J. Cryptol. (2008) 21: 250–279
DOI: 10.1007/s00145-007-9018-2

Journal of
CRYPTOLOGY

Probabilistic Reliability and Privacy of Communication Using Multicast in General Neighbor Networks

Jérôme Renault

CEREMADE, Université Paris Dauphine, Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France
renault@ceremade.dauphine.fr

Tristan Tomala

HEC, 78351 Jouy-en-Josas Cedex, France
tomala@hec.fr

Communicated by Stefan Wolf

Received 27 June 2005 and revised 7 August 2007
Online publication 16 October 2007

Abstract. This paper studies reliability and security of information transmission in networks. We consider the framework of Franklin and Wright (J. Cryptol. 13(1):9–30, 2000): multicast communication and byzantine adversary. Franklin and Wright studied particular neighbor graphs with *neighbor-disjoint* paths. The aim of the present work is to drop this assumption and to give necessary and sufficient conditions on the neighbor graph allowing reliable and secure information transmission.

Key words. Communication networks, Graphs, Security, Multicast, Repeated games, Incomplete information.

1. Introduction

We study how players can reliably and securely exchange information: player a (the sender) wants to send a message to player b (the receiver) reliably, i.e. b gets the correct message, and securely, i.e. the content of the message is known to a and b only. If players a and b are connected by a private and authenticated channel, this is possible. In many situations, players a and b are distant nodes in a network where some players are possibly byzantine. Secure communication in networks has been studied in many papers. A widely investigated communication method is the *unicast* one where players can send different messages to different neighbors. Refs. [6,7] study the possibility of perfectly secure message transmission, i.e. the correct message is transmitted with certainty, and relate this possibility to the connectivity of the graph. Other papers study probabilistic reliability, i.e. the correct message is transmitted with high probability. Refs. [2,3] study this notion and show how the use of private authentication keys reduces the required connectivity of the graph. Ref. [13] characterizes the possibility

of probabilistic reliability for directed graphs and a general class of adversaries. The relationship between the present work and unicast results is discussed in the concluding section.

Refs. [9,10] and [5] (among others) have studied reliable and secure communication in *multicast* models. Communication channels are multicast, if whenever a player casts a message, this message is received by *all* its neighbors. Many examples of multicast channels can be found, like a radio broadcast, an Ethernet bus or a token ring. In this setup, Ref. [10] studies secure communication with passive adversaries, Ref. [9] treats the case of byzantine adversaries and Ref. [5] studies the efficiency of protocols in Ref.'s [9] model.

Another motivation for the study of multicast models comes from game theory. Given a neighbor graph on a set of players, one defines a dynamic game as follows. The game proceeds in rounds. At each round, each player has to choose an action, the choices being synchronous. Before proceeding to the next round, each player observes the actions chosen by his neighbors: the graph is a *monitoring network*. At each round, a player gets a reward—or payoff—depending on all actions chosen and his aim is to get a large average payoff (over time). The typical solution concept is the Nash equilibrium: a specification of the strategies, such that no player can increase his payoff by unilateral deviation. In the case of the complete graph, called the *perfect monitoring case*, the characterization of Nash equilibria is well-known, this is the Folk Theorem, due to Aumann and Shapley in the 70's (see the re-edition Ref. [1]). To construct an equilibrium, one establishes a *contract* specifying the actions to be actually played. If a player deviates from the contract, all his neighbors (i.e. all the players when the graph is complete) observe it and coordinate to punish him. Games with *imperfect monitoring* have received a lot of attention in the game-theoretic literature. Refs. [4,11] consider the case of a non-complete monitoring graph. In such a model, only the neighbors of the deviating player are aware of the deviation. Ref. [11] uses then the monitoring graph as a communication graph, i.e. the neighbors of the deviating players use their actions as messages to signal to other players that a deviation from the contract occurred. A strategy specification can then be formally identified with a communication protocol and the multicast assumption is a consequence of the monitoring structure. Ref. [11] studies the existence of a communication protocol such that, under any deviation from the contract, each non-deviating player outputs with certainty the name of the deviating player, and prove that such a protocol exists if and only if the graph is 2-connected. In a slightly more general model of games, in addition to this description, some players know the value of a payoff-relevant parameter called the state variable, and may wish to transmit this value reliably and securely to uninformed players: since the contract may depend on the state, it is important that players agree on the state value. This is deeply related to reliable and secure communication and Ref. [12] shows how the possibility of reliable and secure information transmission relates to the construction of Nash equilibria.

The present work is placed in Ref.'s [9] setup. Ref. [9] characterizes the possibility of reliable and secure communication in neighbor graphs with neighbor-disjoint paths and prove that reliable and secure information transmission is possible if and only if the number of paths from the sender to the receiver exceeds the number of faulty players. The aim of the present paper is to extend this characterization to general neighbor graphs. In Ref. [12], we treated this problem for one faulty player only, which is the im-

portant case for the study of Nash equilibria. The present paper thus also extends some of Ref.'s [12] results.

In the model we consider, communications takes places in rounds and is synchronous. The adversary is byzantine: given a number of players t, the adversary takes control of a coalition of t nodes and chooses their messages at will. The case of specific faults (passive, fail/stop), is not considered here, see Ref. [13] for more general adversary models in the unicast case. To characterize reliability we follow the same route as e.g. Ref. [2]: for every pair (T, T') of candidates for the set of bad parties, we characterize (T, T')-reliability, that is reliability when the adversary controls either T of T'. We deduce then the general characterization.

We describe formally the model and the notions of reliability and security in Sect. 2. In Sect. 3, we study reliability. We first state the characterization then prove that the conditions are sufficient and necessary. The protocol constructions blend those of Refs. [9] and [11,12]. The proof that the conditions are necessary is quite involved so we first prove it on an example and appendicize the general proof. Section 4 is devoted to security. The protocol constructions generalize those found in Ref. [9]. We provide concluding remarks in Sect. 5. The appendix contains the general proof of the necessity part of Theorem 3.10.

2. The Communication Model

Let $G = (V, E)$ be an undirected graph with a finite set of nodes (or players) V and set of edges $E \subset V \times V$. For each i in V we let $G(i)$ be the set of players who are directly connected to i including i himself:

$$G(i) = \{j \in V, (i, j) \in E\} \cup \{i\}.$$

We fix once and for all G and two distinct nodes in V: a (the sender) and b (the receiver). The aim of communication is to transmit a message from a to b. This message will be henceforth called a *state*. This variable has two possible values ω and ω' and we let $\Omega = \{\omega, \omega'\}$. Initially the value of the state is known to a but not to b.

We consider multicast communication. When a node sends or multicasts a message, all its neighbors in the graph hear it, only these neighbors hear it, and the correct value of the message is received by each neighbor. In other words, a player cannot eavesdrop on a line to which he does not belong nor can he falsify the messages on this line.

Communication takes place in rounds and is synchronous. At each round, each player sends the same message to all his neighbors. The message sent by a player at a given round depends on the previous messages sent by him, the previous messages sent by his neighbors and the random input of this player. For player a, his messages also depend on the actual value of the state. A communication protocol is a specification of a space of messages, of the way players send messages, of the number of rounds and of the output produced by player b at the last round.

We give now a formal definition of a protocol using the game theoretic language. We choose a finite message space M, common to all players. At round 1, each player chooses a message in M and multicasts it. At round $r > 1$, each player reads his new messages and according to his history of messages, chooses the message to send at round r. For each node i, we let H_r^i be the set of messages received and sent by player i up to round r: $H_r^i = (M^{G(i)})^r$.

A protocol then specifies how players choose their messages according to their observations.

Definition 2.1.

- If $i \neq a$, a *pure strategy* for player i is a deterministic way of choosing his new message according to previous messages, i.e. it is a mapping σ^i from the set of all finite histories of messages $H^i = \bigcup_{r\geq 0} H^i_r$ to M which prescribes after each history, the next message to be multicast by player i.
- A *mixed strategy* for player $i \neq a$ is the random choice of a pure strategy: this is just a probability distribution over the set of pure strategies.
- A *behavioral strategy* for player i is a probabilistic way of choosing his new message according to previous messages, i.e. it is a mapping σ^i from $H^i = \bigcup_{r\geq 0} H^i_r$ to the set of probability distributions on M which prescribes after each history, the coin flip used by player i to choose his next message.
- Since player a knows the value of the state, his behavior is described by a pair of strategies (pure, mixed or behavioral) $\sigma^a = (\sigma^a_\omega, \sigma^a_{\omega'})$ where σ^a_ω (resp. $\sigma^a_{\omega'}$) is the strategy used by a if the state is ω (resp. ω').

Remark 2.2. These definitions concern how players use random strings. A player using a pure strategy flips no coins. Put in another way, a pure strategy is a deterministic rule of behavior used by the player, given his random inputs.

Mixed and behavioral strategies are two ways of modelling the way players generate their random inputs. The traditional model in the cryptography literature is that each player chooses a random string before the start of the protocol and lets the messages he sends depend on it. This means that the player chooses randomly an element s from a set S equipped with a probability measure μ, and then uses a pure strategy σ^i_s depending on s. Equivalently, player i may as well choose a pure strategy at random, the probability of choosing σ^i being set as $\sum_{s:\sigma^i_s=\sigma^i} \mu(s)$. This is formally equivalent to a mixed strategy, i.e. a probability distribution on the set of pure strategies.

A player using a behavioral strategy chooses a fresh random string at the beginning of each round and uses it just at this round. It is obvious that this can be represented by a mixed strategy: the player just has to choose all the local random strings at the beginning. Conversely, the choice of an initial random string can always be decomposed as the sequence of choices of local strings provided that the player has *perfect memory*, i.e. always recalls past messages. This is known as Kuhn's theorem [8]. These alternative representations will be useful in proofs: whenever it is convenient, we shall either assume that players perform randomizations before the first round or locally at each round.

In the following, the term strategy shall be used to mean either a mixed or a behavioral strategy (except when indicated). A protocol specifies a strategy for each player.

