Radio Networks With Reliable Communication

Yvo Desmedt[1⋆], Yongge Wang[2⋆⋆], Rei Safavi-Naini[3], and Huaxiong Wang[4]

[1] University College London (y.desmedt@cs.ucl.ac.uk)
[2] University of North Carolina at Charlotte (yonwang@uncc.edu)
[3] University of Wollongong (rei@uow.edu.au)
[4] Macquarie University (hwang@comp.mq.edu.au)

Abstract. Problems of secure communication and computation have been studied extensively in network models, for example, Franklin and Yung have studied secure communications in the general networks modeled by hypergraphs. Radio networks have received special attention in recent years. For example, the Bluetooth and IEEE 802.11 networks are all based on radio network technologies. In this paper, we use directed colored-edge multigraphs to model the radio networks and study reliable and private message transmissions in radio networks.
Keywords: radio network, privacy, reliability

1 Introduction

If two parties are connected by a private and authenticated channel, then secure communication between them is guaranteed. However, in most cases, many parties are only indirectly connected, as elements of an incomplete network of private and authenticated channels. In other words they need to use intermediate or internal nodes. Achieving participants cooperation in the presence of faults is a major problem in distributed networks. The interplay of network connectivity and secure communication have been studied extensively (see, e.g., [2, 5, 9, 10, 16]). For example, Dolev [9] and Dolev et al. [10] showed that, in the case of k Byzantine faults, reliable communication is achievable only if the system's network is $2k + 1$ connected. Hadzilacos [16] has shown that connectivity $k + 1$ is required to achieve reliable communication in the presence of k faulty participants even if those faults are not malicious.

Goldreich, Goldwasser, and Linial [15], Franklin and Yung [14], Franklin and Wright [13], and Wang and Desmedt [20] have initiated the study of secure communication and secure computation in *multi-recipient (multicast)* models. A "multicast channel" (such as Ethernets) enables one participant to send the same message—simultaneously and privately—to a fixed subset of participants. Franklin and Yung [14] have given a necessary and sufficient condition for individuals to exchange private messages in multicast models in the presence of passive adversaries (passive gossipers). For the case of active Byzantine adversaries, many results have been presented by Franklin and Wright [13], and, Wang and Desmedt [20]. Note that Goldreich, Goldwasser, and Linial [15]

⋆ A part of this research was done while visiting the University of Wollongong. A part of this work has been funded by CCR-0209092. The author is BT Professor of Information Security.
⋆⋆ A part of this research was funded by NSF.

have also studied fault-tolerant computation in the public multicast model (which can be thought of as the largest possible multirecipient channels) in the presence of active Byzantine adversaries. Specifically, Goldreich, Goldwasser, and Linial [15] has made an investigation of general fault-tolerant distributed computation in the full-information model. In the full information model no restrictions are made on the computational power of the faulty parties or the information available to them. (Namely, the faulty players may be infinitely powerful and there are no private channels connecting pairs of honest players). In particular, they present efficient two-party protocols for fault-tolerant computation of any bivariate function.

There are many examples of multicast channels. A simple example is a local area network like an Ethernet bus or a token ring. Another example is the Bluetooth or IEEE 802.11 network.

We consider a *radio network* in which stations can communicate with each other using frequencies allocated to them. Let F be the set of frequencies. Each station knows a subset of F. However at any given time it can only use a subset of its allocated frequencies, according to a defined *frequency schedule*. Communication can be *jammed* due to *intentional or accidental jamming*. The aim of this paper is to analyze these networks and construct protocols that allow reliable communication when it is possible.

The radio networks studied in [1] is similar to our model. In particular, they considered a special case of jamming as follows: a processor receives no messages if it is the recipient of of two or more partial broadcasts simultaneously. However, they do not consider privacy.

Note that a special case of frequencies allocation problem is the random key predestribution problem. Recently, Eschenauer and Gligor [12] constructed a specific random key distribution scheme and used it to build random sensor networks.

