and traffic load of the network. In Fig. 12, we decreased the number of nodes in the network to 100 to decrease the network density. Figs. 12a and 12b show the theoretical upper bounds on critical transmission power and the simulation results for 85 and 95 percent guaranteed delivery. We see that our theoretical upper bounds are still very close to the simulation results. We also find that the upper bound on critical transmission power increases as η increases. Comparing Fig. 12 with Fig. 11, we find that the upper bounds on critical transmission power in Fig. 12 are larger than those in Fig. 11, which indicates the upper bound on critical transmission power increases as node density decreases. This is because larger node density shortens the average distance between nodes and thereby reduces the probability of delivery failure caused by void nodes.

We then varied traffic load by different intervals for CBR traffic generator. Figs. 12, 13, and 14 show the relationship between the probability of η-guaranteed delivery and the transmission power with 100 nodes in the network, under different intervals 2, 1 and 0.5. Smaller interval means higher traffic load. It is obvious to see that our theoretical upper bounds are very close to the simulation results. Comparing Figs. 12, 13, and 14, we find the upper bounds on critical transmission power follow Fig. 14 > Fig. 13 > Fig. 12, which indicates the upper bound on critical transmission power increases as traffic load increases. This is because heavier traffic load increases congestion and collision and thereby increases the probability of delivery failure.

To measure the effects of holes on data deliverability, we conducted experiments with holes in simulation. Figs. 15a and 15b show the theoretical upper bounds on critical transmission power and the simulation results for 85 and 95 percent guaranteed delivery with 200 nodes in the network. Fig. 15 mirrors Fig. 11 due to the same reasons explained in Fig. 11. Comparing Figs. 15 and 11, we see that the upper bounds in Fig. 15 are larger than that in Fig. 11. This is because the holes in Fig. 15 increase the delivery failure probability.

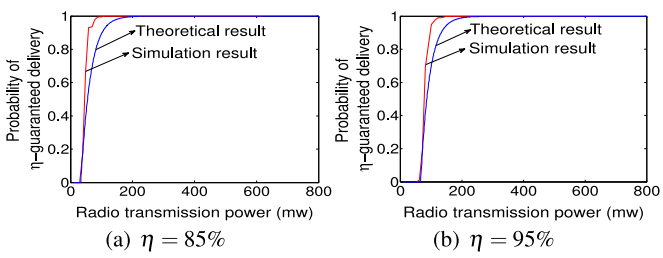


Fig. 11. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 200$, interval = 2 seconds).

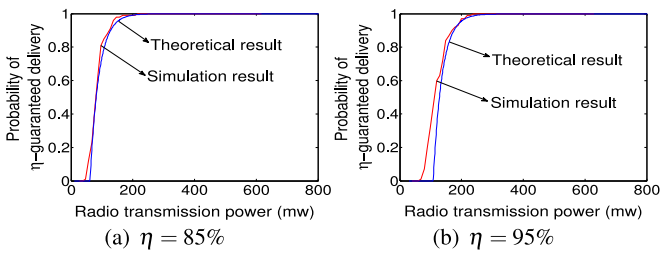


Fig. 12. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 100$, interval = 2 seconds).

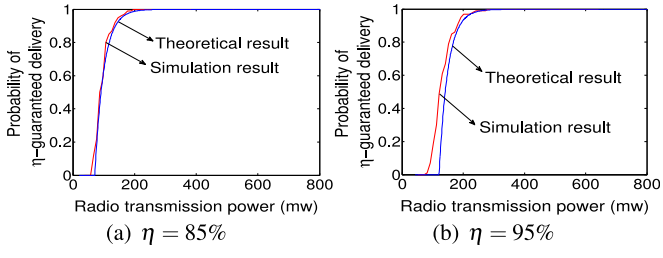


Fig. 13. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 100$, interval = 1 second).

