Jamming-Resilient Message Dissemination in Wireless Networks

Yifei Zou, *Member, IEEE,* Dongxiao Yu, *Senior Member, IEEE,* Pengfei Hu, *Member, IEEE,* Jiguo Yu, *Senior Member, IEEE,* Xiuzhen Cheng, *Fellow, IEEE,* Prasant Mohapatra, *Fellow, IEEE*

Abstract—This paper initiates the study for the basic primitive of distributed message dissemination in multi-hop wireless networks under a strong adversarial jamming model. Specifically, the message dissemination problem is to deliver a message initiating at a source node to the whole network. An efficient algorithm for message dissemination can be an important building block for solving a variety of high-level network tasks. We consider the hard non-spontaneous wakeup case, where a node only wakes up when it receives a message. Under the realistic SINR model and a strong adversarial jamming model that removes the budget constraint commonly adopted in previous work by the adversary, we present a distributed randomized algorithm that can accomplish message dissemination in $\mathscr{T}(O(D(\log n + \log R)))$ time slots with a high probability performance guarantee, where $\mathscr{T}(U)$ is the number of time slots in the interval from the beginning of the algorithm's execution that contains U unjammed time slots, n is the number of nodes in the network, D is the network diameter, and R is the distance with respect to which the network is connected. Our algorithm is shown to be almost asymptotically optimal by the lower bound $\Omega(D \log n)$ for non-spontaneous message dissemination in networks without jamming.

Index Terms—Jamming-Resilience, Global Message Dissemination, SINR Model.

1 Introduction

Jamming is a common phenomenon in real-world wireless networks. It can be caused by both natural factors (such as when concurrently operating wireless networks use the same channel) as well as security attacks. Jamming can be very harmful to communications but it is hard to avoid. For example, a jammer can prevent the widely used IEEE 802.11 MAC protocol from delivering any message [4] by jamming only a small fraction of the time slots. Hence, devising jamming-resilient communication protocols has become imperatively important and necessary.

In previous work, it was common to assume that an adversary can have full control of the jamming on the shared channel, such that the worst case always occurs and needs to be considered. In order to derive efficient algorithms with provable performance guarantees, a more reasonable mechanism (e.g., in [26], [27], [31], [32]) was proposed, which sets an energy budget constraint for the adversary so that it can only jam the shared channel within a specified fraction of the time slots. In this case, nodes can appropriately adapt to the contention on the channel by correctly detecting the transmissions in the unjammed time slots. However, if the jammer is sufficiently strong, jamming can still occur much more frequently than expected and only a small fraction of the time slots can be used for message transmissions. Under such situations, a more comprehensive model is needed to cover the jamming scenarios that are as general as possible, such that the designed algorithms can perform well in reality when facing strong adversaries.

In this paper, we adopt a strong adversarial jamming model based on the Signal-to-Interference-plus-Noise-Ratio (SINR) interference model, which was newly proposed in [48] in 2019, to depict the jamming phenomena in reality. SINR has been widely adopted by researchers in recent years in the wireless algorithm domain due to its proximity to reality in depicting interference, unlike those oversimplified graph based models. The global definition of interference, however, poses a great challenge for interference control using localized distributed algorithms. The main feature of the strong jamming model lies in that it removes the energy budget constraint on the adversary, which is set by almost all previous work, to allow jamming on the shared channel to occur in any round at will.

Under the strong adversarial jamming model, we choose a frequently used primitive operation in wireless networks to illustrate our approach to overcoming jamming. More specifically, we study the basic primitive of message dissemination, in which a source message $\mathcal{M}$ from the source node s is required to be delivered to all nodes in the network via transmissions on an unreliable multiple access channel. The solutions for message dissemination have been widely used as building blocks for high-level communication tasks. A successful message dissemination can also help simulate a single-hop network on top of a multi-hop one, which greatly simplifies the design and analysis of higher-level algorithms. A non-spontaneous wakeup mode is considered in this paper, where a node does not wake up until receiving a message. Clearly, compared with the setting in which

- *Y. Zou, D. Yu (Corresponding author), P. Hu (Corresponding author) and X. Cheng are with Institute of Intelligent Computing, School of Computer Science and Technology, Shandong University, P.R. China. E-mail:{yfzou,dxyu,phu,xzcheng}@sdu.edu.cn*
- *J. Yu is with the School of Computer Science and Technology, Qilu University of Technology (Shandong Academy of Sciences), Jinan, 250014, P. R. China, and also with the Shandong Computer Science Center (National Supercomputer Center in Jinan), Jinan, 250014, P. R. China. E-mail: jiguoyu@sina.com.*
- *P. Mohapatra is with Department of Computer Science, University of California, Davis, USA. E-mail: pmohapatra@ucdavis.edu*

Manuscript received MM DD, YYYY; revised MM DD, YYYY.

all nodes keep waking up from the beginning, the non-spontaneous wakeup mode is more energy-efficient but is much harder to handle, as it is impossible to construct a backbone to facilitate message dissemination.

Our main result is a nearly asymptotically optimal distributed and randomized algorithm for jamming-resilient message dissemination. Obviously, a distributed solution is more suitable for implementations in decentralized large-scale networks such as Internet-of-Things. The proposed algorithm can accomplish message dissemination in $\mathscr{T}(O(D(\log n + \log R)))$ time slots with high probability (i.e., with probability $1 - n^{-c}$ for some constant $c > 0$, denoted by w.h.p for short in sequel) in networks with size of n, diameter of D, and distance of R[1], where $\mathscr{T}(U)$ is the number of time slots during the interval from the beginning of the algorithm's execution that contains U unjammed time slots. Note that in [38], it was shown that $\Omega(\log n)$ is a lower bound for a successful transmission even without interference and jamming; hence $\Omega(D \log n)$ is a trivial lower bound for non-spontaneous message dissemination. On the other hand, in reality, R is usually bounded by $poly(n)$ and is just a constant in many cases. Therefore, our algorithm is nearly asymptotically optimal.

Our algorithm adopts a simple transmission scheme in which each node transmits with a fixed constant probability, to counter unpredictable jamming. Surprisingly, this simple scheme turns out to be extremely effective in balancing contention as we will illustrate later. More importantly, this fixed scheme is not susceptible to jamming attacks. Furthermore, though we assume a synchronous environment for communications, the global clock can no longer help to perfectly coordinate the operations of the nodes, as the nodes cannot acquire by themselves information regarding how many rounds were jammed in the past. To solve this problem, we let the nodes accumulate messages received from their neighbors, and use this information to estimate the number of steps the algorithm has been executed. Based on this estimation, the nodes can correctly determine the operations in the coming round.

Roadmap. The remainder of the paper is organized as follows. We present the related work and the jamming model in Sec. 2 and Sec. 3, respectively. The message dissemination algorithm is introduced in Sec. 4, followed by the corresponding analysis in Sec. 5. Simulation results are reported in Sec. 6, and Sec. 7 concludes the paper.

2 Related Work

In the past few decades, several models have been proposed to depict jamming in reality. The simplest one perhaps is the oblivious jamming model, in which a jamming schedule is determined at the beginning and remains unchanged during the algorithm execution. Based on this model, many mechanisms were designed for the purpose of avoiding/detecting jamming at the physical layer [21], [25], [33] and MAC layer [1], [11], [37], or hiding the transmission messages from adversaries [36]. Subsequently, two more comprehensive jamming models, namely the adaptive adversary jamming model [2], [9], [29], [32] and the reactive adversary jamming model [26], [27], [30], [31] (or the adaptive model and the reactive model, respectively, in short) were proposed. Unlike the oblivious jamming model, an adversary in the adaptive model is assumed to be aware of the protocol and the communication history information, thus can on-line jam the network. Here "on-line" means at the beginning of each round the adversary makes a new decision on jamming or not according to what it has already known. A reactive adversary, on the other hand, also gets the current network information to make an on-line decision. Generally speaking, no matter whether the adaptive or the reactive model is adopted, the following assumption is always made to simplify the algorithm design and analysis: only a constant fraction of the time steps can be jammed by the adversary and the jamming strategy in the whole network is the same at each time step. Here are a few examples. The problem of medium access control in a multi-hop network was studied in [32] under the adaptive model, and a jamming-resilient MAC protocol based on the adaptive model in a single-hop network, which attains a constant competitive throughput, was proposed in [2]. These protocols were then extended to the adaptive model in multi-hop networks and to the reactive model in a single-hop network in [29] and [30], respectively. Based on the reactive model, the problem of self-stabilizing leader election in a single-hop network was investigated in [31]. Note that all the above results were derived under graph-based interference models. Even through SINR is more accurate and realistic in depicting the interference in transmissions, it presents a great challenge for distributed algorithm design; thus only a few SINR-based jamming-resilient protocols were proposed in recent years. For examples, in [26] and [27], distributed MAC protocols were presented under an SINR-based adaptive adversarial jamming model with energy budget limitation. Unlike the previous work mentioned above, the jamming model proposed in [48] made a breakthrough in that it removed the energy budget on an adversary so that the adversary could jam the network in any round at will, which was obviously much more comprehensive and realistic than the previous ones. Under such a strong jamming model, the work in [48] considered a backbone construction via local broadcast between spontaneous wakeup nodes. Here, in this paper, we also adopt such a strong jamming model, and try to solve the global message dissemination problem under the hard non-spontaneous wakeup cases.

As one of the most fundamental and extensively studied communication primitives, message dissemination in wireless networks (without considering the existence of jamming) has been investigated under both graph-based models [3], [5], [6], [7], [12], [14], [19], [20] and the SINR model [8], [13], [15], [17], [18], [22], [23], [24], [34], [35], [39]. For message dissemination with non-spontaneous wakeup nodes under graph-based models, the best randomized results are $O(D \log(n/D) + \log^2 n)$ [12], [20] and $O(D + \log^6 n)$ [14] without and with collision detection, respectively; for the SINR model, the best known algorithm was proposed in [16], which can accomplish message dissemination in $O(D \log^2 n)$ rounds. As for the global message dissemination in jammed networks, to the best of our knowledge, no known result exists and our work offers the first distributed randomized solution that has an

1. the network is connected with respect to distance R

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2021.3108004, IEEE Transactions on Mobile Computing

asymptotically optimal time complexity guaranteed by a high probability.

3 Model and Definition

We assume a 2-dimensional Euclidean space with n nodes arbitrarily deployed. The time is divided into rounds, with each of which containing a constant number of slots. A slot is a time unit that is long enough for the nodes to transmit or receive a message. The transmissions between nodes at each slot are synchronized.

Communication Model. Assume that the nodes transmit in a multiple access channel, and the simultaneous transmissions between nodes interfere with each other. An SINR model is used to depict the interference caused by simultaneous transmissions. Within each slot, we use transmitter/listener to indicate the nodes who transmit/listen, and $\mathcal{T}_{u,v}$ to indicate the transmission from transmitter u to listener v. For a fixed $\mathcal{T}_{u,v}$, let W be the set of other transmitters who simultaneously transmit with u, $\mathcal{I}_W(v, \mathcal{T}_{u,v})$ be the sum of the interference at listener v caused by the nodes in the set W, and $SINR(v, u, W)$ be the SINR rate of the transmission $\mathcal{T}_{u,v}$. Then

$$\begin{aligned} \mathcal{I}_W(v, \mathcal{T}_{u,v}) &= \sum_{w \in W} P_w \cdot d(w, v)^{-\alpha} \\ SINR(v, u, W) &= \frac{P_u \cdot d(u, v)^{-\alpha}}{\mathcal{N} + \mathcal{I}_W(v, \mathcal{T}_{u,v})} \end{aligned} \tag{1}$$

In the above equations, P_w is the transmission power of node w; $d(w, v)$ is the Euclidean distance between node w and v; $\alpha \in (2, 6]$ is the path-loss exponent determined by the environment; and $\mathcal{N}$ is the ambient noise in the network. This SINR model defines that transmission $\mathcal{T}_{u,v}$ succeeds if and only if $SINR(v, u, W) \geq \beta$, where $\beta > 1$ is a constant threshold determined by hardware. A series of works in SINR model can be found in [40], [41], [42], [46], [49].

Strong Adversarial Jamming Model. When the ambient noise is too large to guarantee the success of transmissions in a network, we say the network is jammed. By normalizing the minimum distance between two nodes to 1, we assume that the network is connected with respect to a distance R[2] when the network is un-jammed. Transmission power among the nodes in the network can be different, P_{min} and P_{max} are the minimum and maximum transmission powers among all the nodes in the network, and P_{max}/P_{min} is assumed to be a constant. Since nodes can transmit with various transmission powers, their communication ranges also vary. For any transmission $\mathcal{T}_{u,v}$ with $d(u, v) \leq r$, we say $\mathcal{T}_{u,v}$ is a transmission within distance r.