The outline of the paper is as follows. We introduce our model in Section 2. In Sections 3, 4, and 5, we study reliable message transmission against passive adversaries, jamming adversaries, and active adversaries in radio networks respectively. We study probabilistically reliable and perfectly private message transmission in certain radio networks in Section 7, and discuss the radio networks with minimal number of frequencies in Section 8. We conclude our paper with some open problems in Section 9.

2 Model

A *radio network* is a *directed colored-edge multigraph* $R(V, E, F, c)$, where V is the node set (corresponding to radio stations), E is the directed edge set (there might be more than one directed edge from one node to another one), F is the frequency (color) set, and c is a map from E to F (the map c assigns a frequency to each edge).

In a radio network, we assume that any message sent by a node v on a frequency f will be received identically by all nodes u such that there is a directed edge $e \in E$ from v to u and $c(e) = f$, whether or not v is faulty, and no other party (even if it has an incoming edge with frequency f originated from another node or it can use frequency f to broadcast to other nodes) learns anything about the content of the message.

Franklin and Yung [14] used hypergraphs[1] to model the multicast networks. A hypergraph H is a pair (V, E) where V is the node set and E is the hyperedge set. Each hyperedge $e \in E$ is a pair (v, v^*) where $v \in V$ and v^* is a subset of V. In a hypergraph, any message sent by a node v will be received identically by all nodes in v^*, whether or not v is faulty, and all parties outside of v^* learn nothing about the content of the message. Unless specified otherwise, we will use radio networks throughout our paper and will not use hypergraph networks.

It is easy to see that Franklin-Yung's hypergraph networks is a special case of our radio networks (the difference will be clear from the adversary model which we will give later).

Let $v, u \in V$ be two nodes of the radio network $R(V, E, F, c)$. We say that there is a "direct link" from node v to node u if there exists a directed edge e from v to u. We say that there is an "undirected link" from v to u if there is a directed link from v to u or a directed link from u to v. If there is a directed (undirected) link from v_i to v_{i+1} for every i, $0 \leq i < k$, then we say that there is a "directed path" ("undirected path") from v_0 to v_k.

Throughout the paper, we consider receiver-jamming, sender-jamming, destroy-jamming, and multicast as our only communication primitives.

1. A node v can receiver-jam on a frequency f if there is a directed edge e from v to some node u with $c(e) = f$. The result of receiver-jamming by v on frequency f is that for any node u such that there is a directed edge e from v to u, u cannot receive any message transmitted on the frequency f by any node.
2. A node v can sender-jam on a frequency f if there is a directed edge e from v to some node u with $c(e) = f$. The result of sender-jamming by v on frequency f is that for any node u such that there is a directed edge e from v to u, u cannot send any message on the frequency f to any node.
3. A node v can destroy-jam on a frequency f if there is a directed edge e from v to some node u with $c(e) = f$. The result of destroy-jamming by v on frequency f is that for any node u such that there is a directed edge e from v to u, u cannot receive or send any message on any frequency.
4. A message that is multicast by a node v on a frequency f in a radio network $R(V, E, F, c)$ shall be received by all nodes u satisfying the following conditions with privacy (that is, other nodes learn nothing about what was sent) and authentication (that is, the node u is guaranteed to receive the value that was multicast and to know which node multicast it)[2]
   - There is a directed edge e from v to u and $c(e) = f$.
   - u is not being jammed on the frequency f.

In addition to the intentional jamming by a malicious adversary, communications in radio networks can be accidentally jammed by honest users when a well planned schedule is not followed. Consider the following scenario, if both nodes u and v try to send messages to the node w on the same frequency f at the same time slot, then it is clear that

[1] Franklin-Yung's hypergraphs are different from the the standard definition in [3].

[2] Note that this is reasonable assumption if both u and v can share a private key. However, if u and v does not share a private key, then no authenticity is guaranteed since nodes v' might impersonate v if there is a directed edge e' from v' to u.

the node w will be "jammed". We call this kind of jamming *accidental jamming*. Accidental jamming is more or less a design problem and we will not further our study on this topic in this paper (more details could be found in [4]).

