Analysis and Optimization on Jamming-resistant Collaborative Broadcast in Large-Scale Networks

Chengzhi Li[1], Huaiyu Dai[1], Liang Xiao [2] and Peng Ning[3]

[1]ECE Dept.,
NC State Univ., Raleigh, NC, USA
{cli3, hdai}@ncsu.edu

[2]Dept. Comm. Engineering,
Xiamen Univ., Xiamen, China
lxiao@xmu.edu.cn

[3]CS Dept.,
NC State Univ., Raleigh, NC, USA
pning@ncsu.edu

Abstract— **Uncoordinated Frequency Hopping (UFH) is a viable anti-jamming solution without dependency on pre-shared secret keys, which nonetheless suffers from low communication efficiency. The Collaborative UFH (CUFH) scheme proposed recently in [1] dramatically improves both communication efficiency and jamming resistance of UFH with the help of relays. In this paper we study CUFH in a large scale broadcast network, with the number of nodes (much) larger than that of channels. In particular the optimal number of relays is derived and the trade-off on the number of packets a message is divided into is investigated, with respect to the network broadcast delay. In addition both upper and lower bounds of the average network broadcast delay are evaluated. Our analytical results are substantiated by simulations.**

I. INTRODUCTION

Jamming attacks are intentional powerful interference, aiming at drowning out the legitimate transmission by overpowering wireless receivers. Lack of immunity to jamming, wireless signals can be blocked, modified or replaced, which may jeopardize personal safety and national security. As a result, jamming-resistant broadcast is crucial to security-critical applications, e.g., emergency alert broadcast and navigation signal dissemination.

A popular strategy against jamming threat is the employment of Spread-Spectrum (SS) techniques, including Direct-Sequence Spread Spectrum (DSSS) and Frequency Hopping (FH). All these classic countermeasures rely on pre-shared secret keys, such as spreading code sequences and frequency hopping patterns, to achieve correct decoding at the receivers. Before the establishment or after the compromise of secret keys, these approaches are inefficacious. Several solutions are proposed recently to remove the dependency of SS techniques on secret keys to enhance their anti-jamming performance. A common strategy adopted by most works is to introduce randomness on the selection of spreading code sequences in DSSS or hopping channels in FH. Uncoordinated DSSS (UDSSS) [2], Uncoordinated FH (UFH) [3] and Randomized Differential DSSS (RD-DSSS) [4] belong to this category. In UDSSS (resp. UFH) nodes randomly select a spreading code (resp. channel) from a set of code sequences (resp. frequency

channels), and in RD-DSSS each bit is encoded using the correlation of unpredictable spreading codes. Randomness enhances the jamming immunity, yet typically degrades the communication efficiency. In [5] UFH was further enhanced by incorporating error control coding and one-way authenticator based on bilinear maps. However such improvement only reduces the communication latency up to one half [5], still far less efficient than the conventional (coordinated) FH. One way to further improve the efficiency is combining Uncoordinated FH with conventional FH, an example of which is given in [6], where the hopping pattern is conveyed through UFH to allow message transmission through coordinated FH. An alternative way is to allow cooperations among nodes. The Collaborative UFH (CUFH) proposed in [1] adopts this idea, where nodes having obtained the message serve as relays to accelerate the broadcast, significantly improving both communication efficiency and jamming resistance of UFH.

In this paper we provide some analysis on the CUFH scheme for a large scale broadcast network, when the number of nodes (far) exceeds that of the available channels. In particular, the optimal choices of two key system parameters, the number of relays and the number of packets that a message is divided into are explored, and both lower and upper bounds of the average network broadcast delay are evaluated.

The remainder of the paper is organized as follows. The system model is introduced in Section II; in Section III the trade-offs concerning the number of relays and packets per message are studied, and the average network broadcast delay is investigated; some simulation results are provided in Section IV; and we conclude this paper in Section V.