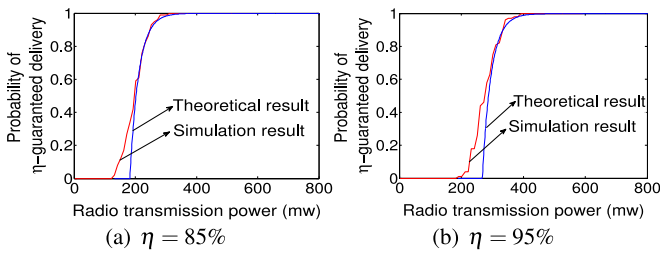


Fig. 14. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 100$, interval = 0.5 second).

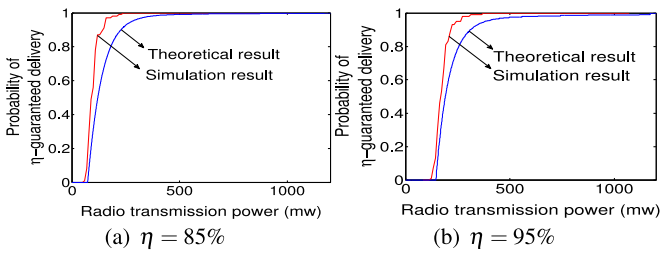


Fig. 15. Probability of η-guaranteed delivery versus transmission power with holes (path-loss exponent $\alpha = 3$, $N = 200$, interval = 2 seconds).

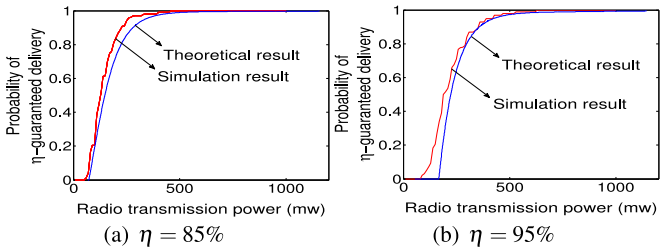


Fig. 16. Probability of η-guaranteed delivery versus transmission power with holes (path-loss exponent $\alpha = 3$, $N = 100$, interval = 2 seconds).

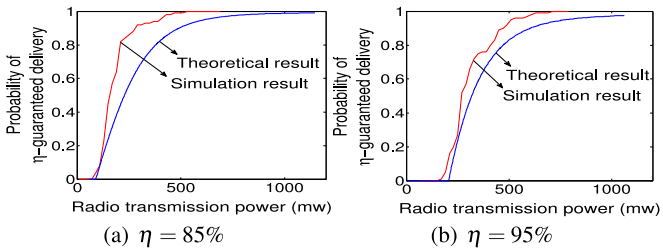


Fig. 17. Probability of η-guaranteed delivery versus transmission power with holes (path-loss exponent $\alpha = 3$, $N = 100$, interval = 1 second).

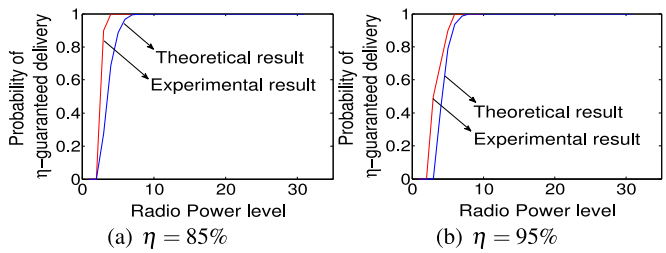


Fig. 18. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 16$, interval = 1 second).

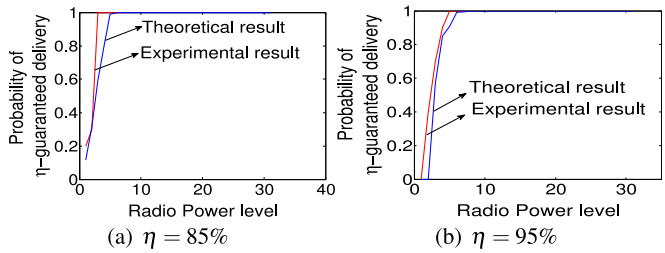


Fig. 19. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 16$, interval = 2 seconds).