To complete the definition of a protocol, we specify the number R of rounds and the condition under which b outputs ω. This is defined by a subset D of H^b_R: player b outputs ω if he observes a history of messages which belongs to D and outputs ω' otherwise. To sum up, we give the definition:

Definition 2.3. A communication protocol π is given by:

- A finite set M, the message space.
- A positive integer R, the total number of rounds.
- A vector of strategies $\sigma = (\sigma^i)_{i \in V}$.
- A subset D of H_R^b.

We model now the adversary. Let t be a fixed integer between 0 and $|V| - 2$, where $|V|$ stands for the cardinality of V. The adversary takes control of a subset $T \subset V \backslash \{a, b\}$ with at most t nodes. The adversary knows the messages sent, the messages received and the random inputs for each node in T, and controls the randomizations and the messages multicast by these nodes. Such a byzantine adversary can also be modelled by strategies.

A history for the adversary after round r is the list of all messages received and sent by all players in T. This is thus an element of $H_r^T = (M^{G(T)})^r$, with $G(T) = \bigcup_{i \in T} G(i)$. A strategy τ^T for the adversary specifies after each such history a vectors of messages $(m^i)_{i \in T}$, i.e. if the adversary selects $(m^i)_{i \in T}$ and each player $i \in T$ multicasts m^i. As above, the adversary might use a mixed or a behavioral strategy: the adversary might choose a random string at the beginning or perform local randomizations at each stage. While randomizations performed by non-faulty players are (probabilistically) independent, the adversary is allowed to choose the random inputs of the faulty players in a correlative way (see one of the concluding remarks in Sect. 5).

We assume that the adversary knows the whole specification of the protocol but that other players do not know which players are adversarial and which strategy the adversary is using.

Let $H = (M^V)^R$ be the set of total histories of the communication protocol. The actual state ω, the protocol π and the strategy of the adversary τ^T define, through the random inputs used be the strategies, a probability distribution on H which we denote by $\mathbf{P}_{\omega,\pi,\tau^T}$. We define now the notion of reliability following e.g. Franklin and Wright [9] (see also [2]).

Definition 2.4. A protocol is ε-reliable if, when the adversary controls any set $T \subset V \backslash \{a, b\}$ of at most t players, the probability that b outputs ω (resp. ω') given that a transmitted ω (resp. ω') is at least $1 - \varepsilon$.

In other words, the protocol $\pi = (M, R, \sigma, D)$ is ε-reliable if for every $T \subset V \backslash \{a, b\}$ with at most t nodes and every strategy τ^T:

$$\mathbf{P}_{\omega,\pi,\tau^T}(D) \geq 1 - \varepsilon, \qquad \mathbf{P}_{\omega',\pi,\tau^T}(D) \leq \varepsilon.$$

The possibility of communication from a to b clearly depends on: the graph G, the positions of a and b in the graph and the maximal number of faulty nodes t.

Definition 2.5. The communication from a to b in G given t is reliable (in short, $\langle G, a, b, t \rangle$ is reliable) if for every $\varepsilon > 0$, there is an ε-reliable protocol π.

Following again [9], we define security by the fact that reliable communication is possible without the adversary knowing the actual state. Let π be a protocol, T be the set of faulty nodes and τ^T be the strategy of the adversary.

Definition 2.6. A protocol π is ε-private if for every $T \subset V\backslash\{a,b\}$ with $|T| \leq t$ and every strategy τ^T of the adversary,

$$\sum_{h \in H^T} |\mathbf{P}_{\omega,\pi,\tau^T}(h) - \mathbf{P}_{\omega',\pi,\tau^T}(h)| \leq \varepsilon.$$

That is, if we let $\mathbf{P}^T_{\omega,\pi,\tau^T}$ be the marginal distribution of $\mathbf{P}_{\omega,\pi,\tau^T}$ on H^T_R, $\|\mathbf{P}^T_{\omega,\pi,\tau^T} - \mathbf{P}^T_{\omega',\pi,\tau^T}\|_1 \leq \varepsilon$, where $\|\cdot\|_1$ is the L_1 norm: $\|p-q\|_1 = \sum_x |p(x)-q(x)|$.

Definition 2.7. $\langle G,a,b,t\rangle$ is secure if for every $\varepsilon > 0$, there is a protocol π which is ε-reliable and ε-private.

Remark 2.8. In the definitions of reliability and security, the condition $\varepsilon > 0$ cannot be replaced by $\varepsilon \geq 0$ without affecting the results, see [9] for a discussion of perfect reliability *vs* almost perfect reliability.

3. Reliability

The receiver does not know the value of the state but is aware that the adversary may control a subset of at most t players. Player b thus has to test the hypothesis {ω is the state and T is the set of faulty players} against {ω' is the state and T' is the set of faulty players}, for all pairs of subsets T and T' with at most t players. We argue now that if b can discriminate these two hypothesis for all pairs T and T', then $\langle G,a,b,t\rangle$ is reliable. A similar reasoning is already met in the literature, see e.g. [2].

Definition 3.1. Let $T, T' \subset V\backslash\{a,b\}$. A protocol is ε-(T,T')-reliable if, when a transmits ω and the adversary controls T, b outputs ω with probability at least $1-\varepsilon$, and when a transmits ω' and the adversary controls T', b outputs ω' with probability at least $1-\varepsilon$.

That is, the protocol π is ε-(T,T')-reliable if for every pair of strategies $(\tau^T, \bar{\tau}^{T'})$,

$$\mathbf{P}_{\omega,\pi,\tau^T}(D) \geq 1-\varepsilon, \qquad \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D) \leq \varepsilon.$$

We say that $\langle G,a,b\rangle$ is (T,T')-reliable if for every $\varepsilon > 0$, there exists a protocol π which is ε-(T,T')-reliable.

Lemma 3.2. *$\langle G,a,b,t\rangle$ is reliable if and only if $\langle G,a,b\rangle$ is (T,T')-reliable for every $T, T' \subset V\backslash\{a,b\}$ with $|T|, |T'| \leq t$.*

Proof. The *only if* part being clear, we only prove the *if* part. Assume that $\langle G,a,b\rangle$ is (T,T')-reliable for every $T, T' \subset V\backslash\{a,b\}$ with $|T|, |T'| \leq t$ and fix $\varepsilon > 0$. We choose an enumeration of the pairs (T,T') of subsets of $V\backslash\{a,b\}$ with $|T|, |T'| \leq t$: $(T_1,T'_1), (T_2,T'_2), \ldots, (T_K,T'_K)$. For each k, $\langle G,a,b\rangle$ is (T_k,T'_k)-reliable so by Definition 3.1 there exists a protocol $\pi_k = (M_k, R_k, \sigma_k, D_k)$ which is ε-(T_k,T'_k)-reliable.

We construct a protocol $\pi = (M, R, \sigma, D)$ by playing the protocols π_k one after the other: use σ_1 for the first R_1 rounds, σ_2 for the next R_2 rounds and so on until σ_K is used for R_K rounds. The set of messages M is $M_1 \cup \cdots \cup M_K$ and the total number of rounds is $R = R_1 + \cdots + R_K$.

Then b outputs ω in π if there exists an instance of the adversary $\overline{T}$ such that b outputs ω from each protocol π_k with $T_k = \overline{T}$. That is, we let D be the set of histories in H_R^b such that: there exists $\overline{T} \subset V\backslash\{a, b\}$ with $|\overline{T}| \leq t$, s. t. for all (T_k, T_k') with $T_k = \overline{T}$, the messages received by b from π_k belong to D_k.

Fix now $T \subset V\backslash\{a, b\}$ with $|T| \leq t$ and assume that the adversary controls the players in T and uses the strategy τ^T. Assume that the state is ω. For each k such that $T_k = T$, b outputs ω from π_k with probability at least $1 - \varepsilon$, so $\mathbf{P}_{\omega,\pi,\tau^T}(D) \geq (1 - \varepsilon)^L$, where $L = \sqrt{K}$ is the number of subsets of $V\backslash\{a, b\}$ of cardinal at most t. Assume now that the state is ω'. For $\overline{T} \subset V\backslash\{a, b\}$ with $|\overline{T}| \leq t$, b outputs ω from π_k with k s.t. $(T_k, T_k') = (\overline{T}, T)$, with probability at most ε. As this holds for every such $\overline{T}$, the probability that b outputs ω from π is at most $L\varepsilon$: i.e. $\mathbf{P}_{\omega',\pi,\tau^T}(D) \leq L\varepsilon$. Since $L\varepsilon \geq 1 - (1 - \varepsilon)^L$, π is $L\varepsilon$-reliable. To construct an η-reliable protocol we just have to choose $\varepsilon = \eta/L$. □

Fixing T, T', we characterize now (T, T')-reliability.

Definition 3.3.

- A path c in the graph G is a finite sequence $c = (c_1, \ldots, c_n)$ such that for each $l = 1, \ldots, n-1$, $(c_l, c_{l+1}) \in E$.
- Given $i, j \in V$, we say that c is a path from i to j if $c_1 = i$ and $c_n = j$.
- If S is a subset of V, we say that c is a path in S and we write $c \subset S$ if for each $l = 1, \ldots, n$, $c_l \in S$.
- We denote $\{c_1, \ldots, c_n\} \cap S$ by $c \cap S$ and say that c goes through S if $c \cap S \neq \emptyset$.

We analyze now simple cases and define simple protocols. We first consider a protocol where a transmits an information to b along a path c from a to b. This protocol is found in [9].