II. SYSTEM MODEL

Consider a time synchronized large scale broadcast network with one source node, N identical destination nodes and C non-overlapping frequency channels, where $C < N$ is assumed for efficient spectrum usage. Each channel accommodates transmission at a constant data rate R. An L-bit message is divided into $M(1 < M \leq L)$ packets and broadcasted by the source node sequentially and repeatedly. Suppose that each packet is attached with O-bit overhead involving the packet ID, Hash index, etc [3], and transmitted within a time slot (hop duration), whose duration is $T_s = \frac{O+L/M}{R}$. Uncoordinated Frequency Hopping is adopted and no channel synchronization between transmitters and receivers is available. At the beginning of each slot a transmitter (receiver) randomly chooses a channel out of the pool to transmit (listen).

A single omniscient jammer[1] with powerful and yet bounded computation and transmission capability is considered, which can perform both non-responsive and responsive jamming[2] [3] independently and simultaneously. In our model the jammer can sense and jam up to C_j channels in total per second; it has full knowledge about the network protocol and the ability to acquire any pre-shared secret keys (the jammer could be an insider). The probability that a packet is jammed is given by

$$p_j = \frac{C_j T_s}{C} = \frac{C_j(O + L/M)}{CR} = \alpha_1 + \frac{\alpha_2}{M}, \qquad (1)$$

where $\alpha_1 = \frac{C_j O}{CR}$ and $\alpha_2 = \frac{C_j L}{CR}$. To possibly evade the jamming attack it is reasonably assumed that $p_j < 1$, i.e., $\alpha_1 < 1$ and $M > \frac{\alpha_2}{1-\alpha_1}$.

III. ANALYSIS ON COLLABORATIVE UFH

Without requiring pre-shared secret keys, UFH exhibits robustness to insider jamming attacks and good scalability with the network size, at the cost of low communication efficiency. Collaborative UFH [1] exploits node cooperation to significantly improve both communication efficiency and jamming resistance. In this section, we first propose a variation of CUFH that is more suitable for application in large scale broadcast networks, where the number of nodes is (much) larger than the number of channels. Our new scheme is then evaluated in terms of network 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. Its performance is further optimized by tuning two key system parameters: the number of packets per message and the number of the relays.

Protocol 1: Collaborative UFH
  1) The source node randomly selects a channel from a pool of C frequency channels and broadcasts the packets of interest sequentially and repeatedly; similarly destination nodes randomly choose a channel to listen.
  2) Destination nodes serve as relays right after obtaining the whole message; similar to the source node, the relays randomly choose a channel and broadcast the packets sequentially and repeatedly.

When the CUFH scheme is applied in a large scale network the number of relays should be controlled. Allowing much more relays than the number of available channels in the network will harm, rather than benefit, the network performance due to the fact that collisions incurred by simultaneous transmissions will congest most of the channels. Hence, our new CUFH scheme is separated into two phases:

P1 Relay accumulation: Protocol 1 is followed until there are N_r relays including the source node[3]; An optimal

---

value of N_r is given in Proposition 1. In practice, it is usually sufficient to control N_r around the number of channels C, as verified below.

P2 Collaborative broadcasting: the N_r relays continue to broadcast their packets until all the remaining nodes receive them. No more new relays are admitted in this phase.

A primary metric of interest in our scheme is the packet reception rate, defined as the probability that a destination node correctly decodes a packet in a time slot. Supposing there are $n_r(> 1)$ relays at the beginning of a slot and noticing the fact that there is no collision if different relays send the same packet into the same channel, the packet reception rate is given by:

$$
\begin{aligned}
p_{n_r}(M) &= \sum_{l=1}^{n_r} \binom{n_r}{l} (\frac{1}{C})^l (1 - \frac{1}{C})^{n_r-l} (\frac{1}{M})^{l-1} (1 - p_j) \\
&= M \sum_{l=1}^{n_r} \binom{n_r}{l} (\frac{1}{CM})^l (1 - \frac{1}{C})^{n_r-l} (1 - p_j) \\
&= M [a^{n_r} - b^{n_r}] (1 - p_j), \qquad (2)
\end{aligned}
$$

where $a = 1 - (1 - \frac{1}{M})\frac{1}{C}$, $b = 1 - \frac{1}{C}$, and p_j is given in Eq. (1). In contrast, the packet reception rate of the original UFH is $p_1(M) = \frac{1}{C}(1 - p_j)$. The cooperation gain $g_c(M) \triangleq \frac{p_{n_r}(M)}{p_1(M)}$ will be examined below.