When the network is un-jammed, the ambient noise is denoted by $\mathcal{N}$. Since the network is connected within distance R when it is un-jammed, an inherent threshold for the ambient noise $\mathcal{N}$ is $\frac{P_{min}}{R^\alpha \beta}$ according to the SINR model. More specifically, for any ambient noise $\mathcal{N} > \frac{P_{min}}{R^\alpha \beta}$, it is impossible to ensure that all transmissions within distance R in the network succeed. However, $\mathcal{N} = \frac{P_{min}}{R^\alpha \beta}$ is also a very ideal case since the transmissions with power P_{min} may still fail if there are other simultaneous transmissions in the multiple access channel. A standard assumption is to set a tighter jamming threshold $N = \frac{P_{min}}{(1+\epsilon)^\alpha R^\alpha \beta}$, with ϵ being a positive constant, i.e., the upper bound for ambient noise in the un-jammed network should be constant times smaller than the inherent threshold to make sure that the transmissions can tolerant some interference in the network. The works in [43], [44], [45], [47] also have the similar assumption. In this paper, we assume that the variance of the ambient noise on the shared channel is round-based, i.e., the ambient noise in the network remains unchanged within a round. At any round, if $\mathcal{N} \leq N$, we say the network is un-jammed in this round. The definition of the jamming behavior in the network is detailed in the following.

In reality, whether the network will be jammed or not is hard to predict since the ambient noise changes rapidly because of natural and artificial factors. To fully consider the jamming caused by the ambient noise changes and ensure that the model is close to reality, we assume that there is a strong adversary who can determine the ambient noise in the network at each round. The adversary has the following capabilities and features:

- Similar to the previous work [26], [32], we assume the uniform jamming pattern in our model, i.e. at each round, the ambient noise for all the nodes in the network is the same.
- The adversary does not have any energy budget, and can jam the network in any round at will. Note that if the adversary sets the ambient noise slightly larger than N, some transmissions between nearby nodes can still succeed. Hence, the adversary without energy budget jams the network by setting the ambient noise larger than P_{max}/β. As the minimum distance between nodes in the network is normalized to 1, when the adversary jams the network by such an ambient noise, all transmissions in the network are destroyed.
- The adversary is reactive, i.e., it knows the history and the current states of the protocol execution, and can instantly make a jamming decision based on that information.

Note that in [26], [27], [30], it is assumed that the adversary can at most jam $(1-\epsilon)$-fraction of rounds in an interval, with the requirement that $\epsilon \in \Omega(1)$ and $\epsilon \in (0, 1)$. Such a kind of jamming model can cover lots of scenarios in reality when the jamming is not heavy. However, the heavy jamming situations with $\epsilon \in o(1)$ are not considered by the models in [26], [27], [30]. In our jamming model, both of the cases with $\epsilon \in \Omega(1)$ and $\epsilon \in o(1)$ are considered since the adversary can jam any round at will. Due to the fraction of unjammed rounds in an interval is unknown, we can only use the notation $\mathscr{T}(U)$ to denote the time complexity of our algorithm.

Knowledge and Capability of the Nodes. Each node has the values of R, $\frac{P_{max}}{P_{min}}$, the SINR parameters α and β, and the network size n. A half-duplex transceiver is equipped on every node; thus nodes can transmit or listen in each slot but cannot do both. Location information is provided to the nodes at the beginning of the algorithm execution by some services such as GPS or other techniques [10]. Physical

2. Usually the ratio of the communication range and the minimum distance between two nodes cannot be exponentially large. Thus, it is not hard to find a distance R, with respect to which the network is connected, and bounded by $poly(n)$; hence $\log R \in O(\log n)$.

carrier sensing is not needed, i.e., nodes have no need to monitor the channel at each slot and know nothing about the transmissions on the channel when it receives no message, which is energy saving.

4 Message Dissemination Algorithm

In this section, we present a message dissemination algorithm which delivers a source message $\mathcal{M}$ from the source node s to all other nodes in the network w.h.p. in an asymptotically optimal running time. Initially, only the source node s has the source message, and all other nodes wake up when receiving the source message, which is known as the non-spontaneous wakeup mode.

Note that some classical schemes for message dissemination can no longer be used under the strong adversary jamming model with the non-spontaneous wakeup setting. For example, the adversary without energy budget makes it almost impossible for the classical adaptive contention balancing strategies to work though they can greatly facilitate message dissemination as demonstrated in previous studies [26], [27]. More specifically, in classical adaptive contention balancing strategies, each node adjusts its transmission probability by detecting the contention on the shared channel to maintain the contention at an appropriate level such that the shared channel can be fully utilized. However, a long and unknown-length jamming interval can simply mislead the nodes when detecting the contention, making it impossible to balance the contention in an acceptable time. Another commonly used scheme is the elect-first and broadcast-later scheme [39], which first elects a leader at each local region and then only lets the leaders disseminate the message. Such a scheme can greatly reduce the interference and consequently decrease collisions. However, it can be easily disrupted without much effort: since a node can hardly know when a leader-election option is finished and whether or not it is elected as a leader because of the unpredictable jamming rounds, all the nodes have to keep executing the leader election process and thus the message cannot be delivered efficiently; additionally, an adversary who already know the protocol can damage the message dissemination by jamming the network only when the leaders are broadcasting the message.

In this study, we also need to address the following challenges: how to control the global interference defined in SINR using a localized distributed coordination approach and how to control the suddenly increased interference due to nodes' non-spontaneous waking up. To address these challenges, we set a fixed constant transmission probability for each node instead of using any adaptive contention balancing strategy; thus the contention in the network cannot be misled by jamming. Additionally at each round, nodes adopt a new elect-and-broadcast scheme that does leader election and message broadcast via a same message, to avoid separating them into two different rounds with different messages; thus the adversary can't easily damage the protocol by jamming only the broadcast rounds. By accumulating the messages received from its neighbors, a node can figure out how many un-jammed rounds in the past and whether it becomes a leader or not. To bound the global interference in the SINR model, we design a TDMA scheme by griding and coloring the nodes in the network, allowing the nodes with the same color to transmit in the same slot of each round to avoid interference from the nearby cells. Only when elected as a leader can a node broadcast the message in a specific slot, which ensures that the message transmitters are sparse enough with each other and the interference caused by the transmitters are not too large. Finally, four states are designed for the non-spontaneous wakeup nodes so that the interference in the network cannot be suddenly increased by a large number of nodes waking up within a round. In our analysis we shall show the above schemes and tricks in more detail, and prove that our algorithm is correct and efficient enough to get an asymptotically optimal result.

0	1	...	c-1	0	1	...
c	c+1	...	2c-1	c	c+1	...
...	...	...	...	...	...	...
(c-1)c	...	...	c*c-1	(c-1)c	...	...
0	1	...	c-1	0	1	...
c	c+1	...	2c-1	c	c+1	...
...	...	...	...	...	...	...

Fig. 1: Coloring of cells

4.1 Preliminaries on Cells and Nodes

We first divide the network area into grids as follows. Denote by $\mathcal{G}$ the grid obtained by the division, which consists of square cells of size $\frac{\epsilon R}{2\sqrt{2}} \times \frac{\epsilon R}{2\sqrt{2}}$. The division is in such a way that all cells are aligned with the coordinate axes: point $(0,0)$ is the grid origin. Each cell includes its left side without the top endpoint, and its bottom side without the right endpoint, and does not include its right and top sides. A cell has the coordinate of (i,j) when its bottom left corner is located at $(\frac{\epsilon R}{2\sqrt{2}} * i, \frac{\epsilon R}{2\sqrt{2}} * j)$, and is denoted as $g(i,j)$, for $(i,j) \in \mathbb{Z}^2$. For a node v with coordinate (x,y) on the plane, it is in cell $g(i,j)$ of grid $\mathcal{G}$ when $i * \frac{\epsilon R}{2\sqrt{2}} \le x < (i+1) * \frac{\epsilon R}{2\sqrt{2}}$ and $j * \frac{\epsilon R}{2\sqrt{2}} \le y < (j+1) * \frac{\epsilon R}{2\sqrt{2}}$.

After the griding process, a coloring scheme is given on the cells and nodes as follows: the cell $g(i,j)$ and the nodes in the cell $g(i,j)$ get the color $c * (i \mod c) + (j \mod c)$, where the constant $c = \lceil ((\frac{P_{max}}{P_{min}} * \frac{32\frac{\alpha-1}{\alpha-2}+4}{(1+\epsilon/2)^{-\alpha}-(1+\epsilon)^{-\alpha}})^{\frac{1}{\alpha}}) * \frac{\sqrt{2}}{\epsilon} + 1\rceil$. Obviously, it uses $c * c$ colors to color all cells and nodes as illustrated in Fig 1. In our algorithm, a round is divided into $2 * c * c$ slots. A node in color j transmits in slot

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2021.3108004, IEEE Transactions on Mobile Computing

j when it is in state $\mathbb{B}$, and transmits in slot $c*c+j$ when it is in state $\mathbb{A}$. The description on the nodes' states is given later.

Based on the above notions and definitions, we can generate a TDMA scheme for the algorithm's execution at each round to avoid the interference from the nodes in nearby cells, which will be detailed in our analysis section.

4.2 Detailed Description for Algorithm Execution

Algorithm 1 presents the pseudo-code for our message dissemination algorithm. The process is divided into successive rounds, with each consisting of 2*c*c slots. There are four states, namely $\mathbb{I}$, $\mathbb{A}$, $\mathbb{B}$, and $\mathbb{S}$ for the nodes in the network. Nodes in different states have different operations at each round. We denote by $\mathcal{M}_u$ the message that contains the source message and the cell ID of node u.

- A node in state $\mathbb{I}$ means that the node is not ready to help deliver the source message $\mathcal{M}$. Considering that nodes have the non-spontaneous wakeup assumption, only when receiving a message can the nodes wake up. All nodes except the source node are in state $\mathbb{I}$ initially. A node in state $\mathbb{I}$ listens at each round, and when receiving message $\mathcal{M}_v$ from transmitter v in the first $c*c$ slots, it wakes up, and changes its state to $\mathbb{S}$ if it is in the same cell with v, or changes to $\mathbb{A}$ otherwise.
- A node in state $\mathbb{A}$ means that the node has already received the source message and will try to help deliver the message. Node u in state $\mathbb{A}$ and color j has two operations within a round. It first listens in the first $c*c$ slots and then transmits message $\mathcal{M}_u$ with constant probability p or listens otherwise in slot $c*c+j$, where $p = \frac{P_{min}^2}{P_{max}^2} * \frac{2^{\alpha}-\epsilon^{\alpha}/(1+\epsilon)^{\alpha}}{3*2^{2\alpha+7}\beta} * (1-2^{1-\alpha/2})$. If u receives a message $\mathcal{M}_v$ from node v in the same cell, u changes its state to $\mathbb{S}$. At the end of each round, if u has received the source message in the first $c*c$ slots for $k*(\log n + \log R)$ rounds, where k is a sufficiently large constant, u changes its state to $\mathbb{B}$.
- A node in state $\mathbb{B}$ means that the node becomes a source message transmitter who helps to deliver the message. Node u in state $\mathbb{B}$ and color j transmits the message $\mathcal{M}_u$ in the j-th slot of each round.
- A node in state $\mathbb{S}$ means that the node does not need to deliver the source message since some other nodes in the same cell will do that. Nodes in $\mathbb{S}$ do nothing in the subsequent rounds.

Figure 2 depicts the states, operations, and the corresponding transformations of the nodes at each round. Initially, only the source node is in state $\mathbb{B}$ and all other nodes are in state $\mathbb{I}$. During the algorithm execution, nodes move from state $\mathbb{I}$ to $\mathbb{A}$ or $\mathbb{S}$ when receiving the source message in the first $c*c$ slots of each round. Meanwhile, nodes in state $\mathbb{A}$ move to state $\mathbb{S}$ when receiving the source message from other nodes in the same cell, or move to state $\mathbb{B}$ if receiving the source message in the first $c*c$ slots for $k*(\log n+\log R)$ rounds. Finally, as we shall prove in the next section, nodes in state $\mathbb{B}$ can accomplish message dissemination w.h.p..

