This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Jamming-Resistant Collaborative Broadcast In Wireless Networks, Part II: Multihop Networks

Liang Xiao
Xiamen University, China 361005
Email: lxiao@xmu.edu.cn

Huaiyu Dai
NC State University, Raleigh, NC 27695
Email: huaiyu_dai@ncsu.edu

Peng Ning
NC State University, Raleigh, NC 27695
Email: pning@ncsu.edu

***Abstract*—We propose in [1] a collaborative broadcast scheme for wireless networks, which applies the Uncoordinated Frequency Hopping (UFH) technique to counteract jamming and exploits node cooperation to enhance broadcast efficiency. In this scheme, some nodes that already obtain the broadcast message are selected to relay the message to other nodes. In this paper, we extend the study to the generalized multihop network scenarios, and provide solutions for important related issues, such as the relay node selection, multiple access control, relay channel selection and packet scheduling. We also study the spatial and frequency (channel) diversity provided by the collaborative broadcast. Simulation results show that the collaborative broadcast achieves low broadcast delay, with low energy consumption and small computational overhead in multihop networks.**

I. Introduction

Jamming-resistant broadcast is important for many safety-critical applications such as emergency alert broadcast and navigation signal dissemination, and is critical for the distribution of important information such as the public key and system control information in wireless systems. As mentioned in Part I [1], anti-jamming communication without presharedkeys has been recognized recently [2]–[11], leading to a series of promising research efforts, including Uncoordinated FH (UFH) [5]–[8] techniques.

In UFH [5], a message is divided into multiple short packets, and each packet is transmitted over a randomly selected channel, independent of each other and only known to the sender. Such rapid channel switching over a large frequency range effectively thwarts the jamming attempts. On the down side, each packet has to be sent multiple times, due to the low rate of successful reception resulting from the uncoordinated channel selection between the sender and the legitimate receivers. To this end, a BMA scheme was proposed to improve the communication efficiency by combining erasure coding and one-way authenticator based on bilinear maps [6]. Some additional efficient packet verification methods were proposed in [8]. In [7], the USD-FH scheme was proposed to further improve the efficiency and robustness, where the hopping pattern is conveyed through UFH to allow message transmission through coordinated FH. Despite all these efforts, the UFH-based anti-jamming communications still need to improve the communication efficiency and are vulnerable to powerful responsive jammers [7].

To further enhance the communication efficiency, we propose a collaborative broadcast scheme to exploit the node cooperation for single-hop wireless networks [1]. As all nodes in the network expect the same message, it is natural and convenient to use a set of nodes that already receive the message to help broadcast it. We design two strategies for relay channel selection: Random Relay Channel selection (RRC) and Static Relay Channel selection (StRC). In RRC, each relay node randomly and independently selects one out of C channels for the transmission of each packet. For the StRC strategy, the relays take *fixed* non-overlapping channels through the message broadcast process (for the transmission of all packets). For example, each relay may select a channel based on its (partial) ID (modulo some prime number and C) so that no overlapping is incurred. Both strategies are amenable to distributed implementation and have good scalability, as each relay node independently performs the strategy disregarding the other relay nodes.

In this paper, we extend our study to the multihop networks, where nodes that have successfully received the message serve as relays to help forward the broadcast message over multiple channels. In this way, both the source node and relay nodes send the message simultaneously at multiple channels over various geographical regions. Thus the receivers have larger opportunity to receive the message against jamming, compared to the broadcast without cooperation. In the multihop setting, besides spectral (channel) diversity, we can further explore spatial diversity to facilitate reliable message broadcast to a much wider geographic area. Unless the jammers are powerful enough to simultaneously block all the channels across the whole geographic area, which is not practical in most multihop radio networks, there is always a chance for the broadcast message to reach nodes outside the fully jammed region, which later relay the message to more nodes in the network.

Compared to [1], we consider a more general jamming model, where each jammer, no matter how powerful she is, can no longer jam all nodes as in the single-hop scenario. While it is sufficient to consider just one powerful jammer with combined jamming capability in the frequency domain in [1],

The work by Xiao is partly supported by NSFC (No.61001072), the Natural Science Foundation of Fujian Province of China (No.2010J01347), SRF for ROCS, SEM, and Tsinghua-Qualcomm research center. The work by Dai and Ning is supported by the US National Science Foundation under grants CNS-1016260 and by the US Army Research Office under grant W911NF-08-1-0105 managed by NCSU Secure Open Systems Initiative (SOSI). The contents of this paper do not necessarily reflect the position or the policies of the U.S. Government.