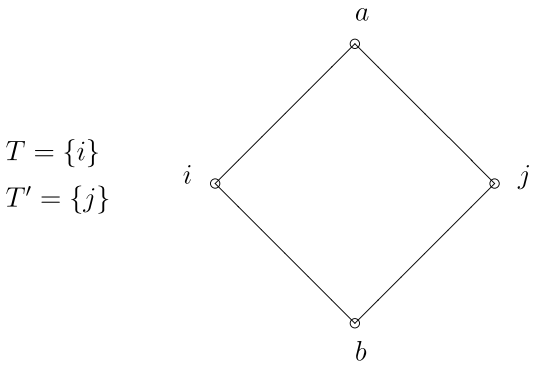
> **Basic propagation protocol.**
> The set of messages M is $\{\omega, \omega'\}$ and the number of rounds R is $n - 1$. The vector of strategies $(\sigma^i)_{i \in V}$ is such that player a transmits the value of the state to player b through the path c : at round 1, player a multicasts the message corresponding to the state, at round 2 player c_2 multicasts the message previously sent by player c_1, and so on until round $n - 1$ where c_{n-1} multicasts the message previously sent by player c_{n-2}.

Lemma 3.4. *If there exists a path $c = (c_1, \ldots, c_n)$ from $a = c_1$ to $b = c_n$ in $V\backslash(T \cup T')$ then the basic propagation protocol is ε-(T, T')-reliable and thus $\langle G, a, b\rangle$ is (T, T')-reliable.*

Proof. If $c \subset V\backslash(T \cup T')$, no player in T or T' can prevent this information transmission: for each pair $(\tau^T, \bar{\tau}^{T'})$, b outputs ω with probability one under (ω, π, τ^T) and with probability zero under $(\omega', \pi, \bar{\tau}^{T'})$. □

The following example was first studied in [9] and was rediscovered independently in [12]. Consider the following graph with $T = \{i\}$ and $T' = \{j\}$.

Example 3.5.



There exist no path from a to b in $V \setminus (T \cup T')$, how can player a send the state to the receiver?

First note that the "naive" protocol where a announces the state and i, j are supposed to repeat it, is not reliable. If i announces that the state is ω' and j announces that the state is ω, there is no way for the receiver to decide whether {the state is ω and the adversary controls i} or {the state is ω' and the adversary controls j}. Still, $\langle G, a, b\rangle$ is (T, T')-reliable, which is shown by the following protocol, see [9,12].

Simple reliable transmission protocol (Example 3.5).
M is a large set, with m_0 in M being fixed, and there are $R = 3$ rounds.

- At round 1, player i chooses a message $\hat{m}$ in M uniformly and multicasts it. Players a and b are thus informed of $\hat{m}$ (unlike player j).
- At round 2, player a repeats the message $\hat{m}$ if the state is ω or multicasts the message m_0 if the state is ω'. Denote by $\bar{m}$ in $\{\hat{m}, m_0\}$ the message multicast by player a at round 2. $\bar{m}$ is received by players i and j.
- At round 3, player j multicasts the message $\bar{m}$.

At the end of round 3, player b knows the value of $\hat{m}$, and the message m sent by player j at round 3. Player b outputs ω if $m = \hat{m}$, so we let D be the set of histories for the receiver such that $m = \hat{m}$.

Remark that at round 1, the same message $\hat{m}$ is received by a and b even if i is byzantine. Sending no message at round 1 is not an option for a byzantine player i in our setup (this is without loss of generality if one specifies a blank message in M meaning "no message").

Lemma 3.6. *In the situation of Example 3.5, the simple reliable transmission protocol is ε-(T, T')-reliable and thus $\langle G, a, b\rangle$ is (T, T')-reliable.*

Proof. If the adversary controls $T = \{i\}$ he can only manipulate the value of $\hat{m}$, so if the state is ω, m and $\hat{m}$ coincide: $\mathbf{P}_{\omega,\pi,\tau^T}(D) = 1$ for each strategy τ^T. Assume now that the state is ω' and that the adversary controls $T' = \{j\}$. Player a sends m_0 at round 2 so m is (probabilistically) independent from $\hat{m}$. Since $\hat{m}$ is uniformly distributed, $\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D) = 1/|M|$, which is small enough if $|M|$ is large, so $\langle G, a, b\rangle$ is (T, T')-reliable. Remark then that $\langle G, a, b, 1\rangle$ is reliable. □

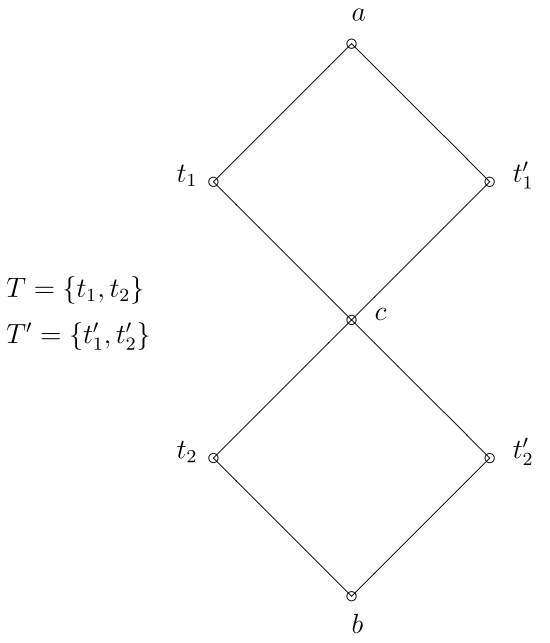
The analysis of these two simple cases leads to the following definition.

Definition 3.7. Let $\Gamma_{T,T'}$ be the symmetric binary relation on $V\backslash(T \cup T')$ defined as follows: $\Gamma_{T,T'}(i, j)$ holds if and only if at least one of the two following conditions (1) and (2) is satisfied:

(1) There is a path c in G from i to j such that $c \subset V\backslash(T \cup T')$,
(2) There is a pair of paths c, c' from i to j in G such that both (i) and (ii) hold:
  (i) $c \subset V\backslash T'$ and $c' \subset V\backslash T$,
  (ii) ($c \cap T$ is a singleton $\{k\}$ such that $k \notin G(T')$) or ($c' \cap T'$ is a singleton $\{k'\}$ such that $k' \notin G(T)$).

The next example shows that $\Gamma_{T,T'}$ may not be transitive.

Example 3.8.



One easily checks that $\Gamma_{T,T'}(a, b)$ does not hold but both $\Gamma_{T,T'}(a, c)$ and $\Gamma_{T,T'}(c, b)$ hold. Here $\langle G, a, b\rangle$ is (T, T')-reliable since an ε-reliable protocol is constructed as

follows: a transmits the value of the state $\frac{\varepsilon}{2}$-reliably to c using the simple reliable transmission protocol and then c transmits the value of the state to $\frac{\varepsilon}{2}$-reliably to b using another instance of the simple reliable transmission protocol.

This example shows the need to iterate the relation $\Gamma_{T,T'}$ and leads to defining the relation $C_{T,T'}$ as the transitive closure of $\Gamma_{T,T'}$.

Definition 3.9. Let $C_{T,T'}(a)$ be the connected component of a in the graph defined by the relation $\Gamma_{T,T'}$ i.e. the set of players $c \in V\backslash(T \cup T')$ such that there exists a sequence $(i_1, \ldots, i_n)$ in $V\backslash(T \cup T')$ satisfying $i_1 = a$, $i_n = c$ and for each k, $\Gamma_{T,T'}(i_k, i_{k+1})$ holds.

Theorem 3.10. *Let $T, T' \subset V\backslash\{a, b\}$. $\langle G, a, b\rangle$ is (T, T')-reliable if and only if $b \in C_{T,T'}(a)$.*

The remainder of this section is devoted to the proof of this theorem. The ideas of the "if" part have already been encountered in the examples studied. The "only if" part expresses the fact that these examples contain all possibilities for reliability. The proof of this part is involved. An illustrative example is given in Sect. 3.2 and the general proof is in the last section of the paper. Using Lemma 3.2, the following corollary of Theorem 3.10 is immediate.

Corollary 3.11. *$\langle G, a, b, t\rangle$ is reliable if and only if for each pair of subsets $T, T' \subset V\backslash\{a, b\}$ with $|T|, |T'| \leq t$, $b \in C_{T,T'}(a)$.*

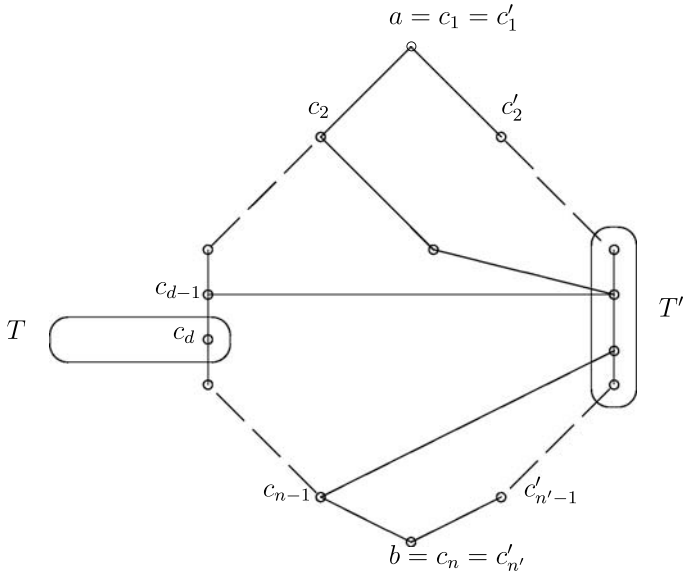
Remark 3.12. Reliability is only defined for transmission of binary information. Since any finite message can be encoded into a finite string of symbols ω, ω', it can be transmitted reliably by using a reliable protocol for each digit of the string. This will be used explicitly in the construction of the *secure* protocol.

3.1. *The ε-Reliable Protocol*

We assume that $b \in C_{T,T'}(a)$. Given $\varepsilon > 0$, we construct a protocol $\pi = (M, R, \sigma, D)$ such that for each pair $(\tau^T, \bar{\tau}^T)$, $\mathbf{P}_{\omega,\pi,\tau^T}(D) \geq 1 - \varepsilon$ and $\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D) \leq \varepsilon$. We first consider the particular case where $\Gamma_{T,T'}(a, b)$ holds and then study the general case.