We assume that all nodes in the radio network know the complete protocol specification and the complete structure of the radio network. In a message transmission protocol, the sender A starts with a message M^A drawn from a message space $\mathcal{M}$ with respect to a certain probability distribution. At the end of the protocol, the receiver B outputs a message M^B. We consider a synchronous system in which messages are sent via multicast in rounds. During each round of the protocol, each node receives any messages that were multicast for it at the end of the previous round, flips coins and perform local computations, and then possibly multicasts a message. We will also assume that the message space $\mathcal{M}$ is a subset of a finite field $\mathbf{F}$.

Throughout this paper k denotes the number of faults under the control of the adversary. We write $|S|$ to denote the number of elements in the set S. We write $x \in_R S$ to indicate that x is chosen with respect to the uniform distribution on S.

We consider three kinds of adversaries. A passive adversary (or gossiper adversary) is an adversary who can only observe the traffic through k internal nodes. A jamming adversary is an adversary who can observe the traffics through some k internal nodes and/or jam from these k internal nodes. An active adversary (or Byzantine adversary) is an adversary with unlimited computational power who can control k internal nodes. That is, an active adversary will not only listen to the traffics through the controlled nodes, but also control the message (might be jamming noise) sent by those controlled nodes. All kinds of adversaries are assumed to know the complete protocol specification, message space, and the complete structure of the radio network. At the start of the protocol, the adversary chooses the k faulty nodes. (An alternative interpretation is that k nodes are collaborating adversaries.) The power of the adversaries is listed as follows (weakest first).

$$k\text{-passive adversary} \rightarrow k\text{-jamming adversary} \rightarrow k\text{-active adversary}$$

Throughout the paper, we assume that an active adversary can mount jamming attacks automatically. We will mainly consider three kinds of jamming in this paper: receiver-jamming, receiver-and-sender-jamming, and destroy-jamming. Thus, we will respectively have three kinds of active adversaries according to their jamming ability: rj-active adversary, rsj-active adversary, and dj-active adversary.

For any execution of the protocol, let adv be the adversary's view of the entire protocol. We write $adv(M, r)$ to denote the adversary's view when $M^A = M$ and when the sequence of coin flips used by the adversary is r.

Definition 1. *1. A message transmission protocol is* δ-reliable *if, with probability at least* $1 - \delta$*, B terminates with $M^B = M^A$. The probability is over the choices of M^A and the coin flips of all nodes.*

2. *A message transmission protocol is* reliable *if it is* 0-reliable.
3. *A message transmission protocol is* ε-private *if, for every two messages M_0, M_1 and every r, $\sum_c |\Pr[adv(M_0, r) = c] - \Pr[adv(M_1, r) = c]| \leq 2\varepsilon$. The probabilities are taken over the coin flips of the honest parties, and the sum is over all possible values of the adversary's view.*

4. *A message transmission protocol is* perfectly private *if it is* 0-private.
5. *A message transmission protocol is* (ε, δ)-secure *if it is* ε*-private and* δ*-reliable.*
6. *An* (ε, δ)*-secure message transmission protocol is* efficient *if its round complexity and bit complexity are polynomial in the size of the network,* $\log \frac{1}{\varepsilon}$ *(if* $\varepsilon > 0$*) and* $\log \frac{1}{\delta}$ *(if* $\delta > 0$*).*

3 Achieving perfect privacy and reliability against passive adversaries

Let $R(V, E, F, c)$ be a radio network, and $S \subset V$ be a node set. Then the reduced radio network $R(V \setminus S, E_{V \setminus_p S}, F, c)$ is defined by letting $E_{V \setminus_p S} = E \setminus E_S^p$, where E_S^p is the set of the following directed edges:

1. all edges originated from nodes in S.
2. all incoming edges of nodes in S.
3. all edges e from u to v such that there is an edge e' from u to some node in S and $c(e) = c(e')$.

Theorem 1. *Reliable and perfectly private message transmission from* u *to* v *in a radio network* $R(V, E, F, c)$ *is possible against a* k*-passive adversary if and only if the following conditions are satisfied:*

1. *There is a directed path from* u *to* v *in* $R(V, E, F, c)$.
2. *For any* k*-node set* S*, there is an undirected path from* u *to* v *in the reduced radio network* $R(V \setminus S, E_{V \setminus_p S}, F, c)$.