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

here we further introduce the concept of jamming radius and consider multiple jammers distributed in the area. In addition, we address the networking issues that are largely ignored in the single-hop case, including multiple access control, packet scheduling and determination of transmission duration, and provide a suite of solutions amenable to distributed implementation.

The remainder of the paper is organized as follows. We formulate the system model in Section II, and discuss some important issues for the collaborative broadcast in the multihop wireless networks in Section III. We present our collaborative broadcast protocols in Section IV, and evaluate their anti-jamming performance in Section V. Finally, we conclude in Section VI.

II. Problem Formulation

We consider anti-jamming broadcast in a multihop radio network, where the transmit power of the source node is not high enough to reach the whole network or it is too costly to do so. Suppose the source node located at the center of a disk area broadcasts a message to N identical randomly located nodes with disk radius R. All these nodes are assumed to employ a common communication range D. Thus it takes at least $\lceil R/D \rceil$ hops for the message to reach to the farthest node.

We suppose each node transmit (or receive) simultaneously across a set of c_m (or c_n) channels selected from C orthogonal channels, where C is typically a large number for strong jamming resistance. In this paper, we assume $c_m = c_n = 1$ for simplicity. Our results can be easily extended to the multi-channel cases. The broadcast message is divided into M short packets, each of which can be transmitted over one time slot (hop) with duration t_p.

Consider a common path-loss model [12], where the transmitted signal power for each node (including the source) satisfies $P_T = (D/R)^\gamma P_{MAX}$, with γ as the path loss exponent and P_{MAX} as the power required for the transmitted signal to successfully cover the whole disk area with radius R. For simplicity, we assume that the minimum energy for a node to transmit a packet E_t is proportional to P_T, neglecting the energy cost on the signal processing in the baseband and IF band, and that the minimum energy to receive a packet, E_r, is constant.

In our study, we consider the most powerful jamming [5], [6], responsive-sweep, where a jammer conducts both non-responsive and responsive jamming independently and simultaneously. The corresponding jamming probability for a single source (without relay) is given in [1] by

$$p_J = \frac{n_s C_s + n_J C_J}{C}. \quad (1)$$

The analysis based on the responsive-sweep jamming provides a lower bound for the broadcast performance, and most conclusions can be easily adapted for other jamming types.

We also consider a smart jamming for the StRC-based protocol, where each jammer knows the StRC relay channel selection strategy and the fixed relay channels in its communication region. It is in the interest of the smart jammer to first jam the fixed and known relay channels, instead of the remaining channels that carry out a packet with less probability. Note that this effort is solely limited by the physical jamming capability of the jammer (i.e., $n_J C_J$), while the sensing capability of the jammer does not help. If power supply permits, the smart jammer then continues to attack the non-relay channels using the responsive-sweep strategy, to prevent successful reception from the source. Clearly this mixed jamming strategy is even more powerful than the responsive-sweep jamming for the StRC-based cooperative broadcast.

Let P_J denote the jamming power, with corresponding jamming radius D_c, and $\rho = P_J/P_T = (D_c/D)^\gamma$ denote the normalized jamming power compared to a legitimate node. The notation summary is listed in Table I.

M	Number of packets consisted in the message to be sent
N	Number of nodes to receive the message
C	Number of channels in the system
R	Radius of the area of interests
D	Average coverage radius for each node
n	Node density ($= ND^2/R^2$)
P_T	Transmit power
Δ	Number of slots that each node transmits
p_a	Probability that a receiver successfully receives a packet
p	Channel accessing probability
J	Number of jammers
p_J	Probability for a channel to be jammed
C_J	Number of channels concurrently blocked by a jammer
C_s	Number of channels concurrently sensed by a jammer
n_J	Number of jamming cycles in a slot
n_s	Number of sensing cycles in a slot
D_c	Jamming radius
P_J	Jamming power
ρ	Normalized jamming power ($= P_J/P_T$)

TABLE I
Summary of notations.