A. Discussion on p_{n_r}

As a key metric, p_{n_r} offers many insights for performance evaluation and optimization. In the following, we show that the optimal number of relays $n_r^*(M)$ and the optimal cooperation gain $g_c^*(M)$ are both $\theta(C)$. We also reveal that $p_{n_r^*(M)}(M)$ increases with M and converges to a nontrivial upper bound.

Proposition 1: $p_{n_r}(M)$ is maximized at

$$n_r^*(M) = \ln \left(\frac{\ln b}{\ln a} \right) / \ln(\frac{a}{b}),$$

where a and b are given after Eq. (2). And

$$C \leq n_r^*(M) \leq 1.4C,$$

for large C.

Proof: It's easy to check that p_{n_r} is a concave function of n_r. The optimal $n_r^*(M)$ follows by solving

$$\frac{dp_{n_r}}{dn_r} = M(a^{n_r} \ln a - b^{n_r} \ln b)(1 - p_j) = 0.$$

Since $n_r^*(M)$ is a decreasing function with M the maximum and infimum of n_r^* are given below respectively:

$$\bar{n}_r^* = n_r^*(2) = \frac{\ln \frac{\ln(1-1/C)}{\ln(1-1/(2C))}}{\ln \frac{1-1/(2C)}{1-1/C}} \approx 2 \ln 2C \approx 1.4C,$$

$$\underline{n}_r^* = \lim_{M \to \infty} n_r^*(M) = \frac{1}{-\ln(1 - 1/C)} \approx C,$$

where the approximation is made through Taylor series expansion for sufficiently large C. ∎

Remark 1: Given M, larger p_{n_r} always leads to smaller broadcast delay. Thus, ideally we should set $N_r = n_r^*(M)$ in

---

[1]In practice, multiple jammers may be deployed, whose influence can be modeled as one omniscient jammer in a broadcast network without loss of generality.

[2]Non-responsive jammers jam a certain amount of channels directly in a time slot and responsive jammers sense a certain amount of channels first and jam those with ongoing signals of interest.

[3]The roles played by the source node and relays are identical for a destination node. However it is assumed that there is no packet synchronization among relays, i.e., relays transmit packets independently.

our scheme. In practice due to the dynamics of the system, it is more feasible to constrain the relays just within a small region around n_r^*. Numerical results (omitted here in the interest of space) also suggest that performance loss is negligible when N_r in our scheme is sufficiently close to n_r^*.

Proposition 2: The optimal cooperation gain

$$g_c^*(M) \triangleq \frac{p_{n_r^*(M)}(M)}{p_1(M)} \in (0.35C, 0.5C], \ \forall M > 1,$$

where $p_1(M)$ is the packet reception rate of the original UFH.

Proof:

$$g_c^*(M) \ = \ \frac{p_{n_r^*(M)}(M)}{p_1(M)} = \frac{M(a^{n_r^*(M)} - b^{n_r^*(M)})}{1/C}.$$

Due to the fact that function $f(M, n) = M(a^n - b^n)$ is a decreasing function of M converging to $\lim_{M\to\infty} f(M, n) = \frac{n}{C}(1 - 1/C)^{n-1}$, and $M > 1$,

$$f(\infty, n_r^*(M)) < g_c^*(M)/C < f(2, n_r^*(M)).$$

Noticing that function $y_1(n) = f(2, n)(y_2(n) = f(\infty, n))$ is maximized (minimized) at $n = \bar{n}_r^*$ for $n_r \in [\underline{n}_r^*, \bar{n}_r^*]$, the conclusion follows after some calculation (plugging $\bar{n}_r^*$ into $y_1(n)$ and $y_2(n)$). ∎

Proposition 3: Given $\alpha \triangleq \frac{\alpha_2}{1-\alpha_1} > 1.4$ and large C, $p_{n_r^*(M)}(M)$ is an increasing function of M and converges to $0.38(1 - \alpha_1)$.