Proof. The proof is the same as that in Franklin and Yung [14] for reliable and perfectly private message transmission in hypergraphs. Q.E.D.

4 Achieving reliability against jamming adversaries

We first give a sufficient and necessary condition for achieving reliability against receiver-jammers. Let $R(V, E, F, c)$ be a radio network, and $S \subset V$ be a node set. Then the radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$ is defined by letting $E_{V \setminus_{rj} S} = E \setminus E_S^{rj}$, where E_S^{rj} is the set of the following directed edges:

1. all edges originated from nodes in S.
2. all edges e from u to v such that there is an edge e' from some node in S to v and $c(e) = c(e')$.

Theorem 2. *Reliable message transmission from* u *to* v *in a radio network* $R(V, E, F, c)$ *against a* k*-receiver-jamming adversary is possible if and only if for any* k*-node set* S*, there is a directed path from* u *to* v *in the reduced radio network* $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$.

Proof. If the condition is not satisfied, then there is a k-node set S such that there is no directed path from u to v in the reduced radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$. Thus if the k-receiver-jammer controls all the nodes in S and keeps receiver-jamming on all available frequencies, all message transmissions from u to v will be blocked.

If the condition of the Theorem is satisfied, then for each k-node set S, there is a directed path p_S from u to v in the reduced radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$. Thus u can transmit the message along all such paths (there are $\binom{|V|-2}{k}$ such paths) with different $\binom{|V|-2}{k}$ time slots. Q.E.D.

Now we give similar necessary and sufficient conditions for achieving reliability against receiver-and-sender-jammers and destroy-jammers. Let $R(V, E, F, c)$ be a radio network, and $S \subset V$ be a node set. Then the radio network $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ is defined by letting $E_{V \setminus_{rsj} S} = E \setminus E_S^{rsj}$, where E_S^{rsj} is the set of the following directed edges:

1. all edges originated from nodes in S.
2. all edges e from u to v such that there is an edge e' from some node in S to v or u and $c(e) = c(e')$.

Similarly, the radio network $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$ is defined by letting $E_{V \setminus_{dj} S} = E \setminus E_S^{dj}$, where E_S^{dj} is the set of the following directed edges:

1. all edges originated from nodes in S.
2. all edges e from u to v such that there is an edge e' from some node in S to v or u.

Theorem 3. *Reliable message transmission from u to v in a radio network $R(V, E, F, c)$ against a k-receiver-and-sender-jamming adversary (resp. k-destroy-jamming adversary) is possible if and only if for any k-node set S, there is a directed path from u to v in the reduced radio network $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ (resp. $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$).*

Proof. The proof is the same as that of Theorem 2. Q.E.D.

In this section, we have studied receiver-only jamming, receiver-and-sender jamming, and destroy-jamming. We will not discuss sender-jamming since a sender-jammer can easily mount receiver-jamming attacks.

5 Achieving reliability against active adversaries

Definition 2. *Let $R(V, E, F, c)$ be a radio network, and $u, v \in V$ be distinct nodes of R. u, v are* k-separable *in R, $k \geq 0$, if there is a node set $W \subset V$ with at most k nodes such that any directed path from u to v goes through at least one node in W. We say that W* separates *u, v.*

We have the following result.

Theorem 4. *The nodes u, v of a radio network R is not $2k$-separable if and only if for all k-node sets $V_1 \subset V$ there is a set S_{V_1} of directed paths from u and v such that for all k-node sets $V_2 \subset V \setminus V_1$, the following conditions hold:*

– *the paths in S_{V_1} are free of nodes in V_1,*
– *there is at least one directed path in S_{V_1} which is free of the nodes in V_2.*

Proof. First consider the case when u, v are not $2k$-seperable. We shall prove that the conditions are satisfied. For any k-node set $V_1 \subset V$, let S_{V_1} be the set of all paths from u to v which are free of nodes in V_1. Now assume that there is one k-node set $V_2 \subset V$ such that all paths in S_{V_1} go through V_2. Then $V_1 \cup V_2$ separates u and v in R. That is u and v are $2k$-separable in R which is a contradiction.