III. Multihop Broadcast Strategies

We consider conveying a message consisting of M packets to N nodes through collaborative broadcast in a multihop wireless network, for both RRC and StRC strategies. Compared with the single-hop oriented work in [1], realizing collaborative broadcast incurs more challenges in the multihop setting. In this section, we discuss several important issues concerning multiple access control (MAC), packet scheduling, transmission duration control, and power control. Then in the following sections, we will introduce our broadcast protocols and evaluate their performance.

A. MAC

In the collaborative broadcast, the source node and relay nodes concurrently send packets over wireless media. Without appropriate MAC mechanism, this multiple access might result in transmission confliction, packet loss and energy waste, especially when ideal coordination is not available. In this work we consider the slotted Aloha scheme for the ease of distributed implementation, and investigate the optimal probability that a transmitter sends a packet to the radio media during a time slot, for both the RRC and StRC relay strategy.

Through our discussion, we assume a large C (greater than 100 as in a typical frequency hopping system) to provide strong jamming resistance. In addition, the largest number of one-hop neighboring nodes (Υ) is assumed to be less than C, which is reasonable for most typical wireless *ad hoc* networks. As to the coordination among the source and relay nodes, we consider two scenarios: synchronous and asynchronous. In the former case, all transmitting nodes in the neighborhood are perfectly synchronized both in time and in transmission content, so no interference is incurred when two more more relays select the same channel. The latter is more realistic, assuming that a collision occurs when two relays hop to the same channel (due to difference in arrival time or transmitted packets).

First, we consider the RRC strategy, where each transmitter randomly selects a channel and sends a packet on it with the access probability p.

Lemma 3.1: If $C > \Upsilon$, the successful packet reception rate of RRC is maximized by $p = 1$.

Proof: Assume that in the neighborhood of a receiver there are m relays, with $m \leq \Upsilon$, each transmitting with probability p on a randomly selected channel according to the RRC strategy. In the synchronous case, a receiver can successfully receive a packet if at least one of the m transmitters are working on its selected receiving channel and the channel is unblocked. The successful packet reception rate is given by

$$p_a^{RRC,syn} = \left(1 - \left(1 - p\frac{1}{C}\right)^m\right)(1 - p_J), \qquad (2)$$

which monotonically rises with p. As the access probability $p \in [0, 1]$, $p = 1$ maximizes $p_a^{RRC,syn}$.

In the asynchronous case, a receiver can successfully receive a packet if exactly one transmitter is accessing the receiving channel. Thus successful packet reception rate in the asynchronous case becomes

$$p_a^{RRC,asyn} = \frac{mp}{C}\left(1 - p\frac{1}{C}\right)^{m-1}(1 - p_J). \qquad (3)$$

Its derivative with respect to p is

$$\frac{\partial p_a^{RRC,asyn}}{\partial p} = \frac{m}{C}(1 - p_J)\left(1 - \frac{p}{C}\right)^{m-2}\left(1 - p\frac{m}{C}\right). \quad (4)$$

Hence $p = \min(C/m, 1)$ maximizes $p_a^{RRC,asyn}$, as $p \in [0, 1]$ and $C \gg 1$. Based on the assumption that $C > \Upsilon \geq m$, we have that $p = 1$ maximizes $p_a^{RRC,asyn}$. ■

Remark: By (2) and (3), both $p_a^{RRC,syn}$ and $p_a^{RRC,asyn}$ monotonically increase with m, which indicates that node cooperation helps reduce the average broadcast delay. Moreover, since C is usually a large number, the relative difference between $p_a^{RRC,syn}$ and $p_a^{RRC,asyn}$ is very small, implying the robustness of RRC against relay synchronization error.

Next, we consider the StRC strategy, where each relay selects a *fixed* non-overlapping channel according to its node ID while the source node still follows the UFH approach. As the known relay channels provide a much larger transmission probability than others, it is in the jammers' interest to first block them. Meanwhile, a smart receiver can also take advantage of these fixed relay channels unless all of them are jammed. Under such strong jamming, a receiver can then switch back to the whole C channels.

Hence in our scheme, each receiver first randomly selects one of these known relay channels. If it finds out that all the relay channels are jammed, it switches to the mode where it randomly selects one out of C channels. Once it comes across a clear relay channel, the receiver restricts itself to the relay channels again. The latter case happen as smart jammers may just spend enough energy to spoof the receivers away, instead of continuously jamming the static relay channels.

Lemma 3.2: The successful packet reception rate of StRC is maximized by $p = 1$.