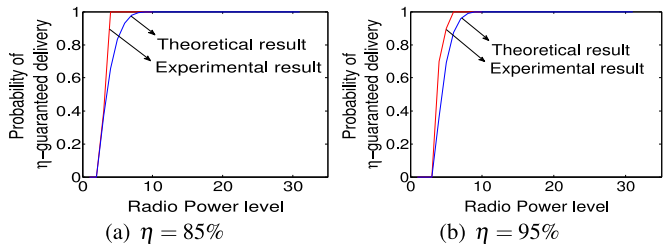


Fig. 20. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 16$, interval = 1 second).

We also varied the network density and traffic load in the network. In Fig. 16, we decreased the number of nodes to 100 to reduce the network density. Fig. 16 mirrors Fig. 12 due to the same reasons explained in Fig. 11. Comparing Figs. 16 to 12, we see that the upper bounds on critical transmission power in Fig. 16 are larger than those in Fig. 12. This is because the holes in Fig. 16 can also cause delivery failure, which increases the probability of delivery failure. Comparing Figs. 16 and 15, we observe that the upper bounds on critical transmission power in Fig. 16 are relatively larger than those in Fig. 15 due to the same reason explained in Fig. 12. In Fig. 17, we increased the traffic load by decreasing the interval for CBR traffic generator to 1. From Fig. 17, we also find that the theoretical upper bounds are close to the simulation results, and the upper bound on critical transmission power increases as η increases due to the same reason explained in Fig. 11. Comparing Figs. 17 to 16, the upper bounds on critical transmission power in Fig. 17 are larger than those in Fig. 16 because the heavier traffic load increases congestion and collision and thus increases the delivery failure probability.

8.3 Real-World Experimental Results

Our testbed [56] consists of 16 Tmote Sky motes [57] running TinyOS 2.1.2. A computer running Ubuntu 12.04 was used to configure all sensor nodes. Each sensor node was configured to periodically sample and transmit data. The network delivery ratio was measured under different traffic loads, network densities, and radio transmission power levels.

Fig. 18 shows the relationship between the probability of η-guaranteed delivery and radio power level for 85 and 95 percent guaranteed delivery. In the test, the interval between two consecutive packet transmissions was set as 1 second. In Fig. 19, we increased the interval between two consecutive packet transmissions to 2 seconds to decrease traffic load. Both Figs. 18 and 19 indicate that the experimental results are close to the theoretical results. By comparing Figs. 18a and 18b, Figs. 19a and 19b, similarly, we see that the upper bound on critical transmission power increases as η increases, which is consistent with numerical results and simulation results. Comparing Figs. 19 and 18, we find that the upper bounds on critical transmission power in Fig. 18 are larger than those in Fig. 19. This result indicates that the upper bound on critical transmission power increases as traffic load increases, which is consistent with our simulation results.

To fully verify the theoretical results derived from our model, we reduced the node density with the network deployment area four times as that in Figs. 18 and 19. The results are shown in Figs. 20 and 21. By comparing Fig. 20 with Fig. 18, and Fig. 21 with Fig. 19, we find the upper bounds in Figs. 20 and 21 are relatively larger than those in Figs. 18 and 19. This is because with larger node density the average distance between nodes is reduced and thus the probability of delivery failure caused by void nodes decreases. By examining Figs. 20 and 21, we find the upper bounds on critical transmission power in Fig. 20 are slightly larger than those in Fig. 21 due to the same reason explained in Fig. 17.

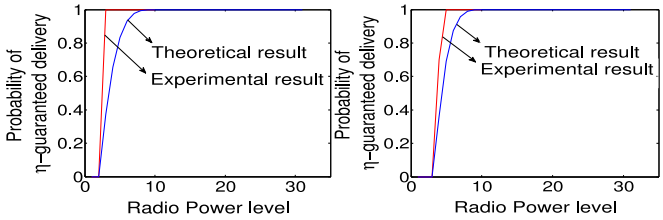


Fig. 21. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 16$, interval = 2 seconds).

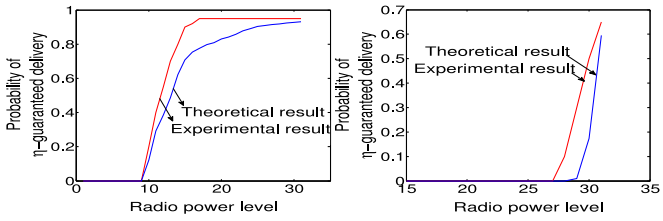


Fig. 22. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 40$, interval = 1 second).