A. Assume that $\Gamma_{T,T'}(a, b)$ holds. If condition (1) of Definition 3.7 is satisfied, we may use the basic propagation protocol. We assume then that condition (2) of Definition 3.7 holds and generalize the simple reliable transmission protocol. By symmetry, one can assume without loss of generality that there exist two paths $c = (c_1, \ldots, c_n)$ and $c' = (c'_1, \ldots, c'_{n'})$ in G satisfying:

$$c_1 = c'_1 = a, \quad c_n = c'_{n'} = b, \quad c \subset V\backslash(T'), \quad c' \subset V\backslash(T),$$
$$c \cap T \text{ is a singleton } \{c_d\}, \quad \text{with } d \in \{2, \ldots, n-1\} \text{ and } c_d \notin G(T').$$



Simple reliable transmission protocol (general case).
We define a protocol $\pi = (M, R, \sigma, D)$, where M is a large set containing $\{\omega, \omega'\}$. Fix a message m_0 in M.

Step 1: First, player a sends the actual state to c_{d-1} via the path $(a, c_2, \ldots, c_{d-1}) \subset V \backslash (T \cup T')$: at the first round a multicasts the state, at the second round c_2 repeats the previous message of a and so on until c_{d-2} repeats the state to player c_{d-1}. This phase lasts $d-2$ rounds and cannot be manipulated by players in T or T'.

Step 2: At round $d-2$ player c_d chooses with uniform probability some element $\hat{m}$ in M and multicasts it. At the end of this round, player c_{d-1} learns the state via the message of player c_{d-2} and also knows the message $\hat{m}$ just announced by player c_d.

Step 3: At round $d-1$, player c_{d-1} repeats $\hat{m}$ if the state is ω, or send the "uninformative" message m_0 if the state is ω'. In other words, player c_{d-1} reveals to his neighbors the message selected by player c_d if and only if the state is ω. Denote by $\bar{m}$ in $\{\hat{m}, m_0\}$ the message sent by c_{d-1} at this round.

Step 4: The value of $\bar{m}$ is transmitted from player c_{d-2} to player b via the path $c_{d-2}, c_{d-3}, \ldots, c_1 = a = c'_1, c'_2, \ldots, c'_{n'} = b$. This phase lasts $d-3+n'-1 = d+n'-4$ rounds.

Step 5: Finally, the value of $\hat{m}$ is transmitted from player c_{d+1} to player b via the path $c_{d+1}, c_{d+2}, \ldots, c_n = b$. This lasts $n-d-2$ rounds.

This protocol lasts in total $R = m' + m + d - 7$ rounds. At the end of step 4, the receiver receives a value m which corresponds to $\bar{m}$ if every player abides by the protocol and at the end of step 5, b receives a value m'

which corresponds to $\hat{m}$ if every player abides by the protocol. To conclude the definition of the protocol, we say that b outputs ω if $m = m'$ so we let D be the set of histories for the receiver such that m and m' coincide.

Lemma 3.13. *If $\Gamma_{T,T'}(a,b)$ holds, the simple reliable transmission protocol is ε-(T,T')-reliable.*

Proof. Assume that the adversary controls the players in T. The only thing which can be manipulated by these players is the value of $\hat{m}$. Hence if the state is ω, m and m' will coincide so $\mathbf{P}_{\omega,\pi,\tau^T}(D) = 1$ for each strategy τ^T. Assume now that the adversary controls the players in T' and that the state is ω'. Player c_{d-1} will send the message m_0 at round $d-1$ and since $c_d \notin G(T')$, m is (probabilistically) independent from $\hat{m}$. Since $\{c_{d+1},\ldots,c_n\} \cap T' = \emptyset$, step 5 cannot be manipulated by players in T' and thus $m' = \hat{m}$. So for any strategy $\bar{\tau}^{T'}$, $\mathbf{P}_{\omega',\pi,\bar{\tau}^T}(D) = \frac{1}{|M|} \leq \varepsilon$ for large $|M|$. □

B. In general, $\Gamma_{T,T'}(a,b)$ may not hold but $b \in C_{T,T'}(a)$. Thus we can find players $c_1,\ldots,c_n$, with $c_1 = a$, $c_n = b$ and $\Gamma_{T,T'}(c_d, c_{d+1})$ for each $d = 1,\ldots,n-1$. Note that no player c_d belongs to T or T'. Fix $\varepsilon > 0$.

For each $d = 1,\ldots,n-1$, from part A there exists an ε-(T,T')-reliable protocol $\pi_d = (M_d, R_d, \sigma_d, D_d)$ for the situation where the sender is player c_d and the receiver is player c_{d+1}. We define the protocol $\pi = (M, R, \sigma, D)$ by concatenating the protocols $\pi_1,\ldots,\pi_{n-1}$ as follows.

General reliable transmission protocol.

- In the first R_1 rounds, the players play according to σ_1.
- For each $k = 1,\ldots,n-1$: At the end of round R_k, player c_{k+1} considers his history of messages. If this history belongs to D_k, he ascribes to the state the value ω and otherwise he ascribes to the state the value ω'. In the next R_{k+1} rounds, the players play according to σ_{k+1} with player c_{k+1} treating the ascribed value of the state as the true one.

This defines σ. The set of messages M is $M_1 \cup \cdots \cup M_{n-1}$ and the total number of rounds is $R = R_1 + \cdots + R_{n-1}$. The set D is defined as the set of histories of player $c_n = b$ such that the sequence of messages received by b during the last R_{n-1} rounds belongs to D_{n-1}.

Lemma 3.14. *If $b \in C_{T,T'}(a)$, the general reliable transmission protocol is $O(\varepsilon)$-(T,T')-reliable.*

Proof. Assume that the adversary controls the players in T with some strategy τ^T. We have:

$$\mathbf{P}_{\omega,\pi,\tau^T}(D^c) \leq \sum_{d=1}^{n-1} \varepsilon, \quad \text{so} \quad \mathbf{P}_{\omega,\pi,\tau^T}(D) \geq 1 - (n-1)\varepsilon \underset{\varepsilon\to 0}{\longrightarrow} 1,$$

where D^c denotes the complementary of D. Assume now that the state is ω' and that the adversary controls the players in T' with some strategy $\bar{\tau}^{T'}$. The probability that every

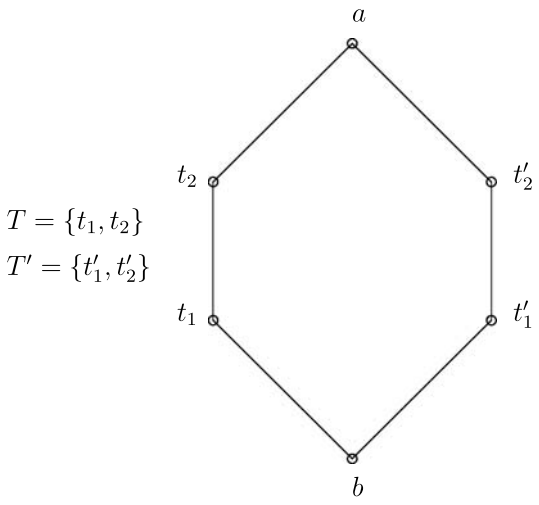
player c_d, for $d = 2, \ldots, n-1$ considers at the end of round $R_1 + \cdots + R_{d-1}$ that the state is ω' is at least $(1-\varepsilon)^{n-2}$ so:

$$\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D^c) \geq (1-\varepsilon)^{n-2}(1-\varepsilon) \quad \text{and} \quad \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D) \leq 1-(1-\varepsilon)^{n-1} \underset{\varepsilon\to 0}{\longrightarrow} 0. \qquad \square$$

3.2. *Non (T, T')-Reliability. An Example*

We show now on an example how to prove the necessity part of Theorem 3.10. The general proof is quite involved so we defer it to the appendix. We feel that the ideas used for the example are enough to grasp the logic of the general proof.

Consider a "slight" modification of Example 3.5.



$\Gamma_{T,T'}(a,b)$ does not hold here, and $b \notin C_{T,T'}(a)$. So Theorem 3.10 asserts that $\langle G, a, b\rangle$ is not (T, T')-reliable,[1] and we prove it now.

Fix a protocol $\pi = (M, R, \tilde{\sigma}, D)$. We construct strategies τ^T and $\bar{\tau}^{T'}$ such that $\mathbf{P}_{\omega,\pi,\tau^T}$ and $\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}$ induce the same probability distributions over the sequences of messages received by b, i.e. over the sequences of messages multicast by b, t_1 and t'_1. This will prove that the receiver cannot distinguish between {the state is ω and the adversary controls T and plays τ^T} and {the state is ω' and the adversary controls T' and plays $\bar{\tau}^{T'}$}, so that $\langle G, a, b\rangle$ is not (T, T')-reliable. We fix a particular message m_0 in M and only consider R-rounds strategies. The construction of τ^T and $\bar{\tau}^{T'}$ are completely symmetric. We first present the main ideas and then give precise definitions.

Assume that the adversary controls T and plays according to τ^T. He will try to convince the receiver that the state is ω' i.e. that player a plays according to $\tilde{\sigma}^a_{\omega'}$ and that the adversary controls T' and plays $\bar{\tau}^{T'}$. To do so, the main points are the followings:

[1] As noticed by an anonymous referee, this might be related to the impossibility result of [7] as follows. Assume that $\langle G, a, b\rangle$ is (T, T')-reliable. The idea is that (T, T')-reliable communication would then be possible in the graph of Example 3.5 with *unicast* communication, setting $T = \{i\}$ and $T' = \{j\}$. This is impossible by Theorem 5.1. of [7].

- Player t_2 will send at each round m_0.
- The messages sent by players a, t_2 and t_2' are not received by player b, so the adversary will construct fictitious messages for them, corresponding to the situation: {the state is ω', the adversary controls T' and player t_2' is sending m_0 at each round}. Player t_1 will then play according to these fictitious messages and to the real messages sent by b (a similar construction is found in [2], Lemma 8).