Proof: A straightforward way is to show $\frac{dp_{n_r^*(M)}(M)}{dM} > 0$, which involves tedious calculation. We adopt a simpler approach. Fix $n_r \in [\underline{n}_r^*, \bar{n}_r^*]$ in Eq. (2), then,

$$p_{n_r}(M)$$
$$\rightarrow \ [(1-\alpha_1)M - \alpha_2][\exp(-\frac{(1-1/M)n_r}{C}) - \exp(-\frac{n_r}{C})]$$
$$= \ [(1-\alpha_1)M - \alpha_2]\exp(-\frac{n_c}{C})(\exp(\frac{n_r}{CM}) - 1)$$

where the approximation is made due to the fact that $\left(1 - \frac{a}{C}\right)^{n_r} \rightarrow \exp(-\frac{an_r}{C})$ for large C and n_r. The derivative of $p_{n_r}(M)$ with respective to M is

$$\frac{dp_{n_r}(M)}{dM} = (1-\alpha_1)[\exp(x_0)(1 - x_0 + \frac{\alpha}{M}x_0) - 1]$$

where $x_0 = \frac{n_r}{CM}$. Due to the fact $M > \alpha$ function $f(x) = \exp(x)(1 - x + \frac{\alpha}{M}x)$ monotonically increases when $x < \frac{\alpha}{M-\alpha}$. Given $\alpha > 1.4$, $x_0 < \frac{\alpha}{M-\alpha}$ which leads to $f(x_0) > f(0) = 1$. so that $\frac{dp_{n_r}(M)}{dM} > 0$. Thus, $p_{n_r}(M)$ is increasing and converges to $y(n_r) = \lim_{M\to\infty} p_{n_r}(M) = \frac{n_r}{C}(1 - \frac{1}{C})^{n_r-1}(1 - \alpha_1)$. The conclusion follows from the fact that $p_{n_r^*(M)}(M) \le p_{n_r^*(M)}(M+1) \le p_{n_r^*(M+1)}(M+1)$, and $p_{n_r^*(\infty)}(\infty) \approx 0.38(1 - \alpha_1)$. ∎

This proposition indicates that dividing the message into more packets benefit packet reception rate, which, however, does not imply the ultimate improvement on network throughput. We will show below that there exists an optimal M so that the broadcast delay is minimized.

B. Broadcast delay analysis

The following lemma is useful in our analysis of the network broadcast delay D. Assume there are n_r relays in the network, which is invariant in the subsequent time. A non-relay node A is in need of m more *distinct* packets. Denote by d_A the time delay, in terms of the number of slots, for node A to receive all the remaining m packets. Then

Lemma 1: the Cumulative Distribution Function (CDF) of d_A, $\Pr(d_A \le q) \triangleq \epsilon(m, n_r, q)$ is

$$\Pr(d_A \le q) \qquad\qquad (3)$$
$$= \ \sum_{k=m}^{M-1} \binom{q}{k} p_{n_r}^k (1 - p_{n_r})^{q-k} \sum_{j=m}^{k} \binom{M-m}{j-m} P(j,k)$$
$$+ \ \sum_{k=M}^{q} \binom{q}{k} p_{n_r}^k (1 - p_{n_r})^{q-k} \sum_{j=m}^{M} \binom{M-m}{j-m} P(j,k),$$

when $q \ge M$,

$$\Pr(d_A \le q) = \sum_{k=m}^{q} \binom{q}{k} p_{n_r}^k (1-p_{n_r})^{q-k} \sum_{j=m}^{k} \binom{M-m}{j-m} P(j,k),$$

when $m \le q < M$, and $\Pr(d_A \le q) = 0$ when $q < m$, where

$$P(j,k) = \sum_{i=0}^{j} (-1)^i \binom{j}{i} (j-i)^k / M^k.$$

And the mean of d_A is given by

$$E(d_A) = \frac{1}{p_{n_r}(M)} \sum_{i=M-m+1}^{M} \frac{M}{M-i+1}$$

where $p_{n_r}(M)$ is given in Eq. (2).