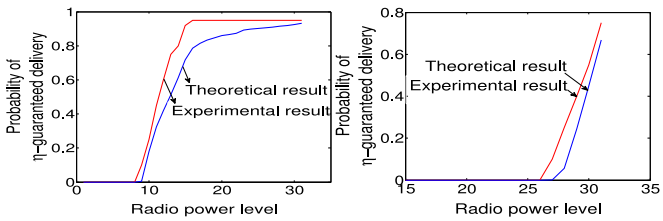


Fig. 23. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 40$, interval = 2 seconds).

To test the effects of holes on data deliverability, we conducted ad-hoc experiment. The testbed consists of 40 Tmote Sky motes running TinyOS 2.1.2. The sensor nodes are deployed over a disk region with radius $R = 12$ m following a Poisson distribution, and 10 holes are distributed over the disk region following a Poisson distribution. The hole size follows a normal distribution with mean $\mu_S = 5$ m^2 and variance $\sigma_S^2 = 0.062$. Each node was configured to periodically sample and transmit data. The network delivery ratio was measured under different network densities, traffic loads, and radio transmission power levels.

Fig. 22 and Fig. 23 show the relationship between the probability of η-guaranteed delivery and radio power level for both 85 and 95 percent guaranteed delivery. In Fig. 22, the interval between two consecutive packet transmissions was set as 1 second. In Fig. 23, we increased the interval to 2 seconds to decrease the traffic load. Fig. 22 mirrors Fig. 18, and Fig. 23 mirrors Fig. 19 due to the same reasons in Figs. 18 and 19, respectively. By examining Figs. 22 and 23, we see that the upper bounds on critical transmission power in Fig. 22 are larger than those in Fig. 23, which is consistent with the simulation results. Comparing Fig. 22 with Fig. 18, we find that the upper bounds on critical transmission power in Fig. 22 are larger than those in Fig. 18 because the holes in Fig. 22 can lead to delivery failure, which increases the probability of delivery failure. Similarly, the upper bounds on critical transmission power in Fig. 23 are larger than those in Fig. 19 due to the same reason.

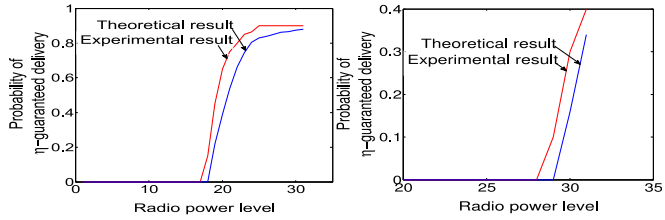


Fig. 24. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 20$, interval = 1 second).

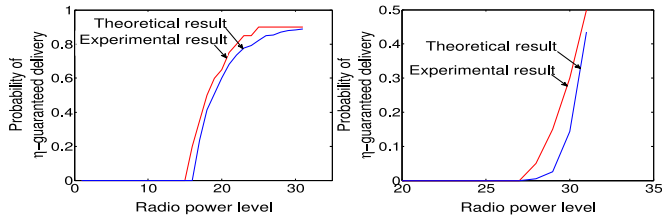


Fig. 25. Probability of η-guaranteed delivery versus transmission power (path-loss exponent $\alpha = 3$, $N = 20$, interval = 2 seconds).

We also reduced the node density by decreasing the number of sensor nodes in the network to 20. The results are shown in Figs. 24 and 25. Fig. 24 mirrors Fig. 20, and Fig. 25 mirrors Fig. 21 due to the same reasons explained in Figs. 20 and 21, respectively. Compare Fig. 24 with Figs. 20 and 25 with Fig. 21, we see that the upper bounds on critical transmission power in Figs. 24 and 25 are larger than those in Figs. 20 and 21 because the holes in Figs. 24 and 25 can cause delivery failure, increasing delivery failure probability. By comparing Fig. 24 with Fig. 22, and Fig. 25 with Fig. 23, we see that the upper bounds in Figs. 24 and 25 are larger than those in Figs. 22 and 23 because with larger node density the average distance between nodes is reduced and the delivery failure probability caused by void nodes decreases. By examining Figs. 24 and 25, we also find the upper bounds on critical transmission power in Fig. 24 are relatively larger than those in Fig. 25 because the heavier traffic load in Fig. 24 introduces congestion and collision, causing high delivery failure probability.