Let us see intuitively why τ^T and $\bar{\tau}^{T'}$ do the job. Consider the point of view of the receiver and assume that player t_1 is telling him via his messages:

> "I do not know what player t_1' is playing, but I can tell you that: t_2 is not faulty, player a says that the state is ω' and t_2' is sending m_0 at each round",

whereas player t_1' tells the receiver:

> "I do not know what t_1 is playing, but I can tell you that: player t_2' is not faulty, player a says that the state is ω and t_2 is sending m_0 at each round".

In this case, the receiver has no way to deduce which players are controlled by the adversary and what is the true state. We formalize these ideas now. In what follows, we shall use both representations of strategies (mixed and behavioral) and perform randomization before the execution or within the execution of the protocol whenever convenient.

The following observation leads to the definition of τ^T. Assume that player a is using some pure strategy σ^a, that player t_2 is using a pure strategy σ^{t_2} and that player t_1 (resp. t_2') has sent, up to some round r, a sequence of messages $m^{t_1}(r) = (m_1^{t_1}, \ldots, m_r^{t_1})$ (resp. $m^{t_2'}(r) = (m_1^{t_2'}, \ldots, m_r^{t_2'})$). Since $G(\{a, t_2\}) = \{a, t_2, t_2', t_1\}$, this defines unambiguously by induction on r, the message sent by the players a and t_2 at rounds $1, \ldots, r+1$. The interpretation is that t_2' and t_1 separate a and t_2 from the rest of the network. We denote the corresponding sequence of messages sent by player t_2 at rounds $1, \ldots, r$ (but not $r+1$) by:

$$m^{t_2}(r)(\sigma^a, \sigma^{t_2}, m^{t_1}(r), m^{t_2'}(r)).$$

Symmetrically, $m^{t_2'}(r)(\sigma^a, \sigma^{t_2'}, m^{t_1'}(r), m^{t_2}(r))$ will denote the sequence of messages sent by player t_2' at rounds $1, \ldots, r$ if: player a uses σ^a, player t_2' uses a pure strategy $\sigma^{t_2'}$ and $m^{t_1'}(r)$, $m^{t_2}(r)$ have respectively being sent by players t_1', t_2.

We now define τ^T as a mixed strategy for the adversary controlling $T = \{t_1, t_2\}$.

- Before round 1, the adversary selects a fictitious pure strategy σ^a for the sender according to the distribution $\tilde{\sigma}^a_{\omega'}$ and for each player i in T a pure strategy σ^i according to $\tilde{\sigma}^i$.
- At each round, player t_2 sends the message m_0.
- At round $r = 1$, player t_1 plays according to the pure strategy σ^{t_1}. After round $r = 1, \ldots, R-1$, the adversary knows, for each player i in $G(T) = \{a, t_1, t_2, b\}$, the sequence of messages $m^i(r) = (m_1^i, \ldots, m_r^i)$ actually sent by player i up to stage r. Player t_1 will send at round $r+1$ the message $\sigma^{t_1}((\hat{m}^i(r))_{i \in G(t_1)})$, where:
  - $\hat{m}^b(r) = m^b(r)$ and $\hat{m}^{t_1}(r) = m^{t_1}(r)$ (player b knows the messages sent by b and t_1, so the adversary cannot cheat on them),

– $\hat{m}^{t_2}(r)$ is a fictitious sequence of messages. $\hat{m}^{t_2}(r)$ is the sequence of messages that player t_2 would have sent if: player t_2' sends m_0 at each round, player t_1 has sent the messages $m_1^{t_1}, m_2^{t_1}, \ldots, m_r^{t_1}$, and players a and t_2 respectively use the pure strategies σ^a and σ^{t_2}. That is, $\hat{m}^{t_2}(r)$ is what we previously denoted by:

$$m^{t_2}(r)(\sigma^a, \sigma^{t_2}, m^{t_1}(r), (m_0, \ldots, m_0)).$$

This ends the definition of τ^T, $\bar{\tau}^{T'}$ is defined symmetrically. To conclude, we fix for each i in $G(b) = \{b, t_1, t_1'\}$, a sequence of messages $m^i(R) = (m_1^i, \ldots, m_R^i)$ and we prove that:

$$\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i(R))_{i\in G(b)}\big) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i(R))_{i\in G(b)}\big).$$

Put $N = \{a, t_1, t_2\}$ and $N' = \{a, t_1', t_2'\}$. Fix two vectors of pure strategies $\sigma^N = (\sigma^a, \sigma^{t_1}, \sigma^{t_2})$ and $\bar{\sigma}^{N'} = (\bar{\sigma}^a, \bar{\sigma}^{t_1}, \bar{\sigma}^{t_2})$. Note that no player in N is controlled by T', and no player in N' is controlled by T. Consider the events:

$$\begin{aligned} H_T(\sigma^N, \bar{\sigma}^{N'}) = \{&\text{the adversary } T \text{ playing } \tau^T \text{ first selects } \sigma^N \text{ and} \\ &\text{each player } i \text{ in } N' \text{ playing } \tilde{\sigma}^i \text{ selects } \bar{\sigma}^i\}, \\ H_{T'}(\sigma^N, \bar{\sigma}^{N'}) = \{&\text{each player } i \text{ in } N \text{ playing } \tilde{\sigma}^i \text{ selects } \sigma^i \text{ and} \\ &\text{the adversary } T' \text{ playing } \bar{\tau}^{T'} \text{ first selects } \bar{\sigma}^{N'}\}. \end{aligned}$$

The probability under (ω, π, τ^T) of $H_T(\sigma^N, \bar{\sigma}^{N'})$ is the product:

$$\tilde{\sigma}^a_{\omega'}(\sigma^a) \times \tilde{\sigma}^{t_1}(\sigma^{t_1}) \times \tilde{\sigma}^{t_2}(\sigma^{t_2}) \times \tilde{\sigma}^a_{\omega}(\bar{\sigma}^a) \times \tilde{\sigma}^{t_1'}(\bar{\sigma}^{t_1'}) \times \tilde{\sigma}^{t_2'}(\bar{\sigma}^{t_2'}),$$

which is also the probability under $(\omega', \pi, \bar{\tau}^{T'})$ of $H_{T'}(\sigma^N, \bar{\sigma}^{N'})$. Since this holds for each pair $(\sigma^N, \bar{\sigma}^{N'})$, it will be sufficient to prove that the following equality between conditional probabilities holds for each $(\sigma^N, \bar{\sigma}^{N'})$:

$$\begin{aligned} &\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i(R))_{i\in G(b)} | H_T(\sigma^N, \bar{\sigma}^{N'})\big) \\ &\quad = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i(R))_{i\in G(b)} H_{T'}(\sigma^N, \bar{\sigma}^{N'})\big). \end{aligned} \tag{*}$$

We show (*) by induction on R. Fixing r in $\{0, \ldots, R-1\}$, it is enough to prove:

$$\begin{aligned} &\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i_{r+1})_{i\in G(b)} | H_T(\sigma^N, \bar{\sigma}^{N'}), (m^i(r))_{i\in G(b)}\big) \\ &\quad = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i_{r+1})_{i\in G(b)} | H_{T'}(\sigma^N, \bar{\sigma}^{N'}), (m^i(r))_{i\in G(b)}\big). \end{aligned} \tag{**}$$

By convention, (**) for $r = 0$ is just:

$$\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i_1)_{i\in G(b)} | H_T(\sigma^N, \bar{\sigma}^{N'})\big) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i_1)_{i\in G(b)} | H_{T'}(\sigma^N, \bar{\sigma}^{N'})\big).$$

We compute the left-hand side of (**). We assume that the state is ω, the adversary controls T, plays according to τ^T and has first selected σ^N, each player i in N' has first selected $\bar{\sigma}^i$ according to its mixed strategy $\tilde{\sigma}^i$ (according to $\tilde{\sigma}^a_{\omega}$ for player a), and

the messages really sent by each player i in $G(b)$ at rounds $r' = 1, \ldots, r$ corresponds to $m^i(r) = (m_1^i, \ldots, m_r^i) \in M^r$. Under these assumptions, which messages are sent at round $r+1$ by the players in $G(b) = \{b, t_1, t_1'\}$?

- The receiver is using his behavioral strategy $\tilde{\sigma}^b$, so he chooses to send his message of round $r+1$ according to the probability $\tilde{\sigma}^b((m^i(r))_{i\in G(b)})$.
- Player t_1' uses the pure strategy $\bar{\sigma}^{t_1'}$, so he sends the message $\bar{\sigma}^{t_1'}((\bar{m}^i(r))_{i\in G(t_1')})$, where $\bar{m}^i(r)$ is the sequence of messages really sent by player i up to round r. Since $G(t_1') = \{b, t_1', t_2'\}$, we have $\bar{m}^b(r) = m^b(r)$, $\bar{m}^{t_1'}(r) = m^{t_1'}(r)$, and we need to compute $\bar{m}^{t_2'}(r)$. $\bar{m}^{t_2'}(r)$ is unambiguously defined by the following facts:
  - player t_2 has sent m_0 at each stage (by definition of τ^T), player t_1' has sent $m^{t_1'}(r)$,
  - players a and t_2' respectively use the pure strategies $\bar{\sigma}^a$ and $\bar{\sigma}^{t_2'}$. That is, $\bar{m}^{t_2'}(r)$ is what we previously defined as $m^{t_2'}(r)(\bar{\sigma}^a, \bar{\sigma}^{t_2'}, m^{t_1'}(r), (m_0, \ldots, m_0))$.
- Player t_1 is controlled by the adversary, which has selected σ^N. By definition of τ^T, player t_1 will send the message $\sigma^{t_1}((\hat{m}^i(r))_{i\in G(t_1)})$, where $\hat{m}^b(r) = m^b(r)$, $\hat{m}^{t_1}(r) = m^{t_1}(r)$ and $\hat{m}^{t_2}(r) = m^{t_2}(r)(\sigma^a, \sigma^{t_2}, m^{t_1}(r), (m_0, \ldots, m_0))$.