Proof:
$$d_A = t_{M-m+1} + ... + t_M, \qquad\qquad (4)$$

where t_i, $i = M-m+1, M-m+2, ..., M$, is the time interval between the ith packet and $i + 1$th (different) packet node A receives, and is geometrically distributed with parameter $\frac{M-i+1}{M} p_{n_r}(M)$. Then,

$$E(d_A) = E(t_{M-m+1}+...+t_M) = \frac{1}{p_{n_r}} \sum_{i=M-m+1}^{M} \frac{M}{M-i+1}.$$

Although d_A is the sum of random variables with known distributions, it's challenging to derive the CDF of d_A directly from Eq. (4). An alternative way is pursued below. The probability that k packets are successfully received within $q(\ge m)$ time slots is $\binom{q}{k} p_{n_r}^k (1 - p_{n_r})^{q-k}$, and the probability that these k successfully decoded packets include the m different packets is $\sum_{j=m}^{k} \binom{M-m}{j-m} P(j,k)$ for $m \le k < M$ and $\sum_{j=m}^{M} \binom{M-m}{j-m} P(j,k)$ for $k \ge M$ (only possible when $q \ge M$), where $P(j,k) = \frac{a(j,k)}{M^k}$ is the probability that k successful decoded packets include exactly j given distinct packets and $a(j,k)$ is derived in Appendix I. ∎

Lemma 1 reveals some insights into the broadcast delay of a particular non-relay node A in Phase 2. At the beginning of Phase 2 node A needs at least one more packet and at most all

the M packets. As a result, the shortest and longest average delay for node A, $t_{A,\min}$ and $t_{A,\max}$, are given by

$$t_{A,\min} = \frac{M}{p_{N_r}} T_s, t_{A,\max} = \frac{1}{p_{N_r}} \sum_{i=1}^{M} \frac{M}{M-i+1} T_s.$$

Substituting T_s into $t_{A,\min}$ and $t_{A,\max}$, and noticing that the harmonic number $\sum_{i=1}^{n} 1/n$ grows as fast as $\ln n$, we have

$$t_{A,\min} = \frac{MO}{p_{N_r}R} + \frac{L}{Rp_{N_r}},$$

and

$$t_{A,\max} \approx \frac{OM \ln M}{Rp_{N_r}} + \frac{L \ln M}{Rp_{N_r}}.$$

Since p_{N_r} is bounded

$$\Theta(M) < t_A < \Theta(M \ln M) \quad O \neq 0$$
$$\Theta(1) < t_A < \Theta(\ln M) \quad O = 0,$$

when M is large. Some interesting observations are in order:
- The broadcast delay increases with M when M is large.
- Overhead results in dramatic increase in the broadcast delay;
- There exists an optimal M such that the broadcast delay is minimized since $t_A \to \infty$ as $M \to \infty$ and $M \to \alpha_2/(1-\alpha_1)$ (in the latter case the jamming probability $p_j = 1$).

Now we are ready to analyze the network average broadcast delay $E(D)$. It's not tractable to derive an exact expression of $E(D)$. Instead we evaluate its upper and lower bounds. Denote by D_i the time slots elapsed during phase i, $i = 1, 2$, and denote by $\bar{X}$ ($\underline{X}$) the upper (lower) bound of $E(X)$. We have

Theorem 1: The upper bound of $E(D)$ is

$$\bar{D} = \bar{D}_1 + \bar{D}_2$$

where

$$\bar{D}_1 = \bar{t}_1 + \sum_{n_r=2}^{N_r-1} \sum_{q=0}^{\infty} (1 - \epsilon(M, n_r, q))^{N-n_r+1}, \text{ with}$$

$$\bar{t}_1 = \sum_{i=0}^{\infty} (1 - (1 - (1-p_1)^i)^M)^N M, \text{ and}$$

$$\bar{D}_2 = \sum_{q=0}^{\infty} (1 - \epsilon(M, N_r, q))^{N-N_r+1}.$$

Proof: We first evaluate $\bar{D}_1$. Assume at each slot at most one relay appears, which offers an upper bound for D_1. Denote by t_{n_r} the time interval before one new relay appears, with the help of n_r relays (including the source). Therefore

$$D_1 \leq \sum_{n_r=1}^{N_r-1} t_{n_r},$$

and

$$t_{n_r} = \min\{t_{n_r,1}, t_{n_r,2}, ..., t_{n_r,N-n_r+1}\}, \tag{5}$$

where $t_{n_r,i}$ is the time delay for the ith non-relay node to receive the whole message. Then,

$$\Pr(t_{n_r} > q) = \Pr(t_{n_r,1} > q, t_{n_r,2} > q, ..., t_{n_r,N-n_r+1} > q),$$

and $E(t_{n_r}) = \sum_{q=0}^{\infty} \Pr(t_{n_r} > q)$.