Our theoretical and real-world experimental results show that by tolerancing to a small percentage of delivery-failure nodes, much energy can be saved.

9 Conclusion

In this paper, we study the deliverability of greedy routing in 2-D WSNs. As opposed to previous works that only analyze the probability of guaranteeing all deliveries and neglect network congestion and collision, we introduce η-guaranteed delivery, where η can be varied and study its probability with the consideration of network congestion and collision. Further more, we consider the effects of holes (e.g., obstacles) on deliverability of greedy routing and derive the upper bounds of critical transmission power, which are more practical and accurate. We adopt a more realistic model to analyze upper bounds on critical transmission power. Through theoretical analysis, we derive the upper bounds on the critical transmission power for achieving η-guaranteed delivery with a given probability. The extensive numerical analysis, simulation and real-world experimental results show that our characterization is closer

to the practical scenarios and our derived upper bounds are correct and tight. In the future, we will consider link scheduling in the SINR model and individual setting of transmission power for each node to further improve energy-efficiency, and we will further consider the effects of nodes' location on network congestion and collision for characterizing the deliverability of greedy routing. Also, we will evaluate the deliverability of greedy routing with various improvements proposed recently for handling void nodes and localization errors.

Acknowledgments

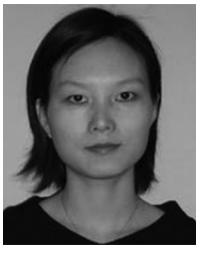
This research was supported in part by US National Science Foundation grants OAC-1724845, ACI-1719397 and CNS-1733596, NSF-1404981, IIS-1354123, CNS-1254006, and CNS-1249603, and Microsoft Research Faculty Fellowship 8300751.