Setting $m^{t_2}(r) = \hat{m}^{t_2}(r)$ and $m^{t_2'}(r) = \bar{m}^{t_2'}(r)$ for symmetry reasons, we obtain that under $\mathbf{P}_{\omega,\pi,\tau^T}$ and conditionally on $(H_T(\sigma^N, \bar{\sigma}^{N'}), (m^i(r))_{i\in G(b)})$, the players in $G(b)$ select their message of round $r+1$ as follows: player b uses the lottery $\tilde{\sigma}^b((m^i(r))_{i\in G(b)})$, player t_1' sends the message $\bar{\sigma}^{t_1'}((m^i(r))_{i\in G(t_1')})$, and player t_1 sends the message $\sigma^{t_1}((m^i(r))_{i\in G(t_1)})$, where $m^{t_2'}(r) = m^{t_2'}(r)(\bar{\sigma}^a, \bar{\sigma}^{t_2'}, m^{t_1'}(r), (m_0, \ldots, m_0))$, and $m^{t_2}(r) = m^{t_2}(r)(\sigma^a, \sigma^{t_2}, m^{t_1}(r), (m_0, \ldots, m_0))$.

We obtain a symmetric expression (in (T, σ^N)–$(T', \bar{\sigma}^{N'})$) so this is also how the players in $G(b)$ select their message of round $r+1$ under $\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}$ and conditionally on $(H_{T'}(\sigma^N, \bar{\sigma}^{N'}), (m^i(r))_{i\in G(b)})$. The proof is thus complete.

4. Security

We give now necessary and sufficient conditions for security of information transmission.

Definition 4.1. Let T be a subset of nodes, and $c = (c_1, \ldots, c_n)$ be a path. We say that T has no consecutive neighbors on c if $\forall m = 1, \ldots, n-1$ $(c_m \in G(T) \Rightarrow c_{m+1} \notin G(T))$.

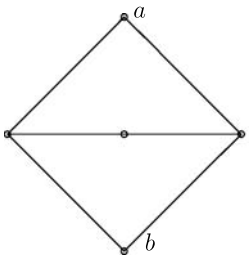
Note that under this condition, $c \cap T = \emptyset$.

Theorem 4.2. *$\langle G, a, b, t\rangle$ is secure if and only if it is reliable and for each $T \subset V\backslash\{a, b\}$ with $|T| \leq t$, there is a path c in G from a to b with $c \subset V\backslash T$ such that T has no consecutive neighbors on c.*

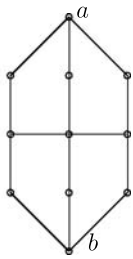
The graphs considered by Franklin and Wright [9] have neighbor-disjoint paths i.e. there are n disjoints lines from a to b and each edge in the graph is on some line.

Franklin and Wright prove then that $\langle G, a, b, t\rangle$ is secure if and only if $n > t$ which can be proven applying Theorems 3.10 and 4.2: one checks easily that the necessary and sufficient conditions we provide are satisfied by Franklin and Wright's graph. We give now examples for which $\langle G, a, b, t\rangle$ is secure but G is not of the type considered by [9].

Example 4.3.



$\langle G, a, b, 1\rangle$ is secure.



$\langle G, a, b, 2\rangle$ is secure.

The sequel is devoted to the proof of Theorem 4.2. We shall use some properties of usual distances between probabilities which we recall now. Let P, Q be two probability distributions on some product of finite sets $X \times Y$, we let $\|P - Q\|_\infty = \sup_A |P(A) - Q(A)|$ and $\|P - Q\|_1 = \sum_{x,y} |P(x, y) - Q(x, y)|$. We have the following properties:

Proposition 4.4.

1. $\|P - Q\|_1 = 2\|P - Q\|_\infty$.
2. *If we let* P^X (*resp.* Q^X) *be the marginal distribution of* P (*resp.* Q) *on* X, *the distances between the marginals are smaller than the distances between the global distributions*:

$$\left\|P^X - Q^X\right\|_\infty \leq \|P - Q\|_\infty, \qquad \left\|P^X - Q^X\right\|_1 \leq \|P - Q\|_1.$$

3. *If* P *and* Q *induce the same conditional distribution on* y *given* x, *i.e.* $P(y|x) = Q(y|x), \forall x, y$, *then*: $\|P^X - Q^X\|_1 = \|P - Q\|_1$.

The proof is straightforward and is omitted.

4.1. *The Reliable and Private Protocol*

We construct a protocol which is ε-reliable and ε-private. The construction is similar to that of [9], adapted to the graph we consider. Let q be a prime integer and let the message space $M = \mathbb{F}_q$ be a finite field with q elements. We first build a sub-protocol $\pi(a, b, T)$ by which a sends a message to b whose content is secret for $T \subset V\backslash\{a, b\}$ using a path c from a to b such that T has no consecutive neighbors on c.

We first start with two distinct nodes i, j and $T \subset V\backslash\{i, j\}$ for which there is a path c from i to j such that:

(i) T has no consecutive neighbors on c;
(ii) $c \cap G(T) \subset \{i, j\}$.

Several cases are consistent with those assumptions. T might hear only i or only j on c, or T both i and j but then there must be $k \neq i, j$ on c which T do not hear.

Let us first assume that $c = (c_1 = i, c_2, \ldots, c_n = j)$ and that $n > 2$. $(c_2, \ldots, c_{n-1})$ are not in $G(T)$.

Sub-protocol $\pi_0(i, j, T)$: i sends the message s_T^i to j, keeping it secret from T.

- Round 1. c_2 draws r_T uniformly from M and multicasts it.
- Round 2. i multicasts $u_T = s_T^i + r_T$.
- Subsequent rounds. c_2 sends $s_T = u_T - r_T$ to j along c (using a basic propagation protocol).
- Let s_T^j be the message received by j.

The other cases to consider are when i and j are neighbors of each other. Then if $c \cap G(T) = \{i\}$, construct $\pi_0(i, j, T)$ as above by letting j play the role of c_2. If $c \cap G(T) = \{j\}$, i just multicasts s_T^i. We get readily the property:

Property. *If the adversary controls T, $s_T^i = s_T^j$ and the distribution of s_T^i given any adversary's history is uniform.*

Let now c be a path from a to b such that T has no consecutive neighbors on c. Note that necessarily, $c \cap T = \emptyset$. We write $c = (c_1 = a, \ldots, c_n = b)$ and decompose it as follows:

$$c = (c_{i_0} = a, \ldots, c_{i_1}, \ldots, c_{i_k}, \ldots, c_{i_{k+1}}, \ldots, c_{i_K} = b)$$

in such a way that for each $k = 0, \ldots, K-1$ c_{i_k} and $c_{i_{k+1}}$ are not consecutive on c (i.e. $i_k + 1 < i_{k+1}$) and that T has no neighbor strictly between these two nodes (i.e. $i_k < i < i_{k+1} \Rightarrow i \notin G(T)$), so that for each k, we can apply $\pi_0(c_{i_k}, c_{i_{k+1}}, T)$.

Sub-protocol $\pi(a, b, T)$: a sends the message s_T^a to b, keeping it secret from T.

- Apply successively $\pi_0(c_{i_k}, c_{i_{k+1}}, T)$ for $k = 0, \ldots, K-1$.
- Let s_T^j be the message received by j.

Property. *If the adversary controls T, $s_T^a = s_T^b$ and the distribution of s_T^a given any adversary's history is uniform.*

We describe now the complete protocol. We fix an enumeration of the set of T's such that $T \subset V \backslash \{a, b\}$ with $|T| \leq t$. When the protocol is supposed to perform a sub-protocol for each T, it means that the sub-protocols are used independently and successively according to this enumeration.

Protocol π: a sends the message ω to b.

- For each T, a chooses (c_T^a, d_T^a) uniformly in M^2 and sends it to b with $\pi(a,b,T)$. Let (c_T^b, d_T^b) received by b.
- For each T, b chooses r_T^b uniformly in M and sets $s_T^b = c_T^b r_T^b + d_T^b$. b transmits $\{(r_T^b, s_T^b), T \subset V\backslash\{a,b\}, |T| \leq t\}$ $\frac{\varepsilon}{4}$-reliably to a. Let $\{(r_T^a, s_T^a), T \subset V\backslash\{a,b\}, |T| \leq t\}$ be received by a.
- a computes $W^a = \{T, s_T^a = c_T^a r_T^a + d_T^a\}$ and $z^a = \omega + \sum_{T \in W^a} c_T^a$. a transmits (W^a, z^a) $\frac{\varepsilon}{4}$-reliably to b. Let (W^b, z^b) be received by b.
- b sets $\omega^b = z^b - \sum_{T \in W^b} c_T^b$.

Lemma 4.5. *π is ε-reliable and ε-private for q large enough.*

Proof. Let ω be the state, $\tilde{T}$ be the set of nodes controlled by the adversary and $\tau^{\tilde{T}}$ the strategy of the adversary, set $P = \mathbf{P}_{\omega,\pi,\tau^{\tilde{T}}}$. Let E be the event where the two reliable transmissions used in the definition of π succeed, $P(E) \geq (1-\frac{\varepsilon}{4})^2 \geq 1-\frac{\varepsilon}{2}$. Conditional on E, set $r_T = r_T^a = r_T^b$, $s_T = s_T^a = s_T^b$, $W = W^a = W^b$, $z = z^a = z^b$. Then for each T,

$$\begin{aligned} P(T \in W,\ c_T^a \neq c_T^b | E) &= P(c_T^b r_T + d_T^b = c_T^a r_T + d_T^a,\ c_T^a \neq c_T^b | E) \\ &= P(r_T = (c_T^b - c_T^a)^{-1}(d_T^a - d_T^b),\ c_T^a \neq c_T^b | E) \\ &\leq P(r_T = (c_T^b - c_T^a)^{-1}(d_T^a - d_T^b) | E) \\ &= \frac{1}{q} \end{aligned}$$

since r_T is uniform in $\mathbb{F}_q$. Then, $P(\omega^b \neq \omega | E) \leq \sum_T P(T \in W,\ c_T^a \neq c_T^b | E) \leq \binom{v}{t}\frac{1}{q}$ with $v = |V-2|$. We get finally, $P(\omega^b \neq \omega) \leq \binom{v}{t}\frac{1}{q} + \frac{\varepsilon}{2} \leq \varepsilon$ for large q, π is thus ε-reliable.