Algorithm 1: Message disseminate for the source message $\mathcal{M}$

```
Initialization:
Source node s: state_s = B; t_s = 0; cell ID: c_s;
  Transmitted message: M_s = {M + c_s};
Any other node u: state_u = I; t_u = 0; cell ID: c_u;
  Transmitted message: M_u = NULL;

At each round, node u in state I:
Listen;
if receive M_v in the first c*c slots then
    if c_v = c_u then
        state_u = S;
    else
        state_u = A;
        M_u = {M + c_u};

At each round, node u in color j, state A:
Listen in the first c*c slots;
if receive M_v in the first c*c slots then
    t_u++;
Transmit M_u with probability p or listen otherwise
  in slot c*c+j;
if receive M_v and c_v = c_u then
    state_u = S;
if t_u = k*(log n + log R) then
    state_u = B;

At each round, node u in color j, state B:
Transmit M_u in slot j;

At each round, node u in state S:
Do nothing;
```

5 Algorithm Analysis

Aiming at proving the correctness and efficiency of our algorithm, we show how the source message $\mathcal{M}$ is disseminated from the source node s to any other node s' in the network within $\mathscr{T}(O(D(\log n + \log R)))$ rounds. Since the network is connected within distance R when it is not jammed, there is always a path, denoted as $\mathcal{P}_{s\to s'}$, starting from node s and ending at node s'. Without loss of generality we define that $\mathcal{P}_{s\to s'} = \{s \to s_1 \to ...s_{|l|-1} \to s'\}$ as following: s_i is the i-th node on $\mathcal{P}_{s\to s'}$ in the direction from s to s', and is in color J_i; for any pair of nodes s_i and s_{i+1} on the path $\mathcal{P}_{s\to s'}$, there is a link from nodes s_i to s_{i+1} with a length no larger than R; positive integer l is the number of hops of the path $P_{s\to s'}$ which is at most D. Nodes s and s' can also be regarded as s_0 and s_l, respectively. In the following, we focus on the message dissemination along the path $\mathcal{P}_{s\to s'}$ link by link.

The following analysis is based on phases, with each of which consisting of $\mathscr{T}(k*(\log n + \log R))$ rounds. Let $\mathfrak{P}_i$ be the i-th phase containing $\mathscr{T}(k*(\log n + \log R))$ rounds, where $i = 1, 2, ..., l$. We plan to show that at phase $\mathfrak{P}_i$, the source message $\mathcal{M}$ is disseminated to s_i.

Lemma 1. At any un-jammed round of $\mathfrak{P}_1$, all the nodes v

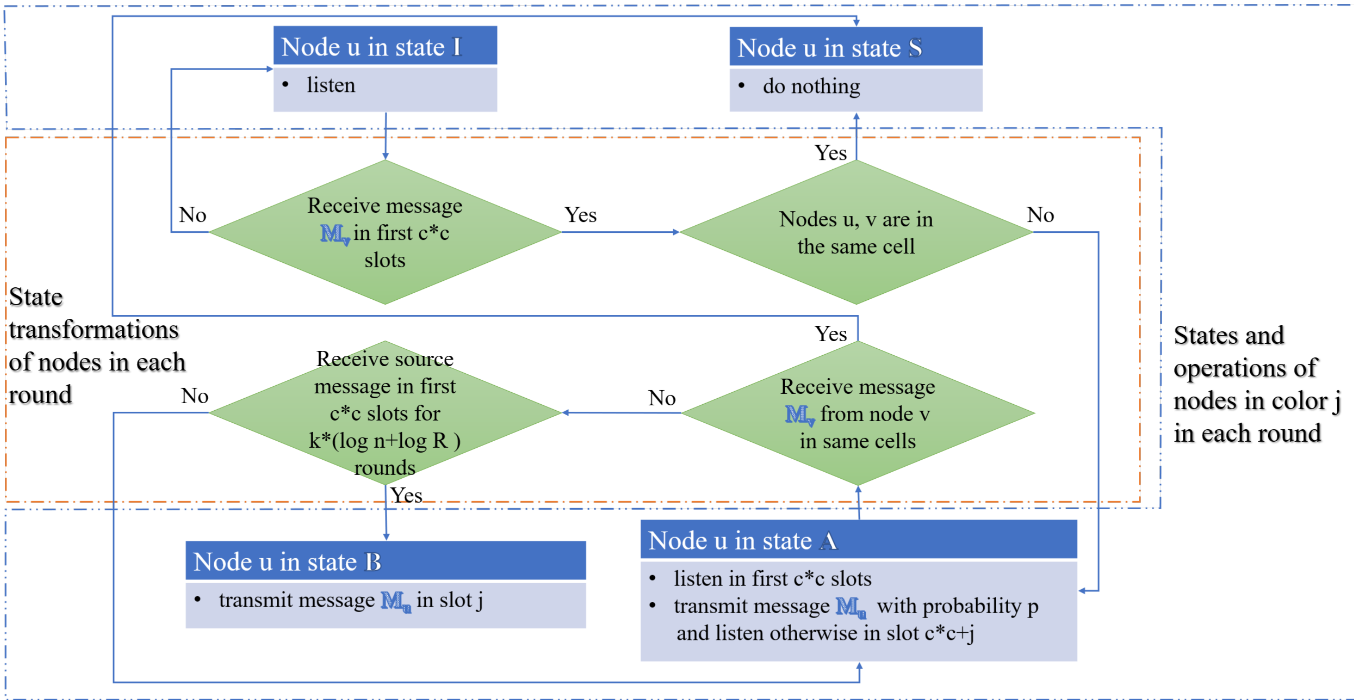


Fig. 2: States, operations and corresponding transformations of nodes at each round

within distance R from s_0 can receive the source message.

Proof. $\mathfrak{P}_1$ consists of $k*(\log n+\log R)$ un-jammed rounds. Initially, only the source node s_0 is in state $\mathbb{B}$, and all the other nodes are in state $\mathbb{I}$. For any node in color j changing state from $\mathbb{I}$ to $\mathbb{B}$, at least $k*(\log n+\log R)$ un-jammed rounds are required to satisfy the condition of having received the source message in the first $c*c$ slots for $k*(\log n+\log R)$ rounds. Thus, s_0 is the only node in state $\mathbb{B}$ and the only transmitter in slot J_0 of each round during $\mathfrak{P}_1$. For the transmission from s_0 to v in an un-jammed round, according to the SINR inequality, we have:

$$\begin{aligned} \mathcal{I}_W(v,\mathcal{T}_{s_0,v})=0,\ \mathcal{N}\leq\frac{P_{min}}{(1+\epsilon)^{\alpha}R^{\alpha}\beta},\ d(s_0.v)\leq R \\ SINR(v,s_0,W)=\frac{P_{s_0}\cdot d(s_0,v)^{-\alpha}}{\mathcal{N}+\mathcal{I}_W(v,\mathcal{T}_{s_0,v})}\geq\beta \end{aligned} \tag{2}$$

Thus, we finish the proof. □

With Lemma 1, we prove that the message dissemination to s_1 succeeds in $\mathfrak{P}_1$. Then we analyze the process of s_2 receiving the source message in $\mathfrak{P}_2$. This process is far more complex than that of s_1 receiving the source message. When s_1 listens, only the source node s_0 holds the source message and transmits. While when s_2 listens, all the nodes within distance R from s_0 know the source message as is shown in Lemma 1, and it is possible for them to become source message transmitters in state $\mathbb{B}$. We need to bound the number of transmitters around s_2 to ensure that the interference at s_2 is not too large for receiving the source message from a transmitter.

Define $\mathcal{G}_1$ to be the set of cells containing the nodes in state $\mathbb{A}$ during $\mathfrak{P}_1$. According to Lemma 1, $\mathcal{G}_1$ is fixed after the first un-jammed round in $\mathfrak{P}_1$ since at each un-jammed round, there is always a same group of nodes receiving the source message from s_0. For any cell $g\in\mathcal{G}_1$, we have the following result.

Lemma 2. At the end of $\mathfrak{P}_1$, there is only one node in state $\mathbb{B}$ at cell g with high probability.

The corresponding proof of this lemma is quite mathematical and technical; thus we put it in the next subsection for a better reading experience.

With Lemma 2, one can see that with high probability at the beginning of phase $\mathfrak{P}_2$, each cell g in the set $\mathcal{G}_1$ has only one node in state $\mathbb{B}$ transmitting at its corresponding slot. When the above case occurs, w.l.o.g. we assume that node s_1 is in cell g_1 and s_1' is the node in state $\mathbb{B}$ at cell g_1. We next focus on the transmission from s_1' to s_2.

Lemma 3. In the first un-jammed round of $\mathfrak{P}_2$, all the nodes u within distance R from s_1 can receive the source message from s_1'.

Proof. Note that s_1 and s_1' are in the color of J_1 as we have assumed. Source message transmitter s_1' transmits the source message $\mathcal{M}$ in the J_1-th slot of each round at $\mathfrak{P}_2$. We analyze the transmission from s_1' to node u in the J_1-th slot of the first un-jammed round in $\mathfrak{P}_2$. For node u, the whole space can be divided into annuluses $\{C_b: b\geq 1\}$, with each C_b having the distance from u between $(b-1)(c-1)*(\frac{\sqrt{2}\epsilon}{4}R)$ and $b*(c-1)*(\frac{\sqrt{2}\epsilon}{4}R)$. Let D_b be the set of source message transmitters in slot J_1 and located at C_b for $b\geq 2$. Since there is at most one node in state $\mathbb{B}$ at each cell, our $c*c$ coloring scheme ensures that any two source message transmitters in slot J_1 are separated by a distance at least $(c-1)*(\frac{\sqrt{2}\epsilon}{4}R)$. Hence, the circles centered at the transmitters in D_b with radius of $(c-1)*(\frac{\sqrt{2}\epsilon}{8}R)$ are disjoint. Additionally, these circles are in the annulus with distance from u between $(b-\frac{3}{2})(c-1)*(\frac{\sqrt{2}\epsilon}{4}R)$ and $(b+\frac{1}{2})*(c-1)*(\frac{\sqrt{2}\epsilon}{4}R)$.

Then the number of transmitters in slot J_1 at each set D_b is upper bounded:

$$\frac{\pi(\frac{\sqrt{2}\epsilon}{4}R)^2 * ((b+\frac{1}{2})^2(c-1)^2 - (b-\frac{3}{2})^2(c-1)^2)}{\pi((c-1)*(\frac{\sqrt{2}\epsilon}{8}R))^2} \leq 16 * b$$

Furthermore, the number of nodes in C_1, which also transmit in the J_1-th slot, is at most 5, including s'_1. For the transmission from s'_1 to u, the interference on u caused by the other 4 transmitters in C_1 is at most $\mathcal{I}_{C_1} = 4P_{max} * ((\frac{\sqrt{2}\epsilon(c-1)}{4})R)^{-\alpha}$. Thus the interference $\mathcal{I}_W(u, \mathcal{T}_{s'_1,u})$ at u for the transmission from s'_1 to u in slot J_1 is bounded by:

$$\begin{aligned} &\mathcal{I}_{C_1} + \sum_{b=2}^{\infty} 16b * P_{max} * ((b-1)(c-1) * \frac{\sqrt{2}\epsilon}{4}R))^{-\alpha} \\ &\leq (4 + 32 * \frac{\alpha-1}{\alpha-2}) * P_{max} * (\frac{\sqrt{2}\epsilon(c-1)}{4})^{-\alpha} * R^{-\alpha} \quad (3) \\ &= (4 + 32 * \frac{\alpha-1}{\alpha-2}) * P_{max} * (\frac{\sqrt{2}\epsilon(c-1)}{4})^{-\alpha} * R^{-\alpha}. \end{aligned}$$

Note that $c = \lceil ((\frac{P_{max}}{P_{min}} * \frac{32\frac{\alpha-1}{\alpha-2}+4}{(1+\epsilon/2)^{-\alpha}-(1+\epsilon)^{-\alpha}})^{\frac{1}{\alpha}}) * \frac{\sqrt{2}}{\epsilon} + 1\rceil$, when s'_1 transmits, u receives the source message based on the SINR condition

$$SINR(u, s'_1, W) \quad \geq \frac{P_{min} * d(s'_1, u)^{-\alpha}}{N + \mathcal{I}_W(u, \mathcal{T}_{s'_1,u})} \geq \beta$$

The above inequality holds because $d(s'_1, u) \leq d(s'_1, v) + d(v, u) \leq (1 + \frac{\epsilon}{2})R$. Thus, all the nodes within distance R from s_1 can receive the source message from s'_1 in the first un-jammed round of $\mathfrak{P}_2$. □

In our analysis, c is a complex constant determined by four parameters. However, when our algorithm is implemented in reality, we can directly set c to be a constant, which is sufficient large than $\lceil ((\frac{P_{max}}{P_{min}} * \frac{32\frac{\alpha-1}{\alpha-2}+4}{(1+\epsilon/2)^{-\alpha}-(1+\epsilon)^{-\alpha}})^{\frac{1}{\alpha}}) * \frac{\sqrt{2}}{\epsilon} + 1\rceil$, to guarantee the correctness of our algorithm. Also, it is a good idea to let the administrator determines the value of c according to whether the message dissemination can succeed, since the message dissemination fails when constant c is not large enough.