References

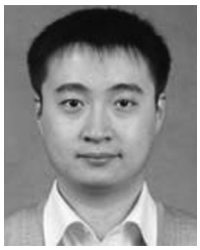
[1] B. O'Flynn, et al., "SmartCoast: A wireless sensor network for water quality monitoring," in *Proc. 32nd IEEE Conf. Local Comput. Netw.*, 2007, pp. 815–816.
[2] A. Cerpa, J. Elson, M. Hamilton, and J. Zhao, "Habitat monitoring: Application driver for wireless communications technology," in *Proc. ACM SIGCOMM Conf.*, 2001, pp. 20–21.
[3] F. Ye, G. Zhong, S. Lu, and L. Zhang, "Gradient broadcast: A robust data delivery protocol for large scale sensor networks," *Wireless Netw.*, vol. 11, no. 3, pp. 285–298, May 2005.
[4] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks," in *Proc. 23rd Int. Conf. Distrib. Comput. Syst.*, 2003, pp. 46–55.
[5] K. Kalpakis, K. Dasgupta, and P. Namjoshi, "Efficient algorithms for maximum lifetime data gathering and aggregation in wireless sensor networks," *Comput. Netw.*, vol. 42, no. 6, pp. 697–716, 2003.
[6] T. Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst.*, 2003, pp. 171–180.
[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, 2000, pp. 56–67.
[8] S. Lindsey and C. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proc. IEEE Aerosp. Conf.*, 2002, pp. 3–1125–3-1130.
[9] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, 2000, pp. 243–254.
[10] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw.*, 2001, pp. 70–84.
[11] P. J. Wan, C. W. Yi, F. Yao, and X. Jia, "Asymptotic critical transmission radius for greedy forward routing in wireless ad hoc networks," in *Proc. 7th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2006, pp. 25–36.
[12] L. Wang, C. W. Yi, and F. Yao, "Improved asymptotic bounds on critical transmission radius for greedy forward routing in wireless ad hoc networks," in *Proc. 9th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2008, pp. 131–138.
[13] Y. Yang, Y. Li, and M. Hou, "Many-to-one deliverability of greedy routing in 2-D wireless sensor networks," in *Proc. IEEE INFOCOM*, 2011, pp. 2777–2785.
[14] L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks," *J. Netw. Syst. Manage.*, vol. 15, no. 2, pp. 171–190, 2007.
[15] X. Li, P. Wan, Y. Wang, and C. Yi, "Fault tolerant deployment and topology control in wireless networks," in *Proc. 4th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2003, pp. 117–128.
[16] S. Lin, J. Zhang, G. Zhou, L. Gu, T. He, and J. A. Stankovic, "ATPC: Adaptive transmission power control for wireless sensor networks," in *Proc. Int. Conf. Embedded Netw. Sensor Syst.*, 2006, pp. 223–236.
[17] J. Sheu, K. Hsieh, and Y. Cheng, "Distributed transmission power control algorithm for wireless sensor networks," *J. Inf. Sci. Eng.*, vol. 25, no. 5, pp. 1447–1463, 2009.
[18] H. Zhang, A. Arora, Y. ri Choi, and M. Gouda, "Reliable bursty convergecast in wireless sensor networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 266–276.
[19] I. Stoica, L. Popa, C. Raiciu, and D. Rosenblum, "Reducing congestion effects by multipath routing in wireless networks," in *Proc. IEEE Int. Conf. Netw. Protocols*, 2006, pp. 96–105.
[20] R. Kleinberg, "Geographic routing using hyperbolic space," in *Proc. IEEE INFOCOM*, 2007, pp. 1902–1909.
[21] T. Moscibrod, R. Wattenhofer, and A. Zollinge, "Topology control meets SINR: The scheduling complexity of arbitrary topologies," in *Proc. 7th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2006, pp. 310–321.
[22] F. Kuhn, R. Wattenhofer, and A. Zollinger, "Worst-case optimal and average-case efficient geometric ad-hoc routing," in *Proc. 4th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2003, pp. 267–278.
[23] R. Sarkar, X. Yin, J. Gao, F. Luo, and X. Gu, "Greedy routing with guaranteed delivery using Ricci flows," in *Proc. Int. Conf. Inf. Process. Sensor Netw.*, 2009, pp. 121–132.
[24] G. Xing, C. Lu, R. Pless, and Q. Huang, "On greedy geographic routing algorithms in sensing-covered networks," in *Proc. 5th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2004, pp. 31–42.
[25] Y. Wang, C. W. Yi, and F. Li, "Delivery guarantee of greedy routing in three dimensional wireless networks," in *Proc. 3rd Int. Conf. Wireless Algorithms Syst. Appl.*, 2008, pp. 4–16.
[26] T. Jurdzinski and G. Stachowiak, "The cost of synchronizing multiple-access channels," in *Proc. ACM Symp. Principles Distrib. Comput.*, 2015, pp. 421–430.
[27] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable information forwarding using multiple paths in sensor networks," in *Proc. 28th Annu. IEEE Conf. Local Comput. Netw.*, 2003, pp. 406–415.
[28] F. Kuhn, R. Wattenhofer, and A. Zollinger, "An algorithmic approach to geographic routing in ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 1, pp. 51–62, Feb. 2008.
[29] W. Wang, Y. Wang, X.-Y. Li, W.-Z. Song, and O. Frieder, "Efficient interference-aware TDMA link scheduling for static wireless networks," in *Proc. 12th Annu. Int. Conf. Mobile Comput. Netw.*, 2006, pp. 262–273.
[30] C. Wang, H. Ma, Y. He, and S. Xiong, "Adaptive approximate data collection for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 6, pp. 1004–1016, Jun. 2012.
[31] P. Floréen, P. Kaski, J. Kohonen, and P. Orponen, "Exact and approximate balanced data gathering in energy-constrained sensor networks," *Theoretical Comput. Sci.*, vol. 344, no. 1, pp. 30–46, 2005.
[32] C. Wang, J. Li, F. Ye, and Y. Yang, "NETWRAP: An NDN based real-time wireless recharging framework for wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 6, pp. 1283–1297, Jun. 2014.
[33] H. Gong, L. Zhao, K. Wang, W. Wu, and X. Wang, "A distributed algorithm to construct multicast trees in WSNs: An approximate steiner tree approach," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 347–356.
[34] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. Hoboken, NJ, USA: Wiley, 2007.
[35] V. Bhandari and N. H. Vaidya, "Reliable broadcast in wireless networks with probabilistic failures," in *Proc. 26th IEEE Int. Conf. Comput. Commun.*, 2007, pp. 715–723.
[36] H. P. Keeler and P. G. Taylor, "A stochastic analysis of a greedy routing scheme in sensor networks," *SIAM J. Appl. Math.*, vol. 70, no. 7, pp. 2214–2238, 2010.
[37] V. Rajendran, K. Obraczka, and J. Garcia-Luna-Aceves, "Energy-efficient, collision-free medium access control for wireless sensor networks," in *Proc. 1st Int. Conf. Embedded Netw. Sensor Syst.*, 2003, pp. 181–192.
[38] B. Hull, K. Jamieson, and H. Balakrishnan, "Mitigating congestion in wireless sensor networks," in *Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst.*, 2004, pp. 134–147.
[39] G. Anastasi, M. Conti, and M. Francesco, "The MAC unreliability problem in IEEE 802.15.4 wireless sensor networks," in *Proc. 12th ACM Int. Conf. Model. Anal. Simul. Wireless Mobile Syst.*, 2009, pp. 196–203.
[40] D. Gross, J. F. Shortle, J. M. Thompson, and C. M. Harris, *Fundamentals of Queueing Theory*. Hoboken, NJ, USA: Wiley, 2013.
[41] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks: Theory and practice," *ACM Trans. Sensor Netw.*, vol. 5, no. 4, pp. 1–24, 2009.