The proof is similar to that to Lemma 3.1.

Note that the source node can only reach the first hop nodes, while the transmission to all the other nodes completely relies on the relay nodes. Under the cooperative broadcast, unless all the channels are simultaneously jammed across the whole area covered by the source node, some nodes in the first hop can receive the message with a large chance, and then send it to the other nodes. The above analysis can be easily adapted for the non-first-hop nodes.

B. Packet Scheduling

As the source and relay nodes cooperate to broadcast multiple packets of the broadcast message, it is necessary to determine when to start the transmission and what to send. We consider two strategies to decide the beginning of the relay mode: The first one is message-based, where each node starts relaying after successfully receiving all the M packets within the broadcast message. The second one is packet-based, where each node relays a packet right after receiving it, during the next time slots assigned to send this packet. In this scheme, the node needs to switch back and forth between the relaying mode and receiving mode.

The former strategy is convenient to implement, without requiring ideal timing and synchronization. On the other hand, the latter strategy may lead to faster broadcast, but it requires perfect timing and fast switching between the transmission mode and the receiving mode to avoid the packet lost. As these requirements are nontrivial to achieve in existing wireless networks, we choose the message-based strategy for convenience, at the expense of slightly slower broadcast speed.

Once starting to relay, each node sends the M packets in sequence, and then periodically repeats this process before the end of the transmission (which will be further discussed below). It is apparent that the minimum broadcast delay for a receiver to successfully obtain these packets is M slots, while mostly the delay is much larger than M due to lack of coordination between the transmitters and receivers.

C. Control of Transmission Duration

In our collaborative broadcast, each transmitter, either the source node or a relay node, stops sending packets once receiving the Acknowledgements (ACKs) from all of its neighboring

nodes or reaching the maximum transmission duration Δ, whichever comes first. The limit on the transmission duration is set to deal with the possible loss of the ACK signal due to the deep fading of wireless channels or the transmission confliction of multiple ACK signals.

Each ACK signal, including the message ID, receiver ID and time stamp, is sent on a fixed and known channel by a node right after successfully obtaining all M packets. In this way, each ACK signal is sent at a time ranging between the M-th slot and the Δ-th, depending on the delay of the message to the node from the source or a relay node.

As we will see, the transmission delay for a message to a 100-node network is usually as large as several thousand time slots, during which the 100 ACK signals are sent at a random time. Consequently, the probability for a node to simultaneously receive multiple ACK signals from its neighbors is small. Moreover, even if some of the ACK signals are lost, the node can still stop the transmission after the transmission limit Δ, and the system still works well.

By integrating the ACK mechanism in the transmission duration control, Δ only provides the upper bound of the transmission time in case the ACK signals are lost. We set $\Delta \triangleq \alpha T_{avg}^{hop}$, where the coefficient $\alpha > 0$ and T_{avg}^{hop} is the average time used for all the receivers within the neighboring area to receive the broadcast message from the transmitter. The average delay is used here, since it is challenging to predict the exact value in practical wireless networks.

For simplicity, assume that a transmitter periodically broadcasts M packets to n identical and independent nodes within its communication range. It is clear that the probability for all these receivers to obtain the packets during the first m slots is $(1-(1-p_a)^m)^{Mn}$. Hence the average broadcast delay over this single hop in terms of time slots is

$$T_{avg}^{hop} = M \sum_{m=0}^{\infty} \left[1-(1-(1-p_a)^m)^{Mn}\right]. \qquad (5)$$

Assuming uniform node placement, we have the average number of the nodes within the reach of one hop, $n = D^2N/R^2$. Hence the transmission duration Δ can be taken as

$$\Delta = \alpha M \sum_{m=0}^{\infty} \left[1-(1-(1-p_a)^m)^{\frac{D^2NM}{R^2}}\right]. \qquad (6)$$

By integrating the ACK mechanism in the transmission duration control, the broadcast performance is not sensitive to the specific value of α. Simulation results have shown that $\alpha = 0.5 \sim 2$ is a good choice, with stable broadcast delay and energy consumption performance.

IV. Broadcast Protocol

After discussing some key issues in the previous section, we now present two anti-jamming collaborative broadcast protocols for multihop wireless networks, based on the RRC and StRC strategies, respectively. It is assumed that each node knows the node IDs of its neighbors, i.e., legitimate nodes within its direct communication radius, and performs a distributed algorithm (Algorithm 1 or 2) to receive and/or transmit a message consisting of M packets.