We prove now that this protocol is ε-secure. We let $Q = \mathbf{P}_{\omega',\pi,\tau^{\tilde{T}}}$ and we want to prove that $\|P^{\tilde{T}} - Q^{\tilde{T}}\|_1 \leq \varepsilon$. First note that in the definition of the protocol π, only z^a depends on ω. Thus for each event A in the set of histories of the adversary, $P(A | z^a = z) = Q(A | z^a = z)$.

The relevant data that the adversary might observe during the execution of the protocol is summarized by the tuple $h = ((c_T^a, d_T^a)_{T \neq \tilde{T}}, (c_T^b, d_T^b)_{T \neq \tilde{T}}, (r_T^a, s_T^a)_T, (r_T^b, s_T^b)_T, W^a)$ and by z^a. Let S be the set of those tuples h for which $\forall T$, $(r_T^a, s_T^a) = (r_T^b, s_T^b)$. From the property of the sub-protocol $\pi(a,b,\tilde{T})$, $\tilde{T} \in W^a$ whenever h belongs to S, thus z^a writes: $z^a = c_{\tilde{T}}^a + \omega + \sum_{T \in W, T \neq \tilde{T}} c_T^a$. The random variables $(c_T^a, d_T^a)_T$ being independent across T's, the conditional distribution of $c_{\tilde{T}}^a$ given h equals the distribution of $c_{\tilde{T}}^a$ given $(r_{\tilde{T}}^a, s_{\tilde{T}}^a)$. For each (c,r,s), we compute $P(c_{\tilde{T}}^a = c | r_{\tilde{T}}^a = r, s_{\tilde{T}}^a = s)$. If $r = 0$, this equals $P(c_{\tilde{T}}^a = c | d_{\tilde{T}}^a = s) = \frac{1}{q}$ since $c_{\tilde{T}}^a$ is uniformly distributed and $c_{\tilde{T}}^a$, $d_{\tilde{T}}^a$ are independent. If $r \neq 0$, $P(c_{\tilde{T}}^a = c | r_{\tilde{T}}^a = r, s_{\tilde{T}}^a = s) = P(d_{\tilde{T}}^a = s - rc) = \frac{1}{q}$ since $d_{\tilde{T}}^a$ is uniformly distributed. The conditional distribution of z^a given h is thus uniform (the sum of a uniform and a constant) for each h in S. By symmetry, this

property holds under P and under Q. It follows that for each h in S and z in $\mathbb{F}_q$, $P(z^a = z, h) = Q(z^a = z, h)$.

Now for each event A in the set of histories of the adversary,

$$\begin{aligned} P(A) &= \sum_{h,z} P(A|z^a = z)P(z^a = z, h) \\ &= \sum_{h\in S}\sum_{z} P(A|z^a = z)P(z^a = z, h) + \sum_{h\notin S}\sum_{z} P(A|z^a = z)P(z^a = z, h) \\ &= \sum_{h\in S}\sum_{z} Q(A|z^a = z)Q(z^a = z, h) + \sum_{h\notin S}\sum_{z} Q(A|z^a = z)P(z^a = z, h). \end{aligned}$$

Similarly,

$$Q(A) = \sum_{h\in S}\sum_{z} Q(A|z^a = z)Q(z^a = z, h) + \sum_{h\notin S}\sum_{z} Q(A|z^a = z)Q(z^a = z, h).$$

It follows,

$$\begin{aligned} |P(A) - Q(A)| &= \sum_{h\notin S}\sum_{z} Q(A|z^a = z)(P(z^a = z, h) - Q(z^a = z, h)) \\ &= |P(S^c) - Q(S^c)| \end{aligned}$$

where S^c is the complementary of S. When the first reliable transmission in π succeeds, the event S occurs, thus $P(S) \geq 1 - \frac{\varepsilon}{4}$ and $Q(S) \geq 1 - \frac{\varepsilon}{4}$. Therefore $\|P^{\tilde{T}} - Q^{\tilde{T}}\|_\infty \leq \frac{\varepsilon}{4}$ and since $\|P^{\tilde{T}} - Q^{\tilde{T}}\|_1 = 2\|P^{\tilde{T}} - Q^{\tilde{T}}\|_\infty$, π is ε-secure. □

4.2. *The Conditions of Theorem 4.2 Are Necessary*

Assume that there is T that has two consecutive neighbors on each path from a to b. Assume further that $\langle G, a, b, t\rangle$ is reliable. Let $\varepsilon > 0$ and π be a protocol such that every strategy τ^T: $\mathbf{P}_{\omega,\pi,\tau^T}(D) \geq 1-\varepsilon$, $\mathbf{P}_{\omega',\pi,\tau^T}(D) \leq \varepsilon$. We prove now that $\|\mathbf{P}^T_{\omega,\pi,\tau^T} - \mathbf{P}^T_{\omega',\pi,\tau^T}\|_1$ cannot be small.

Let us fix such $\varepsilon > 0$, π and a strategy τ^T of the adversary. Define the following sets of nodes:

- M is the set of nodes $i \in V$, for which there is a path c from a to i such that T has no consecutive neighbors on c.
- $N = V\backslash M$.

The following claim follows directly from the definition of M.

Claim 4.6.

(1) *If $i \in M$ has a neighbor $j \notin M$, then both i and j are neighbors of T.*

(2) *If $i \in N$ has a neighbor $j \notin N$, then both i and j are neighbors of T.*

We let now $U = (G(M)\backslash M) \cup (G(N)\backslash N)$. From the previous claim, a member i of M is in U iff it has a neighbor j in N and then j is in U and both are neighbors of T.

Each path from a to b has to cross U on two consecutive nodes which are neighbors of T. So all information regarding the value of the state has to transit by U, i.e. there is a cut in the network such that the adversary hears all communication exchanged on this cut.

We let $P = \mathbf{P}_{\omega,\pi,\tau^T}$ and $Q = \mathbf{P}_{\omega',\pi,\tau^T}$. For each $S \subset V$, we let P^S (resp. Q^S) be the marginal of P (resp. Q) on histories for S. We also let $\tilde{P}$ (resp. $\tilde{Q}$) be the marginal of P (resp. Q) on histories of messages *sent* by U.

Lemma 4.7. *The distribution of histories for N conditional on messages sent by U does not depend on ω.*

Proof. By induction on R. The claim is obvious for $R = 1$ since $a \in M$. Assume this property to be true for histories of length $R-1$. Given the messages sent by U at round $R-1$, the next messages chosen by nodes in $G(N)$ are selected according to distributions that do not depend on ω. □

Now, if b is informed of ω it has to be through U and thus T is also informed. We get the following inequalities.

$$1 - 2\varepsilon \leq^{(a)} \left\| P^b - Q^b \right\|_\infty \leq^{(b)} \left\| P^N - Q^N \right\|_\infty = \frac{1}{2} \left\| P^N - Q^N \right\|_1$$

$$=^{(c)} \frac{1}{2} \left\| \tilde{P} - \tilde{Q} \right\|_1 \leq^{(d)} \frac{1}{2} \left\| P^T - Q^T \right\|_1$$

where: (a) follows from π being ε-reliable; (b) holds since P^b (resp. Q^b) is a marginal of P^N (resp. Q^N); (c) follows from Lemma 4.7 since the distribution of histories for N conditional on messages sent by U is the same under P^N and Q^N; (d) holds since $\tilde{P}$ (resp. $\tilde{Q}$) is a marginal of P^T (resp. Q^T).

This proves that π cannot be ε-reliable and ε-private for ε small.

5. Concluding Remarks

The Unicast Case. The notions of reliability and security are also naturally defined in the unicast setup. The analog of Theorem 3.11 is the following: regarding unicast communication, $\langle G, a, b, t\rangle$ is (T, T')-reliable if and only if there exists a path from a to b included in $V \setminus (T \cup T')$. This can be deduced, e.g., from Theorem 23 in [2] or from Theorem 3 in [13]. Regarding privacy of information transmission, we believe that one can proceed as in Sect. 4.1 of [9] or of Sect. 4.1 of the present paper to obtain that in the unicast setup, $\langle G, a, b, t\rangle$ is secure if and only if it is reliable.

It appears thus that for undirected communication graphs, it is easier to obtain reliable and secure communication in the multicast setup than in the unicast setup. This is not *a priori* obvious, as discussed in the fourth paragraph of the introduction in [9]: in the multicast setup, compared to the unicast one, the adversary may *a priori* benefit from the loss of privacy in the communication between the other players. However, the adversary also suffers from a restriction, since an incorrect transmission from a faulty player will be received identically by all the nodes connected to this player. In the

present setting, as in [9], the change from unicast to multicast communication hurts the adversary more than it helps. It would be interesting to determine whether this property is robust and can be extended to more general setups, e.g. to directed communication graphs.

Efficiency. We did not address the question of efficiency of the protocols. As pointed out by an anonymous referee, the message complexity of the protocols constructed here is exponential when t is large but the round complexity is polynomial. The existence of efficient communication protocol in this setup is an open problem.

Independence and Correlation of Random Inputs. In the model studied here, non-faulty players use independent randomizations while the adversary is allowed to correlate the randomizations of the faulty players. It might be the case that the results would remain the same if we restricted the adversary to perform randomizations which are independent across faulty players. The conditions obviously remain sufficient but in the proof of the necessity part of Theorem 3.10, the strategies constructed for the adversary use correlated randomizations. It is not clear whether this proof may be adapted.

On the other hand, allowing non-faulty players to perform correlated randomizations would certainly affect the results. The random inputs of players i and j are correlated when they both depend on a common random element known to both i and j, which might be interpreted as an authentication key. The study of reliable and secure communication with authentication keys is done by [2] for the unicast case. An interesting line of research is thus to study how the existence of authentication keys affects our characterization.