When $n_r = 1$, i.e., only the source node broadcasts, we calculate the delay in rounds with each composed of M slots (since we are concerned with an upper bound here). Thus,

$$\begin{aligned}\Pr(t_1 > iM) &= \Pr(t_{1,1} > iM, t_{1,2} > iM, ..., t_{1,N} > iM) \\ &= (\Pr(t_{1,1}) > iM)^N \\ &= (1 - (1 - (1-p_1)^i)^M)^N\end{aligned}$$

which leads to $\bar{t}_1 = \sum_{i=0}^{\infty} (1 - (1 - (1-p_1)^i)^M)^N M$.

For $n_r > 1$, the upper bound $\bar{t}_{n_r}$ is given by:

$$\begin{aligned}\bar{t}_{n_r} &= \sum_{q=0}^{\infty} (\Pr(t_{n_r,1}) > q)^{N-n_r+1} \\ &= \sum_{q=0}^{\infty} (1 - \epsilon(M, n_r, q))^{N-n_r+1},\end{aligned}$$

assuming the worst possible scenario that all the non-relay nodes are waiting for all the M packets.

$\bar{D}_1$ follows after summing up $\bar{t}_1$ and all the $\bar{t}_{n_r}$, $2 \leq n_r \leq N_r - 1$.

Next we investigate $\bar{D}_2$. According to our protocol

$$D_2 = \max(t_{N_r,1}, t_{N_r,2}, ..., t_{N_r,N-N_r+1}).$$

Then,

$$\Pr(D_2 \leq q) = \Pr(t_{N_r,1} \leq q, t_{N_r,2} \leq q, ..., t_{N_r,N-N_r+1} \leq q).$$

Again the upper bound $\bar{D}_2$ follows from the assumption that none of the non-relay nodes has ever received any packet successfully, i.e.,

$$\Pr(D_2 \leq q) = (\Pr(d_1) \leq q)^{N-N_r+1} = \epsilon(M, N_r, q)^{N-N_r+1}.$$

$\blacksquare$

The lower bound of D is obtained by considering a hypothetical network where there are $N_r = n_r^*$ identical source nodes and N destination nodes. These source nodes transmit the packets sequentially and repeatedly but each starts transmission from a random packet. Due to the cooperation gain given in Prop. 2, this hypothetical network performs better than the original network. Then the lower bound is given by

Theorem 2:

$$\underline{D} = \sum_{q=0}^{\infty} (1 - \epsilon(M, n_r^*, q)^N).$$

The proof follows from the derivation of $\bar{D}_2$ in last theorem.

Note that we have ignored the delay in Phase 1 in Theorem 2. With the observation that t_1 usually is a significant portion of D_1, in practice we may use $\underline{D} + \bar{t}_1$ to estimate $E(D)$.

IV. SIMULATION RESULTS

We substantiate our theoretical results above by simulations in this section. The following simulation setting is adopted unless otherwise noted: the number of channels $C = 64$, $O = 10$bits, $L = 300$ bits, $R = 1k$bps, $C_j = 640/\text{sec}$, and $M = 5$. Fig.1 shows the average network broadcast delay (in time slots) for different number of relays[4]. We can see

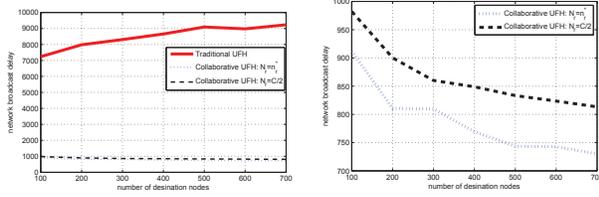[4]The right figure is the amplified version of the left one.