A. RRC-based Broadcast

In the RRC-based protocol, each node other than the source node first enters the receiving mode. In this mode, a node independently and randomly selects one out of C channels and listens, and switches to another randomly selected channel after one or several time slots to counteract jamming. This process repeats until the node successfully receives all M packets.

while *The node has not received all M packets yet* **do**
  $ChID$ = an integer randomly selected from [1,C] ;
  Listen to the $ChID$-th channel;
end
Send ACK (Message ID, Node ID, Time Stamp);
$\Delta \leftarrow$ Eq. (6) ;
for $i \leftarrow 1$ **to** Δ **do**
  if *has not received ACKs from all its neighbors yet* **then**
    $ChID$ = an integer randomly selected in [1,C] ;
    Send a packet on the $ChID$-th channel;
  else
    Stop the transmission immediately
  end
end

Algorithm 1: RRC version of the anti-jamming collaborative broadcast protocol

Next, the node sends an ACK signal to inform its neighbors about its successful reception of the message, and then enters the transmission mode. The ACK signal containing the message ID, node ID and time stamp, is sent on a fixed and known channel.

The transmission mode of different nodes starts at different time (e.g., the source node enters this mode from the very beginning while a node at the edge of the network may never enter the transmission mode). In the transmission mode, each node randomly selects a channel out of the C channels and sends a packet.

In order to deal with the possible loss of ACK signals due to channel fading or jamming, we introduce a timeout mechanism, where each transmission stops after Δ slots, given by Eq. (6), even without receiving enough ACK signals. The node repeats this process to send all M packets in sequence, until it receives all the ACK signals from its neighbors, or Δ time slots elapse, whichever comes first.

B. StRC-based Broadcast

In the StRC-based protocol, each node relays the message on a fixed channel, assumed distinctly related to its node ID. Each node is assumed to know the relay channels that its neighbors may use. As mentioned in Section III-A, in order to counteract a smart jamming, each node has two receiving modes, based on whether any relay channel is not blocked: If that is true, the node is focused on the relay channels by randomly selecting one of the potential relay channels in the neighborhood; otherwise, the node randomly selects one out of all the C channels.

```
FlgClearRelayChannel=True;
while The node has not received all M packets yet do
    if FlgClearRelayChannel=True then
        ChID=an integer randomly selected from the relay
        channel set in its neighborhood;
    else
        ChID = an integer randomly selected from [1,C];
    end
    Listen to the ChID-th channel;
    if FlgClearRelayChannel=True then
        if All recent R_p packets are jammed then
            FlgClearRelayChannel=False;
        end
    else
        if The ChID-th channel is a unblocked relay channel
        then
            FlgClearRelayChannel=True;
        end
    end
end
Send ACK ( Message ID, Node ID, Time Stamp);
Δ ← Eq. (6) ;
ChID = an integer derived from its Node ID ;
for i ← 1 to Δ do
    if has not received ACKs from all its neighbors yet then
        Send a packet on the ChID-th channel;
    else
        Stop the transmission immediately
    end
end
```

Algorithm 2: StRC version of the anti-jamming collaborative broadcast protocol

Correspondingly, the StRC protocol uses such a status flag that is set to be true at the beginning, and then updates it according to the CRC checking results of the recent packets. When working on the relay channels, the receiver changes the flag to be false, if failing to receive all the recent R_p packets, which means that all these relay channels are very likely to be jammed. The parameter R_p is the actual number of neighboring nodes, or the average neighboring nodes n if the former is unknown. When coming across a clear relay channel, the node sets the flag to be true and focuses on the relay channels again.

Next, like the RRC-based protocol, the node also sends an ACK signal to its neighbors before entering to the transmission mode. Then the node sends the packets on a *fixed* channel corresponding to the partial node ID modulo C. The transmission duration is also determined by a timer of length Δ and the reception of the ACK signals from its neighbors.