With Lemma 2 and 3, we prove that in our algorithm, when s_1 receives the source message in $\mathfrak{P}_1$, s_2 receives the source message in $\mathfrak{P}_2$ w.h.p.. With a similar definition, analysis and proof, we can get that (1) at the end of $\mathfrak{P}_2$, there is only one node in state $\mathbb{B}$ at cell g with high probability, where g can be any of the cells that once contain nodes in state $\mathbb{A}$ during $\mathfrak{P}_1$ and $\mathfrak{P}_2$; (2) in the first un-jammed round of $\mathfrak{P}_3$, all the nodes within distance R from s_2 can receive the source message from s'_2, i.e. the source message is disseminated to s_3 w.h.p. in $\mathfrak{P}_3$. We can continue this analysis and prove that s_l receives source message in $\mathfrak{P}_l$ w.h.p. when s_{l-1} receives the source message in $\mathfrak{P}_{l-1}$. In other words, when nodes in a same cell receive the source message, a leader will be elected first, and then the leader will disseminate the source message across the next hop. Thus, for the path $\mathcal{P}_{s\to s'}$ from the source s to any node s', the message dissemination can be finished in $\mathfrak{P}_l$ w.h.p., where l is the number of hops in $\mathcal{P}_{s\to s'}$.

Theorem 1. The message dissemination in our algorithm can be finished with high probability with time complexity of $\mathscr{T}(O(D * (\log n + \log R)))$, for a network with size of n, diameter of D, and distance of R.

5.1 Technical Proof for Lemma 2

We consider the situation at cell g during $\mathfrak{P}_1$ and all the results in this proof only hold in $\mathfrak{P}_1$. Assume that the nodes in g have color j. For brief description, we call a node **active** if it is in state $\mathbb{A}$, and when it changes state to $\mathbb{S}$, we say it becomes **inactive**. Thus, the active node v in cell g transmits message $\mathcal{M}_v$ with probability p in the $c*c+j$-th slot from the first un-jammed round in $\mathfrak{P}_1$. When receiving $\mathcal{M}_u$ from other active nodes in the same cell, v in state $\mathbb{A}$ changes to state $\mathbb{S}$; and after having received the source message in the first $c*c$ slots for $k*(\log n + \log R)$ rounds, node v in state $\mathbb{A}$ changes to state $\mathbb{B}$ at the end of the current round. Note that $\mathfrak{P}_1$ consists of $k*(\log n + \log R)$ un-jammed rounds, and for any node v in cell g, it receives the source message in the first $c*c$ slots of an un-jammed round and receives nothing in a jammed round. Thus, any active node at the end of $\mathfrak{P}_1$ changes state to $\mathbb{B}$. The proof is completed if we can prove that at the final un-jammed round of $\mathfrak{P}_1$, there is one and only one active node left in cell g.

We assume that there are n' active nodes in cell g after s_0 transmits at the J_0 slot of the first un-jammed round in $\mathfrak{P}_1$. We consider the case where $n' \geq 2$ as otherwise we have already finished the proof. When $n' \geq 2$, the active nodes in cell g are in set V, and are divided into classes $\{V_i : i = 0, 1, \ldots, \log \frac{\epsilon}{2}R\}$. For an active node v with its nearest active neighbor u which is also at cell g, v is in the set V_i for $0 \leq i \leq \log \frac{\epsilon}{2}R - 1$ if the distance between u and v is within $[2^i, 2^{i+1})$, and is in the set $V_{\log \frac{\epsilon}{2}R}$ otherwise. The above division is only used for analysis purpose and the nodes know nothing about it. Let n_i be the number of nodes in the set $|v_i|$. From round t to round $t+1$ in $\mathfrak{P}_1$, one can see that firstly n_i does not increase since no new nodes in g changes state to $\mathbb{A}$ and secondly n_i may decrease because some active nodes become inactive.

Note that when all V_i for $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2}R - 1\}$ are reduced to empty, only one active node is left in the cell g. The following analysis contains two steps: we first prove that at each un-jammed round r of $\mathfrak{P}_1$, a constant fraction of active nodes in each set V_i become inactive at least with a constant probability; second we prove that by setting the parameter k sufficiently large, at the end of $\mathfrak{P}_1$, no node is left in the classes $\{V_i : i = 0, 1, \ldots, \log \frac{\epsilon}{2}R - 1\}$.

For $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2}R\}$, we use $V_{<i}(r)$ to denote the sets of nodes in classes V_js for $j < i$ at the beginning of a round r. Let $n_{<i}(r) = |V_{<i}(r)|$. Then, we get the following Lemma 4 as the result for our first step.

Lemma 4. At any un-jammed round r of $\mathfrak{P}_1$, $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2}R - 1\}$, if $n_{<i}(r) \leq \frac{1-(2^{1-\alpha/2})}{2} * n_i(r)$, then γ fraction of the nodes in V_i become inactive with probability $1 - e^{\Omega(n_i(r))}$, where $\gamma = \frac{p(1-p)}{8*(2s+5)^2}$, and $s = (\frac{P_{max}}{P_{min}} \cdot \frac{3\cdot 2^{2\alpha+7}\beta}{2^\alpha - \epsilon^\alpha/(1+\epsilon)^\alpha} \cdot \frac{1}{1-2^{1-\alpha/2}})^{\frac{1}{\alpha/2-1}}$.

Proof. Let $A(u, d)$ be the set of active nodes within distance d from u. The *exponential annulus* $E_t^i(u) = A(u, 2^{t+1}2^i) \setminus A(u, 2^t 2^i)$. An active node u in cell g is defined to be a *Sparse Node* if for every $t \in \{0, 1, ..., \log \frac{\epsilon}{2}R - 1\}$,

$E_t^i(u) \cap V \leq 48 * 2^{t(\alpha/2+1)}$. $S_i \subseteq V_i$ is the largest subset of $Sparse\ Node$s in V_i and for any pair of nodes u, v in S_i, the distance $d(u,v) \geq (s+2)2^i$, where $s = (\frac{P_{max}}{P_{min}} \cdot \frac{3 \cdot 2^{2\alpha+7}\beta}{2^\alpha - \epsilon^\alpha/(1+\epsilon)^\alpha} \cdot \frac{1}{1-2^{1-\alpha/2}})^{\frac{1}{\alpha/2-1}}$.

Claim 1. At any round r, for $i \in \{0, 1, ..., \log \frac{\epsilon}{2}R - 1\}$, if $n_{<i}(r) \leq \frac{1-(2^{1-\alpha/2})}{2} * n_i(r)$, then a constant fraction of the nodes in V_i are sparse.

Proof. For a node $u \in V_i$, if for every $t \in \{0, 1, ..., \log \frac{\epsilon}{2}R - 1\}$, it holds that $|E_t^i(u) \cap V_{\geq i}| \leq 24 * 2^{t(\alpha/2+1)}$ and $|E_t^i(u) \cap V_{<i}| \leq 24 * 2^{t(\alpha/2+1)}$, we say u is an $excellent\ node$. Clearly, an excellent node must be a sparse node. We next show that a fraction of the nodes in V_i are excellent nodes, by which a lower bound on the fraction of the sparse nodes can be obtained.

We first show the condition of $|E_t^i(u) \cap V_{\geq i}|$ in an excellent node. Because the nodes in $V_{\geq i}$ have distance at least 2^i with each other, the disks centered at nodes in $V_{\geq i}$ with radius 2^{i-1} are disjoint. Considering any given annulus $E_t^i(u)$, using an area argument shown in the following (4), it can be shown that for each node $u \in V_i$, $|E_t^i(u) \cap V_{\geq i}| \leq 24 * 2^{2t}$, which is smaller than $24 * 2^{t(\alpha/2+1)}$.

$$\begin{aligned} &\frac{\pi(2^{t+1}2^i + 2^{i-1})^2 - \pi(2^t 2^i - 2^{i-1})^2}{\pi 2^{2(i-1)}} \\ &= 3 * 2^{t+2} * (2^t + 1) \leq 3 * 2^{2t+3} < 24 * 2^{t(\alpha/2+1)} \end{aligned} \quad (4)$$

Then, we consider $|E_t^i(u) \cap V_{<i}|$ for node $u \in V_i$. Fix i and t. Let Γ_t^i be the sum of the nodes in $E_t^i(u) \cap V_{<i}$ for all the nodes in V_i. Then we have

$$\begin{aligned} \Gamma_t^i &= \sum_{u \in V_i} |E_t^i(u) \cap V_{<i}| = \sum_{u \in V_{<i}} |E_t^i(u) \cap V_i| \\ &\leq n_{<i}(r) * 24 * 2^{2t} \leq \frac{1-(2^{1-\alpha/2})}{2} * n_i(r) * 24 * 2^{2t} \end{aligned} \quad (5)$$

From (5) and the definition of excellent nodes, it is easy to see that there are at most $\frac{1-(2^{1-\alpha/2})}{2} 2^{t(1-\alpha/2)}$ fraction of the nodes in V_i that are not excellent ones in annulus $E_t^i(u)$ for each node $u \in V_i$, as otherwise the above inequality would be violated. Then we sum up the number of non-excellent nodes at each annulus as follows, which is an upper bound on the number of non-excellent nodes in V_i.

$$\begin{aligned} &\sum_{t=0}^{\log \frac{\epsilon}{2}R-1} n_i(r) * \frac{1-(2^{1-\alpha/2})}{2} * 2^{t(1-\alpha/2)} \\ =& n_i(r) * \frac{1-(2^{1-\alpha/2})}{2} * \sum_{t=0}^{\log \frac{\epsilon}{2}R-1} (2^{1-\alpha/2})^t \\ \leq& n_i(r) * \frac{1-(2^{1-\alpha/2})}{2} * \frac{1}{1-(2^{1-\alpha/2})} \\ =& \frac{1}{2} n_i(r). \end{aligned}$$

Thus, with the assumptions in Claim 1, at least half of the nodes in V_i are sparse nodes. □

Claim 2. For any $V_i, i \in \{0, 1, ..., \log \frac{\epsilon}{2}R-1\}$, at least $\frac{1}{(2s+5)^2}$ fraction of the sparse nodes are in the set S_i.

Proof. Because S_i is the largest subset of the sparse nodes that have distance $(s+2)2^i$ pairwise, the disks with radii $(s+2)2^i$ centered at nodes in S_i can cover all the sparse nodes in V_i. To get $|S_i|/|V_i|$, it suffices to upper-bound the number of sparse nodes covered by a node in S_i. This can be done using an area argument.

Now consider a node $v \in S_i$ and the sparse nodes in V_i within distance 2^i. Let D_v and D'_v be the disks centered at v that have radius $(s+2)2^i$ and $(s+\frac{5}{2})2^i$, respectively. Notice that each pair of the sparse nodes in D_v have distance at least 2^i. This means that the disks centered at these nodes with radii 2^{i-1} are disjoint, and all these disks are covered by D'_v. Then one can see that the number of sparse nodes in D_v is at most

$$\frac{\pi * ((s+2)2^i + 2^{i-1})^2}{\pi * (2^{i-1})^2} = (2s+5)^2$$

The Claim then follows. □

Claim 3. At each un-jammed round r of $\mathfrak{P}_1$, for $i \in \{0, 1, ..., \log \frac{\epsilon}{2}R - 1\}$, a constant fraction of the nodes in S_i become inactive with probability of $1 - e^{-\Omega(|S_i|)}$.

Proof. We first show that with a constant probability, a node $u \in S_i$ becomes inactive at the end of round r. Then the Claim can be obtained by the Chernoff bound.

We bound the probability under which $u \in S_i$ receives a message from its neighbors in the same cell. Let $\mathcal{E}$ be the event that u listens and its nearest neighbor (in the same cell) transmits. We have $Pr(\mathcal{E}) = p(1-p)$. We next assume that $\mathcal{E}$ occurs. Under this assumption, one can calculate the number of nodes receiving messages from their nearest neighbors.

To analyze the reception of the transmissions, we need to bound the interference at each node $u \in S_i$. Let T_i be the set of nearest neighbors of all nodes S_i. The interference are divided into two components, namely the interference from the nodes in $S_i \cup T_i$ and that from the other nodes.

We first bound the interference from the nodes in $S_i \cup T_i$. Consider a node $u \in S_i$. Notice that each node in S_i has distance at least $(s+2)2^i$ from u and has distance with its nearest neighbor in the range $[2^i, 2^{i+1})$. Thus the nodes in $(S_i \cup T_i) \setminus \{u, v\}$ have distance at least $s * 2^i$ from u. Then the interference at u from the nodes in $(S_i \cup T_i) \setminus \{u, v\}$ can be bounded as follows:

$$I_1 = \sum_{t=\log s}^{\infty} |E_t^i(u)| \frac{P_{max}}{(2^i 2^t)^\alpha} \leq \frac{48 P_{max}}{2^{i\alpha}} \cdot \frac{1}{s^{\alpha/2-1}} \cdot \frac{1}{1-2^{1-\alpha/2}}. \quad (6)$$

We next bound the interference from the nodes not in $S_i \cup T_i$. In particular, we show that with a moderate probability, a constant fraction of the nodes in S_i experience the interference that is caused by the nodes not in $S_i \cup T_i$ and is not large. Combining the previous results, we can finally prove the claim.