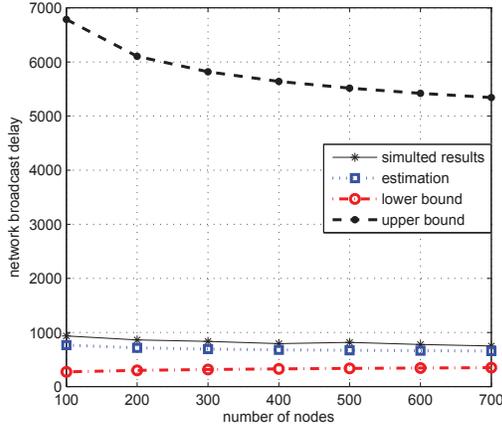Fig. 1: The average broadcast delay VS the number of relays

Fig. 2: The average broadcast delay: simulated results VS theoretical results

Fig. 3: The CDF of average broadcast delay for different M

that Collaborative UFH significantly outperforms UFH and appropriate selection of the number of relays further improves the network throughput. Another interesting observation is that, for CUFH the broadcast delay decreases with the number of nodes. The intuition behind this observation is that larger multiuser diversity is beneficial for relay accumulation at Phase 1, which more than compensates the extra need at Phase 2.

Fig. 2 compares the average network broadcast delay in our theoretical analysis and simulation. It is found that the lower bound given in Theorem 2 is much tighter than the upper bound given in Theorem 1, and the pragmatic estimation is close to the simulation result. Additionally, the estimation curve reveals that t_1 not only dominates in the delay of Phase 1 but also contributes much to the total delay.

Fig. 3 shows the CDF of the broadcast delay (in second) for different M, where $N = 200$ and other parameters keep the same. The trade-off in M is clearly demonstrated in the figure: there exists an optimal M ($M = 11$ in the figure) such that the broadcast delay is minimized.

V. CONCLUSIONS

In this paper we have studied Collaborative UFH in a large scale broadcast network. We have revealed that to maximize the packet reception rate the number of relays is roughly equal to the number of channels, and there exists an optimal number of packets per message such that the average broadcast delay is minimized. We have also derived a technical result on the CDF
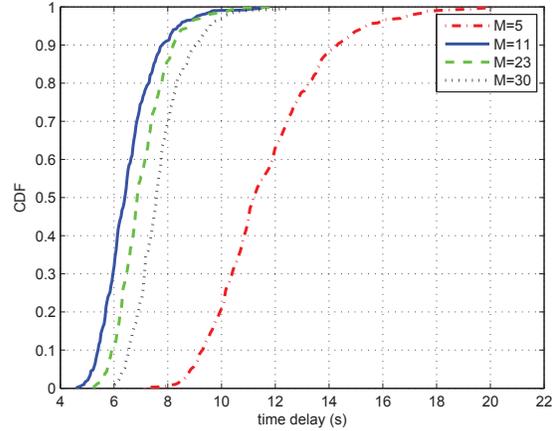
of the delay that a node need to receive the remaining packets for a message, based on which some lower and upper bounds of the average network broadcast delay have been obtained. We plan to extend our study to the multi-hop scenario in our future work.

APPENDIX I
THE DERIVATION OF $a(j, k)$

Our case is equivalent to the scenario where k eggs are independently put into one of j baskets. $a(j, k)$ is the number of possibilities that each basket at least has one egg, which can be calculated recursively as

$$a(j, k) = j^k - \sum_{i=1}^{j-1} \binom{j}{i} a(i, k),$$

which leads to $a(j, k) = \sum_{i=0}^{j} (-1)^i \binom{j}{i} (j - i)^k$ after some computation.

REFERENCES

[1] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using frequency hopping," *IEEE Trans. Wireless communication*, 2011, submitted.
[2] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared key," in *Proc. USENIX Security symposium*, 2009.
[3] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jammming-resistant key setablishment using uncoordinated frequency hopping," in *Proc. IEEE symposium on security and privacy*, 2008.
[4] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: jamming-resistant wireless boradcast commuincation," in *Proc. inforcom*, 2010.
[5] M. Strasser, C. Popper, and S. Capkun, "Efficient uncoordinated fhss anti-jammming communication," in *Proc. Mobihoc*, 2009.
[6] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "USD-FH: Jamming-resistant wireless communicatin using frequency hopping with uncoordinated seed disclosure," in *Proc. 7th IEEE international conference on mobile ad-hoc and sensor systems*, 2010.