For the converse observe that the conditions on the paths S_{V_1} make it impossible to have a k-node set $V_2 \subset V$ such that $V_1 \cup V_2$ separates u and v. Indeed if there where such a set $V' = V_1 \cup V_2$ to separate u and v then there would be no path in S_{V_1} free of the of V_1 and V_2. Q.E.D.

For a radio network $R(V, E, F, c)$ and a node set $S \subset V$, the reduced radio networks $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$, $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$, and $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$ are defined in Section 4. In the next Theorem, we give a sufficient and necessary condition for achieving reliable communication against a k-active adversary over radio networks.

Theorem 5. *A necessary and sufficient condition for reliable message transmission against a k-rj-active (resp. k-rsj-active and k-dj-active) adversary from u to v is that for any s-node set S ($s < k$), u and v are not $2(k-s)$-separable in the reduced radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$ (resp. $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ and $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$).*

Proof. First assume that for any s-node set S ($s < k$), u and v are not $2(k-s)$-separable in the reduced radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$ (respectively, $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ and $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$). Let $\mathcal{P}$ be the set of all directed paths from u to v. The paths in $\mathcal{P}$ will be used for transmitting messages by u to v. Let m_u be a message selected by u for transmission via these paths. Now apply Theorem 4. For any s-node set S, let V_1 be a $(k-s)$-node set and $\mathcal{P}_{V_1}$ be the set of paths in $\mathcal{P} \cap R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$ (resp. $\mathcal{P} \cap R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ and $\mathcal{P} \cap R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$) which are free of nodes in V_1. Then:

– If the adversary mounts jamming attacks in the s nodes from S and send malicious message from the $k - s$ nodes in V_1, v will receive the same messages m_u via all the paths in $\mathcal{P}_{V_1}$ (since the adversary is bounded to k nodes and $\mathcal{P}_{V_1}$ is free of the nodes in V_1).
– If the adversary mounts jamming attacks in the s nodes from S and send malicious messages from some node outside V_1, there is a set V_2 which contains all these nodes. By the property of $\mathcal{P}$, there will be a directed path $P \in \mathcal{P}_{V_1}$ which is free from the nodes controlled by the adversary. In this case the messages received by v via the paths $\mathcal{P}_{C_1}$ may *not* all be the same, if the adversary is active.

Assuming that v knows the jamming nodes set S, then it follows that v can distinguish the case when the message m_u is corrupted by the adversary from the case when it is not, by testing the messages received via the paths $\mathcal{P}_{V_1}$, for the s-node set S and each $(k-s)$-node set V_1. However, an active adversary may try to control a node w in such a way that it will jam on some frequencies available to w and send malicious messages on other available frequencies to w. An active adversary could also send out malicious

message no matter it has been receiver-jammed or not. Thus, the node v generally cannot learn from the received messages which set is the S. To achieve reliability, u sends to v via the paths $\mathcal{P}_{V_1}$ the message m_u labeled by (S, V_1), for each s-node set S and each $(k-s)$-node set V_1. v checks the messages received via the paths in $\mathcal{P}_{V_1}$, for each label (S, V_1). After receiving all these messages, v recover the message according the the following rules: First, for the 0-node set $S = \emptyset$ and each k-node set V_1, v tries to recover the message from the messages received from the paths in $\mathcal{P}_{V_1}$. If v succeeds then v outputs the message. Otherwise, for each possible 1-node set S (possible jammers) and each $(k-1)$-node set V_1, v tries to recover the message from the messages received from the paths in $\mathcal{P}_{V_1}$. If v succeeds, then v outputs the message. v repeat the above steps until v finds the message. ¿From our discussion above, v will find the correct the message with 100%-reliability.