[42] G. Bianchi, "Performance analysis of the IEEE 802.11 distributed coordination function," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.
[43] S. De, A. Caruso, T. Chaira, and S. Chessa, "Bounds on hop distance in greedy routing approach in wireless ad hoc networks," *ACM Wireless Mobile Comput.*, vol. 1, no. 2, pp. 131–140, 2006.
[44] S. M. Harb and J. Mcnair, "Analytical study of the expected number of hops in wireless ad hoc network," in *Proc. 3rd Int. Conf. Wireless Algorithms Syst. Appl.*, 2008, pp. 63–71.
[45] K. Stamatiou and M. Haenggi, "Delay characterization of multihop transmission in a poisson field of interference," *IEEE/ACM Trans. Netw.*, vol. 22, no. 6, pp. 1794–1807, Dec. 2014.
[46] X. Yin, X. Zhou, R. Huang, Y. Fang, and S. Li, "A fairness-aware congestion control scheme in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5225–5234, Nov. 2009.
[47] P. Balister, Z. Zheng, S. Kumar, and P. Sinha, "Trap coverage: Allowing coverage holes of bounded diameter in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2009, pp. 136–144.
[48] H. Shokri-Ghadikolaei and C. Fischione, "Millimeter wave ad hoc networks: Noise-limited or interference-limited?" in *Proc. IEEE Globecom Workshops*, 2015, pp. 1–7.
[49] D. Wang, B. Xie, and D. P. Agrawal, "Coverage and lifetime optimization of wireless sensor networks with Gaussian distribution," *IEEE Trans. Mobile Comput.*, vol. 7, no. 12, pp. 1444–1458, Dec. 2008.
[50] S. Huang, H. Chang, and K. Wu, "A Jigsaw-based sensor placement algorithm for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2013, pp. 1–11, 2013.
[51] F. Yu, S. Park, E. Lee, and S.-H. Kim, "Hole modeling and detour scheme for geographic routing in wireless sensor networks," *J. Commun. Netw.*, vol. 11, no. 4, pp. 327–336, 2009.
[52] S. Lin, G. Zhou, K. Whitehouse, Y. Wu, J. Stankovic, and T. He, "Towards stable network performance in wireless sensor networks," in *Proc. IEEE Real-Time Syst. Symp.*, 2009, pp. 227–237.
[53] T. Moscibroda, Y. Oswald, and R. Wattenhofer, "How optimal are wireless scheduling protocols?" in *Proc. IEEE INFOCOM*, 2007, pp. 1433–1441.
[54] H. Li, Q. Hua, C. Wu, and F. Lau, "Minimum-latency aggregation scheduling in wireless sensor networks under physical interference model," in *Proc. 13th ACM Int. Conf. Model. Anal. Simul. Wireless Mobile Syst.*, 2010, pp. 360–367.
[55] NS2. [Online]. Available: http://www.isi.edu/nsnam/ns/, Accessed on: Mar. 2016.
[56] A. R. Dalton and J. O. Hallstrom, "An interactive, source-centric, open testbed for developing and profiling wireless sensor systems," *Int. J. Distrib. Sensor Netw.*, vol. 5, no. 2, pp. 105–138, 2009.
[57] Moteiv, "Tmote sky," [Online]. Available: http://www.eecs.harvard.edu/ konrad/projects/shimmer/references/tmote-sky-datasheet.pdf, Accessed on: Mar. 2016.