Let $\hat{I}(v)$ be the interference at the nodes in S_i that is generated by a node $v \notin S_i \cup T_i$. For a node $v \notin S_i \cup T_i$, $\hat{I}(v)$ can also be recorded as the sum of the interference on the nodes in $E_t^i(v) \cap S_i$ over all annulus. Using an area argument as before, it can be obtained that $|E_t^i(v) \cap S_i| \le 24 * 2^{2t}$. Then

$$\begin{aligned}\hat{I}(v) &\le \sum_{t=0}^{\infty} |E_t^i(v) \cap S_i| \frac{P_{max}}{(2^i 2^t)^\alpha} = \frac{P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{|E_t^i(v) \cap S_i|}{2^{t\alpha}} \\ &\le \frac{P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{24 * 2^{2t}}{2^{t\alpha}} = \frac{24 P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{1}{2^{t(\alpha-2)}} \\ &< \frac{24 * P_{max}}{2^{i\alpha}} (\frac{1}{1 - 2^{2-\alpha}})\end{aligned} \tag{7}$$

Let $C_{max} = \frac{48}{1-2^{1-\alpha/2}}$ and we have $\hat{I}(v) < c_{max} P_{max}/2^{i\alpha}$. We next prove the conclusion that for any constant c_1, by setting $p = c_1/(4c_{max})$, with probability $1 - e^{-\frac{c_1^2}{24 c_{max}^2}|S_i|}$, at least half of the nodes in S_i experience the interference that is caused by the nodes not in $S_i \cup T_i$ and is not larger than $c_1 P_{max}/2^{i\alpha}$.

We prove the conclusion in two cases.

Case 1. $c_1 \ge c_{max}$.

Consider a node $u \in S_i$. Let $I(u)$ denote the interference experienced by u that are caused by the nodes not in $S_i \cup T_i$. Then

$$\begin{aligned}I(u) &\le \sum_{t=0}^{\infty} |E_t^i(u)| \frac{P_{max}}{(2^t 2^i)^\alpha} = \frac{P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{|E_t^i(u)|}{2^{t\alpha}} \\ &\le \frac{P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{48 * 2^{t(\alpha/2+1)}}{2^{t\alpha}} = \frac{48 P_{max}}{2^{i\alpha}} \sum_{t=0}^{\infty} \frac{1}{2^{t(\alpha/2-1)}} \\ &< \frac{48 P_{max}}{2^{i\alpha}} (\frac{1}{1 - 2^{1-\alpha/2}}) \le c_{max} P_{max}/2^{i\alpha}\end{aligned}$$

Case 2. $c_1 < c_{max}$.

We define a random variable x_v

$$x_v = \begin{cases} \hat{I}(v) 2^{i\alpha}/(c_{max} P_v) & \text{when node } v \text{ transmits} \\ 0 & \text{when node } v \text{ listens} \end{cases}$$

Then we have

$$\begin{aligned}\mathbb{E}\left[\sum_{v \notin S_i \cup T_i} x_v\right] &= \sum_{v \notin S_i \cup T_i} p * \hat{I}(v) 2^{i\alpha}/(c_{max} P_v) \\ &= p \sum_{v \notin S_i \cup T_i} \hat{I}(v) 2^{i\alpha}/(c_{max} P_v)\end{aligned}$$

For the case when $|S_i| c_1 P_{max}/2^{i\alpha+1} > \sum_{v \notin S_i \cup T_i} \hat{I}(v)$, this claim can be directly proved. For the other case when $|S_i| c_1 P_{max}/2^{i\alpha+1} \le \sum_{v \notin S_i \cup T_i} \hat{I}(v) \le |S_i| c_{max} P_{max}/2^{i\alpha}$, we can get $(c_1^2/8c_{max}^2)|S_i| \le \mathbb{E}\left[\sum_{v \notin S_i \cup T_i} x_v\right] \le c_1 P_{max}|S_i|/(4 P_{min} c_{max})$. Let $\mu = \mathbb{E}[\sum_{v \notin S_i \cup T_i} x_v]$. Notice that $x_v \in [0, 1)$. Then using the standard Chernoff bound for the set of independent random variables $\{x_v : v \notin S_i \cup T_i\}$, it follows that

$$\begin{aligned}&Pr\Big(\sum_{v \notin S_i \cup T_i} x_v \ge 2 * (c_1 P_{max}|S_i|/(4 P_{min} c_{max}))\Big) \\ \le &Pr\Big(\sum_{v \notin S_i \cup T_i} x_v \ge 2\mu\Big) \le e^{-\mu/3} \le e^{-\frac{c_1^2}{24 c_{max}^2}|S_i|}\end{aligned}$$

Thus, we prove with probability at least $1 - e^{-\frac{c_1^2}{24 c_{max}^2}|S_i|}$,

$$\begin{aligned}\sum_{v \notin S_i \cup T_i} \hat{I}(v) &= \sum_{v \notin S_i \cup T_i} x_v * c_{max} P_v / 2^{i\alpha} \\ &\le (2 c_1 P_{max}|S_i|/(4 P_{min} c_{max})) * c_{max} P_v/2^{i\alpha} \\ &= c_1 |S_i| \frac{P_{max}^2}{P_{min}} / 2^{i\alpha+1}\end{aligned}$$

Therefore it is impossible for more than half of the nodes in S_i to experience interference from the nodes not in $S_i \cup T_i$ larger than $c_1 \frac{P_{max}^2}{P_{min}}/2^{i\alpha}$.

Combining all the above results together and setting $c_1 = \frac{P_{min}^2}{P_{max}^2} * \frac{2^\alpha - \epsilon^\alpha/(1+\epsilon)^\alpha}{2^{2\alpha+1}\beta}$, one can see that with probability at least $1 - e^{-\frac{c_1^2}{24 c_{max}^2}|S_i|}$, at least half of the nodes $u \in S_i$ have the interference not larger than $2c_1 \frac{P_{max}^2}{P_{min}}/2^{i\alpha}$. Then by the SINR condition, we show that u can receive a message from its nearest neighbor v as follows.

$$SINR(v, u) > \frac{P_{min}/2^{\alpha(i+1)}}{2c_1 \frac{P_{max}^2}{P_{min}}/2^{i\alpha} + N} \ge \beta$$

Notice that the above analysis is based on the assumption that u listens and its nearest neighbor v transmits. This occurs with probability $p(1-p)$. Hence, under the condition that at least half of the nodes in $|S_i|$ can receive messages from their nearest neighbors, $p(1-p) * |S_i|/2$ nodes become inactive in expectation. Using the Chernoff bound, the Claim is then proved. □

With the above claims, one can see that for $i \in \{0, 1, 2, ... \log \frac{\epsilon}{2} R - 1\}$, (1) when $n_{<i}(r) \le \frac{1-(2^{1-\alpha/2})}{2} * n_i(r)$, $\frac{|S_i|}{|V_i|} \ge \frac{1}{2(2s+5)^2}$; (2) at each un-jammed round of $\mathfrak{P}_1$, with probability at least $1 - e^{\Omega(|V_i|)}$, more than $\frac{p(1-p)}{4}|S_i|$ nodes become inactive. Thus Lemma 4 is proved. □

Even with Lemma 4, we still have a long way to go to analyze the reduction process of the active nodes in cell g. We also need to consider the impact of jamming on the reduction process, and how to satisfy the assumption between $n_{<i}(r)$ and $n_i(r)$ in Lemma 4. Additionally, nodes in $V_{<i}$ may join into the set V_i when their nearest active neighbors become inactive. It is necessary to show that even with these influences, the process of reduction on each class V_i for $i \in \{0, 1, 2, ... \log \frac{\epsilon}{2} R - 1\}$ is still correct and efficient.

We define a series of vectors $\{m_i(t) : t \ge 0 \ and \ 0 \le i \le \log \frac{\epsilon}{2} R - 1\}$ shown below to help analyze the reduction process on each V_i.

$$\forall t \ge 0 : m_i(t) = \begin{cases} n/\gamma_1 & t \le T_i \\ \lfloor m_i(t-1) * \gamma_2 \rfloor & t > T_i \end{cases}$$

Here, $\gamma_1 = 1 - \gamma$ and $\gamma_2 = \gamma_1 + \rho/(1-\rho)$, where ρ is a sufficiently small constant which satisfies the following analysis; and $T_i = i * h$ and $h = \lceil \log_{\gamma_2} \rho \rceil$.

Mathematically, when $\hat{T} \in O(\log n + \log R)$, $\forall 0 \le i \le \log \frac{\epsilon}{2} R - 1$, we have $m_i(\hat{T}) = 0$. Define random events $\mathcal{E}(j)$s for $j \ge 0$: $\mathcal{E}(j)$ occurs when $n_i(r) \le m_i(j)$ for all $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2} R - 1\}$ at some round r. Then, $\mathcal{E}(0)$ always occurs and when $\mathcal{E}(\hat{T})$ occurs, $n_i = 0$ for

$i \in \{0, 1, \ldots, \log \frac{\epsilon}{2} R - 1\}$. We next consider when $\mathcal{E}(\hat{T})$ occurs.

We construct a twin vector $\hat{m}_i(t)$ for $m_i(t)$ with $\hat{m}_i(t) = \frac{\gamma_1}{\gamma_2} m_i(t)$, and construct a sufficient condition for $\mathcal{E}(j+1)$ to occur when $\mathcal{E}(j)$ has occurred.

Lemma 5. When $\mathcal{E}(j)$ occurs, and $n_i(r) \le \hat{m}_i(j+1)$ at some round r, then $n_i(r+1) \le m_i(j+1)$.

Proof. If the network is jammed at round r, no transmission can succeed. Thus, the states of the nodes in the network do not change between r and $r+1$, i.e. $n_i(r+1) = n_i(r) \le \hat{m}_i(j+1) \le m_i(j+1)$. In the situation when the network is not jammed on round r, we prove this lemma by considering two cases. Case 1: when $m_i(j) = n/\gamma_1$, we have $n_i(r+1) \le n < m_i(j+1) \le \frac{\gamma_2}{\gamma_1} n$; case 2: when $m_i(j) < n/\gamma_1$, considering that $\mathcal{E}(j)$ occurs and $n_i(r) \le m_i(j)$ for $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2} R - 1\}$, we get

$$\begin{aligned} n_i(r+1) &\le n_i(r) + \sum_{s=0}^{i-1} n_s(r) \le \hat{m}_i(j+1) + \sum_{s=0}^{i-1} m_s(j) \\ &\le m_i(j)\gamma_2 - m_i(j)\rho/(1-\rho) + m_i(j)\rho/(1-\rho) \\ &= m_i(j+1) \end{aligned}$$

So no matter whether the network is jammed or not, the lemma holds. □

Lemma 6. If $\mathcal{E}(j)$ occurs at an un-jammed round r, then with probability at least $1 - e^{-\Omega(n_i(r))}$, we have $n_i(r+1) < m_i(j+1)$, where $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2} R - 1\}$.

Proof. Obviously, when $m_i(j) = n/\gamma_1$, $\hat{m}_i(j+1) = n$, the lemma can be directly proved; and when $n_i(r) < \hat{m}_i(j+1)$, the lemma can be proved by Lemma 5. We next consider the last case when $n_i(r) \ge \hat{m}_i(j+1)$ and $m_i(j) < n/\gamma_1$.

Because $\mathcal{E}(j)$ occurs and $m_i(j) < n/\gamma_1$, we get

$$\begin{aligned} n_{<i}(r) &\le m_{<i}(j) \le \frac{\rho m_i(j)}{1-\rho} \le \frac{\rho \hat{m}_i(j+1)}{\gamma_1(1-\rho)} \\ &\le \frac{\rho n_i(r)}{\gamma_1(1-\rho)} \le \frac{1-(2^{1-\alpha/2})}{2} * n_i(r) \end{aligned}$$

The last inequality is satisfied by setting the constant ρ to be small enough to guarantee that $\frac{\rho}{\gamma_1(1-\rho)} \le \frac{1-(2^{1-\alpha/2})}{2}$. We obtain $n_{<i}(r) < \frac{1-(2^{1-\alpha/2})}{2} n_i(r)$ from the above inequality. Then, in the un-jammed round r, by Lemma 4, with probability $1 - e^{-\Omega(n_i(r))}$, we have

$$\begin{aligned} n_i(r+1) &\le \gamma_1 n_i(r) + \sum_{s=0}^{i-1} n_s(r) \le \gamma_1 m_i(j) + \sum_{s=0}^{i-1} m_s(j) \\ &= \hat{m}_i(j+1) + \sum_{s=0}^{i-1} m_s(j) \le m_i(j+1) \end{aligned}$$

□

The next step is to bound the number of un-jammed rounds used for $\mathcal{E}(j+1)$ to occur when $\mathcal{E}(j)$ has already occurred. Let $c_1 = \max\{\frac{2\gamma_1/\gamma_2}{a_1(1-\gamma_2)}, 2\gamma_1/\gamma_2\}$, a_1 is the constant behind the Ω notation in the probability guarantee in Lemma 6.