Next assume that there exists an s-node set S ($s < k$) such that u and v can be separated by a $2(k-s)$-node set W in the reduced radio network $R(V \setminus S, E_{V \setminus_{rj} S}, F, c)$ (resp. $R(V \setminus S, E_{V \setminus_{rsj} S}, F, c)$ and $R(V \setminus S, E_{V \setminus_{dj} S}, F, c)$). Suppose that π is a message transmission protocol from u to v and let $W = W_0 \cup W_1$ be a $2(k-s)$-node separation of u and v with W_0 and W_1 each having at most $k-s$ nodes. Let m_0 be the message that u transmits. The adversary will attempt to maintain a simulation of the possible behavior of u by executing π for message $m_1 \neq m_0$. In addition to controlling the nodes in S, the strategy of the adversary is to flip a coin and then, depending on the outcome, decide which set of W_0 or W_1 to control. Let W_b be the chosen set. In each execution step of the transmission protocol, the adversary sends receiver-jamming (resp. receiver-and-sender jamming and destroy-jamming) messages on all nodes in S and causes each node in W_b to follow the protocol π as if the protocol were transmitting the message m_1. This simulation will succeeds with nonzero probability. Since v does not know whether $b = 0$ or $b = 1$, at the end of the protocol v cannot decide whether u has transmitted m_0 or m_1 if the adversary succeeds. Thus with nonzero probability, the reliability is not achieved. Q.E.D.

6 Achieving reliability and perfect privacy against active adversaries

Theorem 6. *Reliable and perfect private message transmission from u to v in a radio network $R(V, E, F, c)$ against a k-rj-active (resp. k-rsj-active and k-dj-active) adversary is possible if for any k-node set S, reliable message transmission against a k-rj-active (resp. k-rsj-active and k-dj-active) adversary is possible in the reduced radio network $R(V \setminus S, E_{V \setminus_p S}, F, c)$, where $E_{V \setminus_p S} = E \setminus E_S^p$ and E_S^p is the set of the following directed edges:*

1. *all edges going to nodes in S.*
2. *all edges e from u to v such that there is an edge e' from u to some node in S and $c(e) = c(e')$.*

Proof. Let $\Gamma = \{S_1, \ldots, S_t\}$ be a list of all k-node subsets of V and m^u be the message that u wants to send to v. u constructs a t-out-of-t secret sharing scheme $(s_1^u, \ldots, s_t^u)$ of m^u. For each $i \leq t$, u reliably sends s_i^u to v via the reduced radio

network $R(V \setminus S_i, E_{V \setminus_p S_i}, F, c)$. For each $i \leq t$, v reliably receives s_i^v on the reduced radio network $R(V \setminus S_i, E_{V \setminus_p S_i}, F, c)$. Now assume that the adversary control all nodes in S_{i_0}, then the adversary will learn no information about $s_{s_0}^u$. Thus the above protocol is perfectly private. It suffices to show that the above protocol is reliable. It is straightforward to show that v reliably receives all correct shares $(s_1^v, \ldots, s_t^v) = (s_1^u, \ldots, s_t^u)$. Thus the above protocol is $(0, 0)$-secure. Q.E.D.

7 Probabilistically reliable and perfectly private message transmission in certain radio networks

In this section, we briefly discuss the possibility of migrating Franklin and Wright's [13] message transmission protocol from neighbor networks to radio networks. Many radio networks have the property that each station can use all available frequencies to him/her both to receive messages and to multicast messages. We call such kind of radio networks *bi-directional radio networks*. Two nodes u and v in a bi-directional radio network $R(V, E, F, c)$ is *weakly (n, k)-connected* if there are n paths $p_1, \ldots, p_n$ between u and v such that for any k-node set $S \subset V$, there exists a path p_i such that there is neither edge from a node in S to a node on P_i nor edge from a node on p_i to a node in S.

Theorem 7. *If two nodes u and v in a bi-directional radio network $R(V, E, F, c)$ is weakly (n, k)-connected for some $n > k$, then there is an efficient probabilistically reliable and perfectly private message transmission between u and v.*

Proof. The proof is the same as that for the corresponding result in neighbor networks by Wang and Desmedt [20]. Q.E.D.