V. Performance Evaluation

We evaluate the performance of the proposed collaborative broadcast, where a message consisting of $M = 7$ packets is broadcast to $N = 100$ nodes over $C = 128$ channels against J jammers with normalized jamming power $\rho = 2$, with the RRC-based strategy or the StRC-based strategy. We calculate the overall broadcast delay, defined as the time duration from the beginning of broadcast till the time when all the nodes in the network successfully receive the entire message, and the corresponding overall energy consumption, defined as the sum of the transmit and the receive energy consumed by all the $N + 1$ legitimate nodes during this process. The energy consumption for a node to send and to receive a packet are set as $E_t = D^\gamma$ and $E_r = 0.1$, respectively.

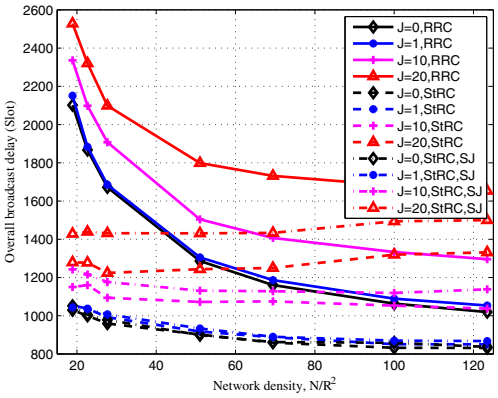
Figure 1 presents the RRC performance in solid curves and the StRC performance in dashed curves, against $J = 0$ to 20 jammers described in different colors. We consider both the responsive-sweep jamming and the smart jamming specifically targeting the StRC-based protocol (in dashed dot curves). It is shown that both schemes consume small energy and broadcast delay, compared to the existing jamming-resistant FH schemes. For example, the average broadcast delays of StRC and RRC are less than 900 and 1100 slots, respectively, for the broadcast of 7 packets to *100 nodes* against one sweep-responsive jammer with normalized jamming power 2, when the node density $N/R^2 \geq 100$ for $N = 100$ and $D = 1$. In this case, each node/jammer can approximately cover the whole network, as assumed in the BMA [6]. The performance of our scheme, especially the StRC version, is better than that of BMA for *a single receiving node* even *without* jamming (e.g., BMA takes approximately 2000 slots to send a message of 7 packets to a single node [6]).

It also confirms that the smart jamming can attack StRC more efficiently, especially when the number of jammers is large. But even in this case, the StRC strategy still outperforms the RRC in most cases. It can also be seen from Figure 1 that the broadcast delay and energy performance of RRC improves with the node density N/R^2, for given N, while the performance of StRC degrades with it when attacked by a large number of strong smart jammers.

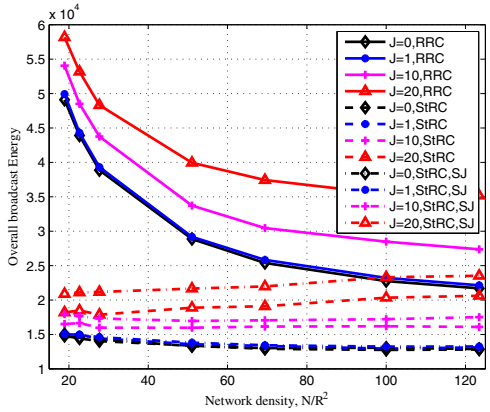
Next, we study the performance against wideband jammers that concurrently attack multiple channels. Assume a limitation on the total energy consumption of a jammer, i.e., a wideband jammer can increase the number of simultaneously attacked channels at the expense of smaller jamming radius. We consider a 3-hop wireless network with $n = 20$, $D = 1$ and $N = 100$. It is shown in Fig. 2 that the protocol can well resist ten jammers each concurrently blocking $C_J \leq 40$ channels with $\rho = 2$. The StRC strategy can provide stronger jamming resistance than the RRC strategy, even under the smart jamming focused on the relay channels.

Moreover, for the RRC strategy, when there are 10 jammers each simultaneously blocking all the C channels with $\rho = 2$, only 28 out of 100 nodes are jammed and the remaining 82 nodes can still successfully receive all the packets. Contrast to the intuition, even when all the channels are simultaneously jammed ($C_J = C$) by the wideband jammers, the collaborative broadcast still partly survives, thanks to the spatial diversity available in multihop networks.