Lemma 7. After $\mathscr{T}(c_1)$ rounds after $\mathcal{E}(j)$ occurs, $\mathcal{E}(j+1)$ occurs with probability at least $1/2$.

Proof. In a carefully designed protocol, nodes in jammed rounds do not change their states and the values of the parameters. Thus we only need to consider the un-jammed rounds in $\mathscr{T}(c_1)$. For $i \in \{0, 1, \ldots, \log \frac{\epsilon}{2} R - 1\}$, when $m_i(j) = 0$ or $n_i = 0$, it is easy to get that $n_i \le m_i(j) \le m_i(j+1)$. For the case when $m_i(j) \ge n_i > 0$, the probability that n_i is larger than $m_i(j+1)$ after $\mathscr{T}(c_1)$ rounds is

$$\begin{aligned} e^{-2\gamma_1 n_i/(\gamma_2(1-\gamma_2))} &\le \gamma_2(1-\gamma_2)/(2\gamma_1 n_i) \\ &\le \gamma_2(1-\gamma_2)/(2\gamma_1 \hat{m}_i(j+1)) \\ &\le (1-\gamma_2)/(2m_i(j+1)). \end{aligned}$$

Take a union bound on the above error probabilities for all is, the probability that at least one n_i larger than $m_i(j+1)$ after $\mathscr{T}(c_1)$ rounds is at most

$$\sum_{i=0}^{\log \frac{\epsilon}{2} R - 1} (1-\gamma_2)/(2m_i(j+1)) \le \frac{1-\gamma_2}{2} \sum_{i=0}^{+\infty} \gamma_2^i \le \frac{1}{2}$$

Hence, with probability at least $1/2$, $\mathcal{E}(j+1)$ occurs $\mathscr{T}(c_1)$ rounds later when $\mathcal{E}(j)$ occurs , which completes the proof. □

Note that $\mathcal{E}(0)$ always occurs. Taking a Chernoff bound, one can see that $\mathcal{E}(\hat{T})$ occurs within $\mathscr{T}(c_1 * (\log n + \log R))$ rounds with high probability. By setting the constant k to be sufficiently larger than c_1, one can see that at the final un-jammed round t of $\mathfrak{P}_1$, $\mathcal{E}(\hat{T})$ occurs w.h.p.. Thus, only one node v in $\mathbb{A}$ is left at cell g in round t. And because of receiving the source message in the first $c * c$ slots for $k * (\log n + \log R)$ rounds, v changes to state $\mathbb{B}$ at the end of round t. Thus, we complete the proof for Lemma 2.

6 Simulation Results

In this section, we investigate the empirical performances of our message dissemination algorithm. Specifically, we focus on (i) the average time used for one-hop message dissemination, and (ii) the total amount of time used for message dissemination, where the number of nodes in the network is n, the diameter is D, and the jamming patterns vary.

Jamming patterns. Similar with the simulation settings in [48], two types of jamming patterns, called Regular Jamming (REGJ) and Bursty jamming (BURJ), are adopted in our simulation study. In REGJ, an adversary has a constant probability $\zeta \in [0, 1)$ to jam the network at each round. In BURJ, an adversary jams the network at round t with the probability $p_t = T_\zeta * \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(t-T_\zeta)^2}{2\sigma^2}}$. In other words, $\frac{p_t}{T_\zeta} \sim N(T_\zeta, \sigma^2)$. Due to the properties of *Normal distribution*, there are about T_ζ jamming rounds occured in our simulation, and the distribution of jamming rounds follows a normal distribution with the mean T_ζ. Figure 3 illustrates the jamming probabilities of several nomral distributions adopted in our simulation. Obviously, the jamming parameters ζ in REGJ and T_ζ in BURJ reflect the jamming levels in the network, i.e., the larger the ζ or the T_ζ, the heavier the jamming in the network.

Parameters. Basically, n nodes including the source node s are randomly and uniformly distributed into a network area of $150m \times 150m$, $200m \times 200m$, $250m \times 250m$, or

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2021.3108004, IEEE Transactions on Mobile Computing

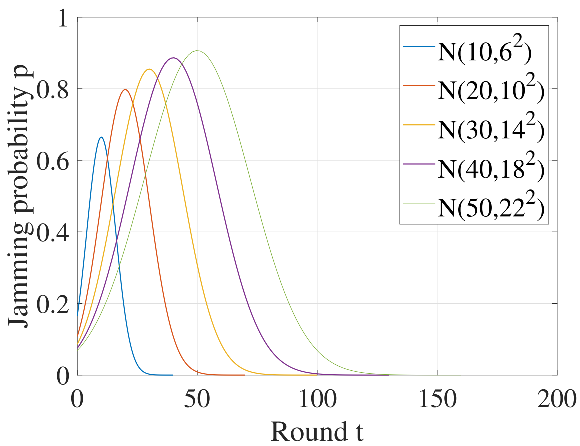


Fig. 3: Normal distribution in the BURJ

TABLE 1: Parameters in simulation

Parameter	Value	Parameter	Value
n	$[1000, 10000]$	R	30m
α	3	β	1.5
P_{min}	$R^\alpha\beta$	P_{max}	$4R^\alpha\beta$
ϵ	1.0	N	$\frac{P_{min}}{(1+\epsilon)^\alpha R^\alpha \beta}$
p	0.2	c	10
ζ	$\{0, 1, 3, 5, 7, 9\} * 10^{-1}$		
T_ζ	$\{0, 1, 2, 3, 4, 5\} * 10$		

$300m \times 300m$. Each node randomly selects a transmission power between P_{min} and P_{max}, and has a constant transmission probability p. Table 1 summarizes the parameters used in our simulation. Such kind of settings on parameters makes sure that our simulation is comprehensive enough to cover a large fraction of scenarios in reality. For example, $n \in [1000, 10000]$, network size varying from $150m \times 150m$ to $300m \times 300m$, and $R = 30m$ makes sure that the density of nodes in network varies from $\frac{1}{90}/m^2$ to $\frac{4}{9}/m^2$, and the number of nodes around a node v within distance R varies from 10π to 400π. Thus, our network topologies in simulation are comprehensive enough to simulate a series of network topologies in reality, from a sparse network to a super dense network. Over 20 runs of the simulation have been carried out for each reported result. All experiments are conducted on a Linux machine with Intel Xeon CPU E5-2670@2.60GHz and 64 GB main memory, implemented in C++ and compiled by g++ compiler.

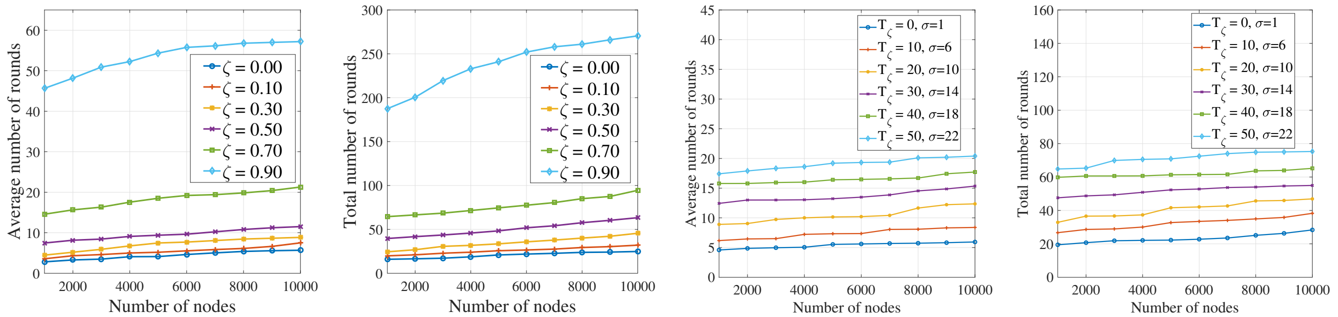
6.1 Algorithm Performance

In our simulations, all the nodes are randomly distributed into the network area. As the algorithm executes, for any path $\mathcal{P}_{s\to s'} = \{s \to s_1 \to ...s_{l-1} \to s'\}$ starting from source node s and ending at node s', the message is disseminated from s to s' hop by hop. The rounds from the moment when s_i receives the source message to the moment when s_{i+1} receives the source message is regarded as the time for one-hop message dissemination, where $i = 1, 2, ...$ We take an average on the time for the one-hop message dissemination and also record the total time used for message dissemination when parameters change, as is illustrated in Fig 4, in which the x-axes represent the number of nodes in the network and the y-axes represent the average number of rounds for one-hop message dissemination or the total number of rounds for message dissemination from s to s'. Fig 4 (a1)-(a4) shows the average number of rounds for one-hop message dissemination or the total number of rounds for message dissemination with REGJ or BURJ in a network of size $150m * 150m$; and (b1)-(b4), (c1)-(c4), and (d1)-(d4) show the corresponding results in networks with size of $200m * 200m$, $250m * 250m$, and $300m * 300m$, respectively.

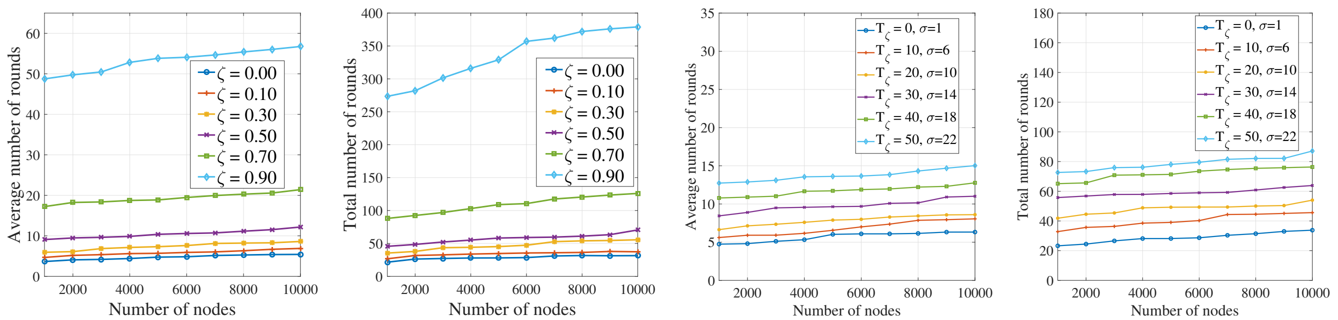
We focus on the results in Fig 4 a(1)-a(4) first. It can be seen that the average number of rounds for one-hop message dissemination in (a1) increases when n gets larger for any fixed jamming ratio ζ, which verifies that our algorithm requires $O(\log n + \log R)$ unjammed rounds to disseminate the message for one hop. Comparisons between the average number of rounds on different jamming ratios ζ indicate the jamming resilience of our algorithm. Specifically, the results in $\zeta = 0.0$ reflect the average number of rounds our algorithm requires in an unjammed situation. In the case of $\zeta = 0$ and $n = 10000$, an average of 5.67 unjammed rounds are required to disseminate the message by one hop. And in the case of $\zeta = 0.9$ and $n = 10000$, the number of required rounds is 57.18, containing $57.18*(1-0.9) = 5.718$ unjammed rounds in expectation, which is almost the same with the case of $\zeta = 0$, $n = 10000$ with respect to the number of unjammed rounds. Therefore one can claim that our algorithm is insensitive to jamming in the sense that the requirement of unjammed rounds in our algorithm is rarely affected by a particular jamming in the network. The total number of rounds for message dissemination in (a2) has a similar tendency with the average results in (a1). Also from (a2), one can see that for a network connected within distance of $30m$ and with size of $150m * 150m$, it requires no more than 30 unjammed rounds to finish the message dissemination regardless of the jamming level in the network. (a3) and (a4) show the average number of rounds for one-hop message dissemination and the total number of rounds for message dissemination in the BURJ pattern. One can see that our algorithm has a better performance under BURJ since the corresponding results in (a3) and (a4) are smaller than those in (a1) and (a2). Also, one can draw the same conclusions from (a3) and (a4) as what we got from (a1) and (a2), even through the jamming patterns vary, which indicates the jamming resilience of our algorithm when facing different jamming patterns.

Comparing the results among (a1)-(a4), (b1)-(b4), (c1)-(c4), and (d1)-(d4), one can also conclude that (i) the average number of rounds for message dissemination is not influenced by the network size and (ii) the total number of rounds for message dissemination increases when the size of the network gets larger.