Jinwei Liu received the MS degree in computer science from Clemson University, South Carolina, and the University of Science and Technology of China, China, and the PhD degree in computer engineering from Clemson University, in 2016. His research interests include wireless sensor networks, cloud computing, data mining, machine learning, and social networks. He is a student member of the IEEE and the ACM.

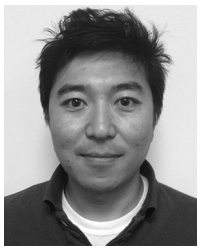


Haiying Shen (M'06-SM'13) received the BS degree in computer science and engineering from Tongji University, Shanghai, China, in 2000, and the MS and PhD degrees in computer engineering from Wayne State University, Detroit, Michigan, in 2004 and 2006, respectively. She is currently an associate professor in the CS Department, University of Virginia. Her research interests include distributed computer systems and computer networks, with an emphasis on P2P and content delivery networks, mobile computing, wireless sensor networks, and grid and cloud computing. She was the program co-chair for a number of international conferences and a member of the program committee of many leading conferences. She is a Microsoft Faculty Fellow of 2010, a senior member of the IEEE, and a member of the ACM.



Lei Yu received the BS and MS degrees in computer science from the Harbin Institute of Technology, China. He is working toward the PhD degree in the School of Computer Science, Georgia Institute of Technology, Georgia. His research interests include sensor networks, wireless networks, cloud computing, and network security.

Husnu Saner Narmanreceived the BS degree in mathematics from Abant Izzet Baysal University, Turkey, in 2006, the MS degree in computer science from the University of Texas at San Antonio, San Antonio, Texas, in 2011, and the PhD degree in computer science from the University of Oklahoma, Norman, Oklahoma, in 2016. Currently, he is a faculty member with Marshall University, Huntington, West Virginia. His research interests include queuing theory, network management, network topology, Internet of Things, LTE, and cloud computing.



Jiannan Zhai received the BE degree in software engineering from Shandong University, the MS degree in computer science from the Beijing University of Posts and Telecommunications, China, and the PhD degree in computer science from Clemson University, in 2014. He serves as the chief engineer of the Institute for Sensing and Embedded Network Systems Engineering (I-SENSE), Florida Atlantic University.

Jason O. Hallstrom received the BS degree in system analysis, and the MA degree in economics, both from Miami University, respectively, and the MS and PhD degrees in computer and information science, both from Ohio State University, respectively. He serves as director of the Institute for Sensing and Embedded Network Systems Engineering (I-SENSE), Florida Atlantic University and professor of computer and electrical engineering and computer science. He is a senior member of the IEEE.

Yangyang He received the BE degree in computer engineering from Beihang University, China, and the MS degree in computer science from Clemson University. He is currently working toward the PhD degree in computer science at Clemson University. His research interests include embedded systems, wireless sensor networks, and heterogeneous computing.