A similar example as in Desmedt and Wang [7] can be used to show that weak (n, k)-connectivity is not a necessary condition for achieving probabilistically reliable and perfectly private message transmissions in bi-directional radio networks. Also, similar example as in Desmedt and Wang [7] shows that there is a radio network where probabilistically reliable message transmission is possible though private message transmission is impossible.

8 Minimizing the number of frequencies in certain radio networks

In this section, we study a specific case of radio networks initially studied in [6]. Let $F = \{f_1, \ldots, f_m\}$, and $\mathcal{B} = \{B_1, \ldots, B_n\}$ where $B_i \subseteq F$. Assume that there are n participants, and each participants p_i is given a set of frequency set B_i. Each participant is able to send messages with any frequency $f_j \in B_i$, and each participant who has the same frequency will receive the message. This scenario can be described by the radio network $R(V, E, F, c)$ as follows: Let $V = \{p_1, \ldots, p_n\}$, $F = \cup_i B_i$, $E = \cup_i \{(p_i, p_j)_f : f \in B_i \cap B_j, i \neq j\}$, and $c((p_i, p_j)_f) = f$.

By using Theorem 2, we derive a sufficient and necessary condition for robust frequency broadcast systems against receiver-jammers. We first introduce some notations. Let $F = \{f_1, \ldots, f_m\}$, and $\mathcal{B} = \{B_1, \ldots, B_n\}$ where $B_i \subseteq F$.

- A system $(F, \mathcal{B})$ is called a *cover free family* $CFF(m, n, k)$ [11] if for any distinct $i, i_1, \ldots, i_k \leq n$, we have $B_i \not\subseteq (B_{i_1} \cup \ldots \cup B_{i_k})$.
- A system $(F, \mathcal{B})$ is called a *key distribution pattern* [17] $KDP(m, n, k)$ if for any $i_1, \ldots, i_k \leq n$ and $i, j \leq n$ (i, j are different from $i_1, \ldots, i_k$), we have $(B_i \cap B_j) \not\subseteq (B_{i_1} \cup \ldots \cup B_{i_k})$.
- A system $(F, \mathcal{B})$ is called a *semi key distribution pattern* $SKDP(m, n, k)$ if for any $i_1, \ldots, i_k \leq n$ and $i, j \leq n$ (i, j are different from $i_1, \ldots, i_k$), at least one of the following conditions holds:
  1. $(B_i \cap B_j) \not\subseteq (B_{i_1} \cup \ldots \cup B_{i_k})$,
  2. there exist $s_1, \ldots, s_t$ for some $t \leq n-2$ such that $(B_i \cap B_{s_1}) \not\subseteq (B_{i_1} \cup \ldots \cup B_{i_k})$, $\ldots$, $(B_{s_t} \cap B_j) \not\subseteq (B_{i_1} \cup \ldots \cup B_{i_k})$

Obviously a $KDP(m, n, k)$ is a $SKDP(m, n, k)$, and a $SKDP(m, n, k)$ is a $CFF(m, n, k)$.

Theorem 8. *Let $V = \{p_1, \ldots, p_n\}$ be the participant set, $F = \{f_1, \ldots, f_m\}$ be the frequency set, and $B_i \subset F$ be the frequency set assigned to the participant p_i. Then any two participants can communicate reliably in the presence of a k-receiver-jamming adversary if and only if the system $(F, \mathcal{B})$ is a semi key distribution pattern $SKDP(m, n, k)$.*

Proof. This follows from Theorem 2 and the above definitions. Q.E.D.

For practical efficient designs, we may be interested in minimizing the number of frequencies to be used while maximizing the possible number k of jammers. For any given n and k, let

- $CFF(n, k)$ denote the minimal m such that a $CFF(m, n, k)$ exists,
- $SKDP(n, k)$ denote the minimal m such that a $SKDP(m, n, k)$ exists,
- $KDP(n, k)$ denote the minimal m such that a $KDP(m, n, k)$ exists.