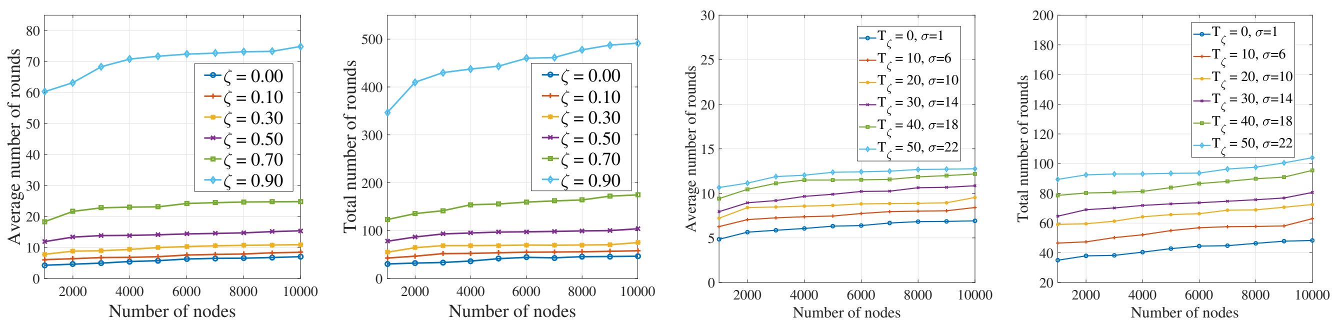
Comparison with existing works. By adopting the anti-jamming schemes in [30], [26] to solve the message dissemination problem, We show the comparison between our algorithm and the existing works. In Figure 5, The anti-jamming algorithms from [30], [26], and our work are termed as Algorithm 1, Algorithm 2, and Algorithm 3, respectively. In (a1)-(a4), we present the total number of rounds taken by Algorithm 1, 2 and 3 on MD with different jamming levels in REGJ or BURJ in networks of size $200m * 200m$. (b1)-(b4) present the corresponding results in networks of size $300m * 300m$. Let t_1, t_2, and t_3 be the time taken by Algorithm 1, 2, 3 to accomplish the message dissemination,



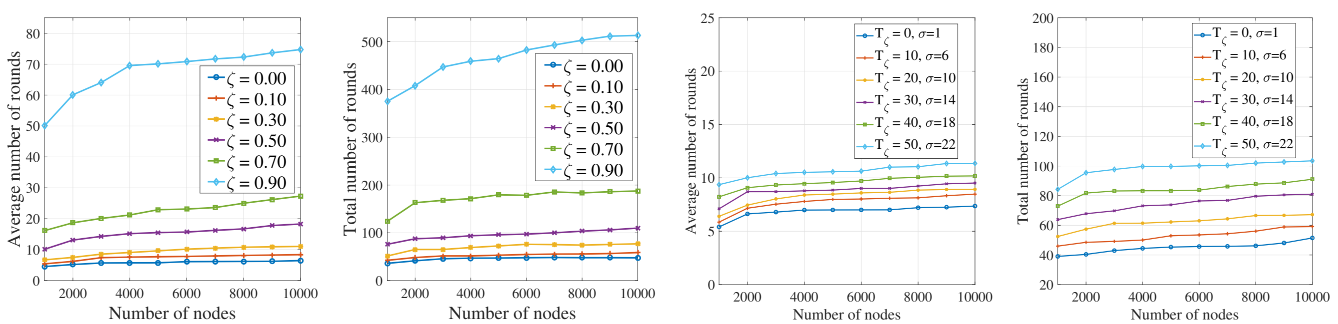
(a1). AVG number of rounds for one-hop MD with REGJ in a $150m * 150m$ network
(a2). Total number of rounds for MD with REGJ in a $150m * 150m$ network
(a3). AVG number of rounds for one-hop MD with BURJ in a $150m * 150m$ network
(a4). Total number of rounds for MD with BURJ in a $150m * 150m$ network



(b1). AVG number of rounds for one-hop MD with REGJ in a $200m * 200m$ network
(b2). Total number of rounds for MD with REGJ in a $200m * 200m$ network
(b3). AVG number of rounds for one-hop MD with BURJ in a $200m * 200m$ network
(b4). Total number of rounds for MD with BURJ in a $200m * 200m$ network

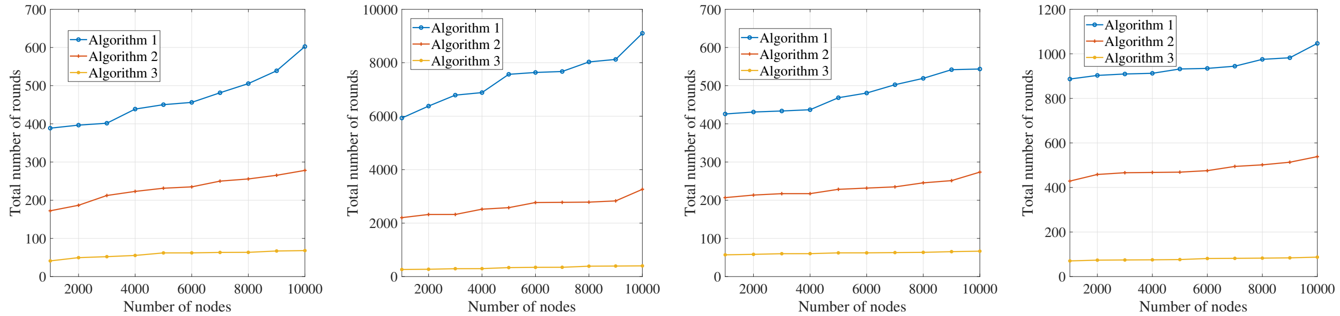


(c1). AVG number of rounds for one-hop MD with REGJ in a $250m * 250m$ network
(c2). Total number of rounds for MD with REGJ in a $250m * 250m$ network
(c3). AVG number of rounds for one-hop MD with BURJ in a $250m * 250m$ network
(c4). Total number of rounds for MD with BURJ in a $250m * 250m$ network

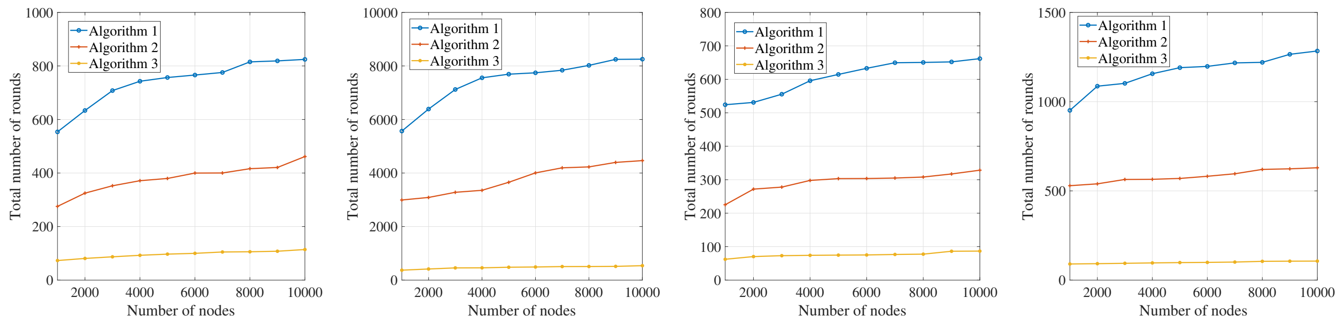


(d1). AVG number of rounds for one-hop MD with REGJ in a $300m * 300m$ network
(d2). Total number of rounds for MD with REGJ in a $300m * 300m$ network
(d3). AVG number of rounds for one-hop MD with BURJ in a $300m * 300m$ network
(d4). Total number of rounds for MD with BURJ in a $300m * 300m$ network

Fig. 4: Performance evaluation. "Average" and "message dissemination" are written as AVG and MD for short. In (a1)-(a4), we present the average numbers of rounds for one-hop MD and the total number of rounds for MD with REGJ or BURJ in networks of size $150m * 150m$. (b1)-(b4), (c1)-(c4), (d1)-(d4) present the corresponding results in networks of size $200m * 200m$, $250m * 250m$, $300m * 300m$, respectively.



(a1). Total number of rounds for MD with $\zeta = 0.50$ in REGJ in a $200m * 200m$ network
(a2). Total number of rounds for MD with $\zeta = 0.90$ in REGJ in a $200m * 200m$ network
(a3). Total number of rounds for MD with $T_\zeta = 30$ in BURJ in a $200m * 200m$ network
(a4). Total number of rounds for MD with $T_\zeta = 50$ in BURJ in a $200m * 200m$ network



(b1). Total number of rounds for MD with $\zeta = 0.50$ in REGJ in a $300m * 300m$ network
(b2). Total number of rounds for MD with $\zeta = 0.90$ in REGJ in a $300m * 300m$ network
(b3). Total number of rounds for MD with $T_\zeta = 30$ in BURJ in a $300m * 300m$ network
(b4). Total number of rounds for MD with $T_\zeta = 50$ in BURJ in a $300m * 300m$ network

Fig. 5: Performance evaluation. "Message dissemination" is written as MD for short. The anti-jamming algorihtms from [30], [26], and our work are termed as Algorithm 1, Algorithm 2, and Algorithm 3, respectively. In (a1)-(a4), we present the total number of rounds taken by Algorihtm 1, 2 and 3 on MD with different jamming levels in REGJ or BURJ in networks of size $200m * 200m$. (b1)-(b4) present the corresponding results in networks of size $300m * 300m$.

TABLE 2: Comparison between Algorithm 1, 2, and 3.

$200m \times 200m$	REGJ		BURJ	
	$\zeta = 0.5$	$\zeta = 0.9$	$T_{\zeta=30}$	$T_{\zeta=30}$
$t1/t3 \approx$	7.8	15.7	8.1	12.1
$t2/t3 \approx$	4.2	8.0	4.1	5.9
$300m \times 300m$	REGJ		BURJ	
	$\zeta = 0.5$	$\zeta = 0.9$	$T_{\zeta=30}$	$T_{\zeta=30}$
$t1/t3 \approx$	8.1	16.3	8.2	11.8
$t2/t3 \approx$	4.1	8.1	3.9	6.0

respectively. Table 2 shows the comparison of our algorihm with algorithms 1 and 2 under different jamming scenarios. Combining Figure 5 and Table 2, the following points can be concluded: (I) When the jamming level, number of nodes, diameter of the netwrok get larger, the running time of all three algorithms increase; (II) Our algorithm has a better performance than algorithms 1 and 2 on running time, especially when the jamming is network is heavy. For example, when $\zeta = 0.5$ in REGJ, our algorithm is about 7 times and 3 times faster then algorithm 1 and 2, respectively. Meanwhile, when the jamming in network becomes heavier, i.e. $\zeta = 0.9$ in REGJ, our algorithm is about 15 times and 7 times faster then algorithms 1 and 2, respectively.

6.2 Summary

In conclusion, our algorithm is verified to be jamming resilient by the above simulation results. The number of unjammed rounds needed for message dissemination is almost uninfluenced by a particular jamming in the network. Additionally, our algorithm uses $O(D(\log n + \log R))$ unjammed rounds to complete the message dissemination. The simulation results indicate that the constant hidden behind the big O notation is not larger than 10.

7 Conclusion

In this paper, we consider the message dissemination primitive in wireless networks with unreliable multiple access channels and non-spontaneous wakeup nodes. Based on SINR, we consider a strong jamming model to remove the energy budget constraint on an adversary, which is adopted in almost all previous work, and thus the adversary in our model can jam the shared channel in any round at will. Obviously, the adopted strong adversarial jamming model is much more comprehensive and realistic than most of those in previous work. Under such a jamming model, we present a distributed and randomized message dissemination algorithm with time complexity of $\mathscr{T}(O(D(\log n + \log R)))$ whose performance is guaranteed with a high probability. This makes our message dissemination algorithm almost asymptotically optimal in terms of time complexity.

8 Acknowledgement

This work is partially supported by the National Key Research and Development Program of China under Grant

2019YFB2102600, the National Natural Science Foundation of China (NSFC) under Grant 6210070740, 61971269, 61832012.

REFERENCES

[1] G. Alnifie and R. Simon. A multi-channel defense against jamming attacks in wireless sensor networks. In *Q2SWinet*, 2007.

[2] B. Awerbuch, A. Richa, and C. Scheideler. A jamming-resistant mac protocol for single-hop wireless networks. In *PODC*, 2008.

[3] R. Bar-Yehuda, O. Goldreich, and A. Itai. On the Time-Complexity of Broadcast in Multi-hop Radio Networks: An Exponential Gap Between Determinism and Randomization. In *J. Comput. Syst. Sci.*, 45(1): 104-126, 1992.

[4] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, B. Thapa. On the performance of IEEE 802.11 under jamming. In *INFOCOM*, 2008.

[5] Z. Cai, Q. Chen. Latency-and-Coverage Aware Data Aggregation Scheduling for Multihop Battery-Free Wireless Networks, in *IEEE Trans. Wirel. Commun.*, 20(3): 1770-1784, 2021.