Finally, the number of jammed nodes is maximizes at $C_J = 63$, which can be theoretically determined as $(C - n_s C_s)/n_J$. It is shown in Eq. (1) that a responsive-sweep jammer can simultaneously jam $Cp_J = n_s C_s + n_J C_J$ channels. All the nodes in its jamming area are blocked when $Cp_J = C$, or $C_J = (C - n_s C_s)/n_J$. Afterwards, the jamming probability no longer further increases with C_J, while the number of nodes



(a) Average broadcast delay



(b) Average energy consumption

Fig. 1. Broadcast performance vs. node density N/R^2, for the broadcast of $M = 7$ packets to $N = 100$ nodes with changing network radius R and signal coverage radius $D = 1$, against J responsive-sweep jammers or smart jammers (SJs).

in its covering area reduces with the shrinking of the jamming radius.

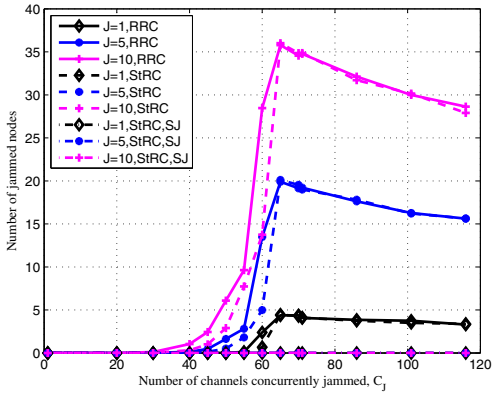


Fig. 2. Average number of jammed nodes by J responsive-sweep jammers each of which concurrently blocks C_J jamming channels with $\rho = 2$, in a broadcast to $N = 100$ nodes over $C = 128$ channels, with $n = 20$ and $D = 1$.

VI. Conclusion

We have proposed a distributed collaborative broadcast protocol that exploits the uncoordinated frequency hopping technique and node cooperation to counteract jamming in multihop wireless networks. With cooperation from relay nodes, this scheme provides spatial and frequency (channel) diversities to resist jamming and enhance communication efficiency. Unless all the channels across the whole geographic area are simultaneously jammed, the collaborative broadcast can always exploit the "white" area not being jammed or "white" channels in the jammed geographic area.

Simulation results show that the collaborative broadcast is robust against responsive smart jammers specially targeting the collaborative relaying strategies. Take the broadcast in a 3-hop network to 100 nodes for example, the protocol can well resist ten responsive-sweep jammers each simultaneously blocking 40 channels with double jamming power ($\rho = 2$). Even when each jammer blocks all $C = 128$ channels at the same time, only 28 nodes are jammed and more than 70% of the nodes can still receive the broadcast message. By exploiting the spatial distribution of the multihop wireless networks, this cooperative broadcast scheme can efficiently improve the communication efficiency against jamming, compared to most existing anti-jamming broadcast schemes, including BMA.

References

[1] L. Xiao, H. Dai, and N. Peng, "Jamming-resistant collaborative broadcast in wireless networks, part I: Singlehop networks," in *Proc. IEEE Globecom 2011, to appear*.

[2] L. Baird, W. Bahn, M. Collins, M. Carlisle, and S. Butler, "Keyless jam resistance," in *Proc. IEEE Information Assurance and Security Workshop*, 2007, pp. 143–150.

[3] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared key," in *Proc. USENIX Security Symposium*, 2009.

[4] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: jamming-resistant wireless broadcast communication," in *Proc. IEEE Infocom*, 2010.

[5] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Proc. IEEE symposium on security and privacy*, 2008.

[6] M. Strasser, C. Popper, and S. Capkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proc. MobiHoc*, 2009.

[7] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure," in *Proc. 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, 2010.

[8] D. Slater, P. Tague, R. Poovendran, and B. Matt, "A coding-theoretic approach for efficient message verification over insecure channels," in *Proc. ACM Conference on Wireless Network Security (WiSec'09)*, 2009.

[9] T. Jin, G. Noubir, and B. Thapa, "Zero pre-shared secret key establishment in the presence of jammers," in *Proc. ACM international symposium on Mobile ad hoc networking and computing*, 2009.

[10] L. Lazos amd S. Liu and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *Proc. ACM WiSec*, 2009.

[11] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "Defending DSSS-based broadcast communication against insider jammers via delayed seed-disclosure," in *Proc. IEEE Annual Computer Security Applications Conference (ACSAC)*, 2010.

[12] A. Goldsmith, *Wireless Communications*, chapter 3, Cambridge University Press, 2005.