From [11] and [19] we know that for any given k, there exist an integer c_1 such that $c_1 \log n \leq CFF(n, k)$, and an integer c_2 such that $KDP(n, k) \leq c_2 \log n$. That is, for a given k there exist integers c_1 and c_2 such that the following inequalities hold.

$$c_1 \log n \leq CFF(n, k) \leq SKDP(n, k) \leq KDP(n, k) \leq c_2 \log n.$$

Thus it shows that there exists an infinite family of radio networks with reliable communication against receiver-jamming adversary, requiring only $O(\log n)$ frequencies for n participants (nodes). We can even give constructions of SKDP with the asymptotically optimal number of frequencies if the network topology can be designed as desired (e.g a complete network in [6]). An interesting question is: if the network topology is fixed and given, how can we design the corresponding SKDP such that the number frequencies is as small as possible? We don't know to to do it, and it seems to be a difficult problem.

9 Conclusion and open problems

In this paper, we have established necessary and sufficient conditions for reliable message transmissions against jamming adversaries and active adversaries. It is easy to show that it is **NP**-hard to check whether these conditions hold for a radio network, and most of our protocols for the sufficient condition has exponential bit-complexity in the size of the radio network. A more general and natural problem is: does there exist more efficient reliable message transmission protocols when the sufficient condition is met?

References

1. N. Alon, A. Bar-Noy, N. Linial, and D. Peleg. On the complexity of radio communication. In *Proceedings of ACM STOC 1989*, pages 274–285.
2. M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computing. In: *Proc. ACM STOC, '88*, pages 1–10, ACM Press, 1988.
3. C. Berge. *Hypergraphs: Combinatorics of finite sets*. Translated from the French. North-Holland Mathematical Library 45, 1989.
4. D. Bertsekas and R. Gallager. *Data Networks*. Prentice-Hall, Inc., 1992.
5. D. Chaum, C. Crepeau, and I. Damgard. Multiparty unconditional secure protocols. In: *Proc. ACM STOC '88*, pages 11–19, ACM Press, 1988.
6. Y. Desmedt, R. Safavi-Naini, H. Wang, L.M. Batten, C. Charnes and J. Pieprzyk. Broadcast anti-jamming systems. *Computer Networks*, **35**(2-3): 223-236, 2001.
7. Y. Desmedt and Y. Wang. Perfectly secure message transmission revisited. In *Proc. EuroCrypt'02*, pages 502-517. Lecture Notes in Computer Science 2332, Springer-Verlag.
8. Y. Desmedt, Y. Wang, and M. Burmester. A critical analysis of models for fault-tolerant and secure computation. In: *Proc. Comm., Network, and Info. Security*, 2003, pages 147-152.
9. D. Dolev. The Byzantine generals strike again. *J. of Algorithms*, **3**:14–30, 1982.
10. D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *J. of the ACM*, **40**(1):17–47, 1993.
11. P. Erdös, P. Frankl, and Z. Furedi. Families of finite sets in which no set is covered by the union of r others. *Israel Journal of Mathematics*. **51**:79-89, 1985.
12. L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In: *Proc. 9th ACM Conference on Computer and Communication Security*, pages 41–47, 2002.
13. M. Franklin and R. Wright. Secure communication in minimal connectivity models. *Journal of Cryptology*, **13**(1):9–30, 2000.
14. M. Franklin and M. Yung. Secure hypergraphs: privacy from partial broadcast. In: *Proc. ACM STOC '95*, pages 36–44, ACM Press, 1995.
15. O. Goldreich, S. Goldwasser, and N. Linial. Fault-tolerant computation in the full information model. *SIAM J. Comput.* **27**(2):506–544, 1998.
16. V. Hadzilacos. *Issues of Fault Tolerance in Concurrent Computations*. PhD thesis, Harvard University, Cambridge, MA, 1984.
17. C. J. Mitchell and F. C. Piper. Key Storage in Secure Networks. *Discrete Applied Mathematics.* **21**: 215-228, 1988.
18. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In: *Proc. ACM STOC '89*, pages 73–85, ACM Press, 1989.
19. D. R. Stinson, T. van Trung and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plan. Infer.* **86**:595-617, 2000.
20. Y. Wang and Y. Desmedt. Secure communication in multicast channels: the answer to Franklin and Wright's question. *J. of Cryptology*, **14**(2):121–135, 2001.