[6] Z. Cai and T. Shi. Distributed Query Processing in the Edge Assisted IoT Data Monitoring System, in *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3026988.

[7] Q. Chen, Z. Cai, L. Cheng and H. Gao. Structure-Free General Data Aggregation Scheduling for Multihop Battery-Free Wireless Networks, in *IEEE Trans. Mob. Comput.*, doi: 10.1109/TMC.2021.3053557.

[8] H. Chen, C. Zheng. Fast and Resource Competitive Broadcast in Multi-channel Radio Networks, in *SPAA*, 2019.

[9] H. Chen, C. Zheng. Brief Announcement: Resource Competitive Broadcast against Adaptive Adversary in Multi-channel Radio Networks, in *PODC*, 2020.

[10] X. Cheng, A. Thaeler, G. Xue, and D. Chen, TPS: a time-based positioning scheme for outdoor sensor networks, in *IEEE INFOCOM*, Vol. 4, pp.2685-2696, March 7-11, 2004.

[11] J. Chiang, Y.-C. Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In *MobiCom*, 2007.

[12] A. Czumaj, and W. Rytter. Broadcasting Algorithms in Radio Networks with Unknown Topology. In *FOCS*, 2003.

[13] S. Daum, S. Gilbert, F. Kuhn, and C.C. Newport. Broadcast in the Ad Hoc SINR Model. In *DISC*, 2013.

[14] M. Ghaffari, B. Haeupler, and M. Khabbazian. Randomized broadcast in radio networks with collision detection. In *PODC*, 2013.

[15] K. Han, J. Luo, L. Xiang, M. Xiao, L. Huang. Achieving Energy Efficiency and Reliability for Data Dissemination in Duty-Cycled WSNs, in *IEEE/ACM Trans. Netw.*, 23(4): 1041-1052, 2015.

[16] T. Jurdzinski, D.R. Kowalski, M. Rozanski, and G. Stachowiak. On the impact of geometry on ad hoc communication in wireless networks. In *PODC*, 2014.

[17] T. Jurdzinski, D.R. Kowalski, and G. Stachowiak. Distributed Deterministic Broadcasting in Uniform-Power Ad Hoc Wireless Networks. In *FCT*, 2013.

[18] T. Jurdzinski, D.R. Kowalski, and G. Stachowiak. Distributed Deterministic Broadcasting in Wireless Networks of Weak Devices. In *ICALP*, 2013.

[19] D.R. Kowalski and A. Pelc. Deterministic broadcasting time in radio networks of unknown topology. In *FOCS*, 2002.

[20] D.R. Kowalski and A. Pelc. Broadcasting in undirected ad hoc radio networks. In *Distributed Computing*, 18(1): 43-57, 2005.

[21] X. Liu, G. Noubir, R. Sundaram, and S. Tan. Spread: Foiling smart jammers using multi-layer agility. In *INFOCOM*, 2007.

[22] J. Luo, Y. He. GeoQuorum: Load balancing and energy efficient data access in wireless sensor networks, in *INFOCOM*, 2011.

[23] J. Luo, A. Iyer, C. Rosenberg. Throughput-Lifetime Trade-Offs in Multihop Wireless Networks under an SINR-Based Interference Model, in *IEEE Trans. Mob. Comput.*, 10(3): 419-433, 2011.

[24] J. Luo, C. Rosenberg and A. Girard. Engineering Wireless Mesh Networks. Joint Scheduling, Routing, Power Control, and Rate Adaptation, in *IEEE/ACM Trans. Netw.*, 18(5): 1387-1400, 2010.

[25] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein. Using channel hopping to increase 802.11 resilience to jamming attacks. In *INFOCOM*, 2007.

[26] A. Ogierman, A.W. Richa, C. Scheideler, S. Schmid, J. Zhang. Competitive MAC under adversarial SINR. In *INFOCOM* 2014.

[27] A. Ogierman, A.W. Richa, C. Scheideler, S. Schmid, J. Zhang: Sade: competitive MAC under adversarial SINR. In *Distributed Computing*, 31(3): 241-254, 2018.

[28] A. Pelc and D. Peleg. Feasibility and complexity of broadcasting with random transmission failures. In *PODC*, 2005.

[29] A. Richa, C. Scheideler, S. Schmid, J. Zhang. A jamming-resistant mac protocol for multi-hop wireless networks. In *DISC*, 2010.

[30] A. Richa, C. Scheideler, S. Schmid, J. Zhang. Competitive and fair medium access despite reactive jamming. In *ICDCS*, 2011.

[31] A. Richa, C. Scheideler, S. Schmid, J. Zhang. Self-stabilizing leader election for single-hop wireless networks despite jamming. In *MobiHoc*, 2011.

[32] A. Richa, C. Scheideler, S. Schmid, J. Zhang. Competitive throughput in multi-hop wireless networks despite adaptive jamming. In *Distributed Computing* 26(3): 159-171, 2013.

[33] M.K. Simon, J.K. Omura, R.A. Schultz, and B.K. Levin. Spread Spectrum Communications Handbook. In *McGraw-Hill*, 2001.

[34] X. Tian, J. Yu, L. Ma, G. Li, and X. Cheng. Distributed deterministic broadcasting algorithms under the SINR model. In *INFOCOM*, 2016.

[35] L. Xiang, J. Luo, C. Rosenberg. Compressed Data Aggregation: Energy-Efficient and High-Fidelity Data Collection, in *IEEE/ACM Trans. Netw.*, 21(6): 1722-1735, 2013.

[36] A. Wood, J. Stankovic, and G. Zhou. DEEJAM: Defeating energyefficient jamming in IEEE 802.15.4-based wireless networks. In *SECON*, 2007.

[37] W. Xu, T. Wood, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Workshop on Wireless Security*, 2004.

[38] D. Yu, Q. Hua, Y. Wang, F. C. M. Lau. An O(log n) Distributed Approximation Algorithm for Local Broadcasting in Unstructured Wireless Networks, in *DCOSS* 2012.

[39] D. Yu, Q. Hua, Y. Wang, H. Tan, and F. C. M. Lau. Distributed multiple-message broadcast in wireless ad hoc networks under the SINR model. In *Theor. Comput. Sci.*, 610: 182-191, 2016.

[40] D. Yu, L. Ning, Y. Zou, J. Yu, X. Cheng and F. C. M. Lau. Distributed Spanner Construction With Physical Interference: Constant Stretch and Linear Sparseness, in *IEEE/ACM Trans. Netw.*, 25(4): 2138-2151, 2017.

[41] D. Yu, Y. Zou, Y. Wang, J. Yu, X. Cheng and F. C. M. Lau. Implementing The Abstract MAC Layer via Inductive Coloring Under the Rayleigh-fading Model, in *IEEE Trans. Wirel. Commun.*, doi: 10.1109/TWC.2021.3072236.

[42] D. Yu, Y. Zou, M. Xu, Y. Xu, Y. Zhang, B. Gong, X. Xing. Competitive Age of Information in Dynamic IoT Networks, in *IEEE Internet Things J.*, doi: 10.1109/JIOT.2020.3038595.

[43] D. Yu, Y. Zou, J. Yu, X. Cheng, Q. Hua, H. Jin, F. C. M. Lau. Stable Local Broadcast in Multihop Wireless Networks Under SINR, in *IEEE/ACM Trans. Netw.*, 26(3): 1278-1291, 2018.

[44] D. Yu, Y. Zou, J. Yu, Y. Zhang, F. Li, X. Cheng, F. Dressler, F. C. M. Lau. Implementing The Abstract MAC Layer in Dynamic Networks, in *IEEE Trans. Mob. Comput.* 20(5): 1832-1845, 2021.

[45] D. Yu, Y. Zou, Y. Zhang, F. Li, J. Yu, Y. Wu, X. Cheng, F. C. M. Lau. Distributed Dominating Set and Connected Dominating Set Construction Under the Dynamic SINR Model, in *IPDPS*, 2019.

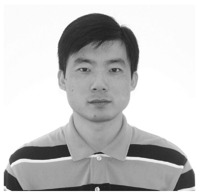
[46] D. Yu, Y. Zou, Y. Zhang, H. Sheng, W. Lv and X. Cheng. An Exact Implementation of the Abstract MAC Layer via Carrier Sensing in Dynamic Networks, in *IEEE/ACM Trans. Netw.*, doi: 10.1109/TNET.2021.3057890.

[47] Y. Zou, M. Xu, H. Sheng, X. Xing, Y. Xu, Y. Zhang. Crowd Density Computation and Diffusion via Internet of Things, in *IEEE Internet Things J.*, 7(9): 8111-8121, 2020.

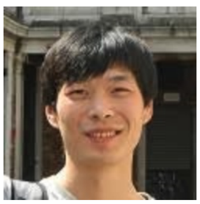
[48] Y. Zou, D. Yu, L. Wu, J. Yu, Y. Wu, Q. Hua, F.C.M. Lau. Fast Distributed Backbone Construction Despite Strong Adversarial Jamming, in *INFOCOM*, 2019.

[49] Y. Zou, D. Yu, J. Yu, Y. Zhang, F. Dressler and X. Cheng. Distributed Byzantine-Resilient Multiple-Message Dissemination in Wireless Networks, in *IEEE/ACM Trans. Netw.*, doi: 10.1109/TNET.2021.3069324.

Yifei Zou received the B.E. degree in 2016 from Computer School, Wuhan University, and the PhD degree in 2020 from the Department of Computer Science, The University of Hong Kong. He is currently an Assistant Professor with the school of computer science and technology, Shandong University. His research interests include wireless networks, ad hoc networks and distributed computing.

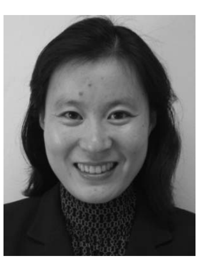


Dongxiao Yu received the BSc degree in 2006 from the School of Mathematics, Shandong University and the PhD degree in 2014 from the Department of Computer Science, The University of Hong Kong. He became an associate professor in the School of Computer Science and Technology, Huazhong University of Science and Technology, in 2016. He is currently a professor in the School of Computer Science and Technology, Shandong University. His research interests include wireless networks, distributed computing and graph algorithms.



Pengfei Hu is a professor in the School of Computer Science and Technology at Shandong University. Before joining Shandong University, he was a researcher with VMWare xLab. He received the Ph.D. in Computer Science from the University of California, Davis (US). His PhD supervisor is Prof. Prasant Mohapatra. His research interests are in the areas of cyber security, data privacy, mobile computing. He has published more than 20 papers in reputed conferences and journals on these topics, including: IEEE communications Surveys & Tutorials, TMC, TDSC, INFOCOM, CoNEXT, SECON, MILCOM, etc. Dr. Hu also holds 5 patents in the area of mobile computing. He served as reviewer for numerous journals and conferences including TIFS, JSAC, TMC, TWC, SECON, CNS, WCNC, MILCOM, etc.

Jiguo Yu received his Ph.D. degree in School of mathematics from Shandong University in 2004. He became a full professor in the School of Computer Science, Qufu Normal University, Shandong, China in 2007. Currently he is a full professor in Qilu University of Technology (Shandong Academy of Sciences), and Shandong Computer Science Center (National Supercomputer Center in Jinan). His main research interests include privacy-aware computing, wireless networking, distributed algorithms, peer-to-peer computing, and graph theory. Particularly, he is interested in designing and analyzing algorithms for many computationally hard problems in networks. He is a senior member of IEEE, a member of ACM and a senior member of the CCF (China Computer Federation).



Xiuzhen Cheng received her M.S. and Ph.D. degrees in computer science from the University of Minnesota – Twin Cities in 2000 and 2002, respectively. She is a professor in the School of Computer Science and Technology, Shandong University. Her current research interests include cyber physical systems, wireless and mobile computing, sensor networking, wireless and mobile security, and algorithm design and analysis. She has served on the editorial boards of several technical journals and the technical program committees of various professional conferences/workshops. She also has chaired several international conferences. She worked as a program director for the US National Science Foundation (NSF) from April to October in 2006 (full time), and from April 2008 to May 2010 (part time). She received the NSF CAREER Award in 2004. She is Fellow of IEEE and a member of ACM.

Prasant Mohapatra is a professor with the Department of Computer Science and is serving as the Vice Chancellor for Research at University of California, Davis. His research interests are in the areas of wireless networks, mobile communications, cybersecurity, and Internet protocols. He has published more than 350 papers in reputed conferences and journals on these topics. He was the editor-in-chief of the IEEE Transactions on Mobile Computing. He has served on the editorial boards of the IEEE Transactions on Computers, the IEEE Transactions on Mobile Computing, the IEEE Transaction on Parallel and Distributed Systems, the ACM Journal on Wireless Networks, and Ad Hoc Networks. He is a fellow of the IEEE and a fellow of the AAAS.