Appendix: The Condition $b \in C_{T,T'}(a)$ Is Necessary in Theorem 3.10

We assume that $b \notin C_{T,T'}(a)$ and show that $\langle G, a, b\rangle$ is not (T, T')-reliable. We fix a protocol $\pi = (M, R, \tilde{\sigma}, D)$ and construct strategies τ^T and $\bar{\tau}^{T'}$ such that $\mathbf{P}_{\omega,\pi,\tau^T}(D) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D)$. This will prove that player b—the receiver—is not able to differentiate between {the state is ω and the adversary controls the players in T} and {the state is ω' and the adversary controls the players in T'}, i.e. that $\langle G, a, b\rangle$ is not (T, T')-reliable.

We fix a message m_0 in M which shall play the role of an uninformative message. We let for simplicity $A = C_{T,T'}(a) \subset V\backslash(T \cup T')$ and $B = C_{T,T'}(b) \subset V\backslash(T \cup T')$. Since b is not in A, we have $A \cap B = \emptyset$. Letting for each S subset of V, $G(S)$ be $\bigcup_{i\in S} G(i)$, we have $G(A)\backslash A \subset T \cup T'$ and $G(B)\backslash B \subset T \cup T'$ and each path in G starting from (a player in) A and arriving to (a player in) B goes through $T \cup T'$. The players in A can communicate with the sender in a safe (i.e. (T, T')-reliable) way so we can think as if each player in A had the information on the state. Similarly, the players in B can communicate safely with the receiver, so when constructing τ^T and $\bar{\tau}^{T'}$ we have to prevent each player in B from learning the state. We distinguish two cases.

6.1. *First Case*

We assume that there exist a path from A to B that does not go through T' and a path from A to B that does not go through T.

This implies (see Definition 3.7) that: if c is a path from A to B that does not go through T', then $c \cap T \neq \emptyset$ and if moreover $c \cap T$ is a singleton $\{k\}$, then $k \in G(T')$ i.e. the messages multicast by player k are received by at least one player in T'. A similar observation holds if we exchange the roles of T and T'.

We start with considerations on the graph G. All what follows is symmetric between T and T'. We first separate the elements of T (resp. T') into 3 disjoint categories: those which are also in T' (resp. T), those which are not in T' (resp. T) and are directly connected to B, and the remaining elements. We define:

$$T'' = T \cap T',$$
$$T_1 = (T \backslash T') \cap G(B), \qquad T_1' = (T' \backslash T) \cap G(B),$$
$$T_2 = T \backslash (T'' \cup T_1), \qquad T_2' = T' \backslash (T'' \cup T_1').$$

We use $\vee$ for the symbol of disjoint union. It is plain that $T = T'' \vee T_1 \vee T_2$, and $T' = T'' \vee T_1' \vee T_2'$. Recall that $A \cap (T \cup T') = \emptyset = B \cap (T \cup T')$, $G(A) \backslash A \subset (T \cup T')$, and $G(B) \backslash B \subset (T \cup T')$. The last inclusion gives $G(B) \subset B \vee T'' \vee T_1 \vee T_1'$. All the information about the state obtained by the players in B come from $T'' \vee T_1 \vee T_1'$. These players will not be able to determine if the adversary controls T (hence T'' and T_1) or T' (hence T'' and T_1'), so they will not determine what the state is. The following sets will also play an important role.

$$N = \{i \in V \backslash B, \text{ there exists a path from } i \text{ to } B \text{ in } V \backslash T'\},$$
$$N' = \{i \in V \backslash B, \text{ there exists a path from } i \text{ to } B \text{ in } V \backslash T\}.$$

Notice that $A \subset N \cap N'$, $B \cap (N \cup N') = \emptyset$, $N \cap T' = \emptyset$, $N' \cap T = \emptyset$, $T_1 \subset N \backslash (N' \cup T')$ and $T_1' \subset N' \backslash (N \cup T)$.

Lemma 6.1.

$$G(N) \subset N \vee B \vee T'' \vee T_2' \vee (T_1' \cap G(T)), \tag{1}$$
$$G(N') \subset N' \vee B \vee T'' \vee T_2 \vee (T_1 \cap G(T')), \tag{2}$$
$$G(N \backslash T_1) \subset N \vee T'' \vee T_2' \vee (T_1' \cap G(T)), \tag{3}$$
$$G(N' \backslash T_1') \subset N' \vee T'' \vee T_2 \vee (T_1 \cap G(T')). \tag{4}$$

Proof. By symmetry, we only prove (1) and (3). The unions are clearly disjoint.

Consider j in $G(N) \backslash (N \vee B \vee T'' \vee T_2')$. Then $j \notin N \cup B$ so each path from j to B goes through T' but $j \in G(i)$ with $i \in N$ thus j is in T'. As $j \notin T_2' \cup T''$, $j \in T_1' \subset G(B)$. If $i \in T$, then $j \in T_1' \cap G(T)$ and we are done. Assume now that $i \notin T$. i belongs to N so there exists a path from i to B in $V \backslash T'$. Also $i \in G(j)$ and $j \in G(B) \backslash T$ so there exists b' in B such that the path $c = (i, j, b')$ goes from i to B in $V \backslash T$. Moreover $c \cap T' = \{j\}$ is a singleton and $i \notin B$ so by the definitions of B and $\Gamma_{T,T'}$, we also have $j \in G(T)$ and (1) is proved.

Notice that if $j \in B$, $i \in G(B) \backslash B \subset T \cup T'$. $i \in N$ so $i \notin T'$, and $i \in T_1$. This proves (3). □

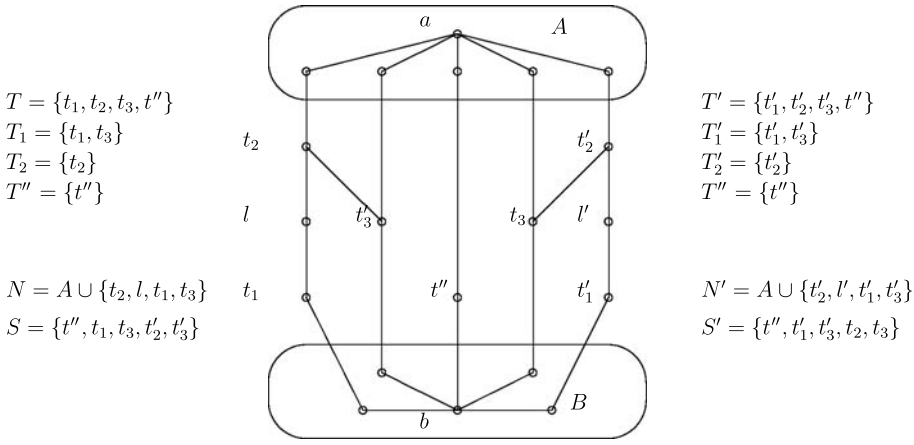


Fig. 1. Illustration.

We now define:

$$S = T'' \vee T_1 \vee T'_2 \vee (T'_1 \cap G(T)) \quad \text{and} \quad S' = T'' \vee T'_1 \vee T_2 \vee (T_1 \cap G(T')).$$

Using inclusions (3) and (4) of Lemma 6.1, we obtain:

$$G(N \backslash T_1) \subset (N \backslash T_1) \vee S, \tag{5}$$

$$G(N' \backslash T'_1) \subset (N' \backslash T'_1) \vee S'. \tag{6}$$

Figure 1 illustrates these definitions.

Assume now that the adversary controls $T = T'' \vee T_2 \vee T_1$ and plays according to τ^T. He tries to convince the receiver that the state is ω', that the adversary controls T' and plays $\bar{\tau}^{T'}$. The ideas are the followings:

- each player in T'' is both in T and T', and will send the message m_0 at each round.
- if $i \in T_2$, every path from i to B goes through $T_1 \vee T'_1 \vee T''$ since $G(B) \subset B \vee T_1 \vee T'_1 \vee T''$. This implies that the players in B will not have a "safe" information about the messages sent by player i. Such a player i will also send the message m_0 at each round.
- if $i \in T_1$, the messages of i are received by the players in B. Player i will pretend that player a says via his messages that the state is ω' and that the players in $T'_2 \vee T''$ are sending m_0 at each round. He will construct, for the players in $N \backslash T_1$, fictitious messages corresponding to this case and will play according to these fictitious messages. Since $G(N \backslash T_1) \subset (N \backslash T_1) \vee S$ and $S \subset G(T) \vee T'_2$, the adversary controlling T will be able to construct these fictitious messages.

Recall that the strategy $\tilde{\sigma} = (\tilde{\sigma}^i)_{i \in V}$ is given by the protocol π. For each player i, $\tilde{\sigma}^i$ is a strategy for player i and if $m(r) = (m^j(r))_{j \in G(i)}$ represents the messages sent by the neighbors of i and himself at rounds $1, \ldots, r$, $\tilde{\sigma}^i(m(r))$ will denote the corresponding probability on M used by player i to select his message at round $r + 1$.

By Kuhn's theorem, $\tilde{\sigma}^i$ can also be seen as a mixed strategy of player i. For player a set: $\tilde{\sigma}^a = (\tilde{\sigma}^a_\omega, \tilde{\sigma}^a_{\omega'})$ where $\tilde{\sigma}^a_\omega$ and $\tilde{\sigma}^a_{\omega'}$ are mixed strategies of player a. All strategies considered in this proof are R-rounds strategies.

The following observation is based on inclusion (5). Fix:

- for each player i in $N\backslash T_1$, a pure strategy σ^i. We let $(\sigma^i)_{i\in N\backslash T_1} = \sigma^{N\backslash T_1}$.
- a round number r in $\{0,\dots,R-1\}$ and for each player i in S a sequence of messages $m^i(r) = (m^i_1,\dots,m^i_r) \in M^r$.

Assume that each player i in $N\backslash T_1$ sends messages according to σ^i and each player i in S sends at each round $r' = 1,\dots,r$ the message $m^i_{r'}$. Because of inclusion (5), this defines by induction, for each player i in $N\backslash T_1$, the message sent by player i at each round $r' = 1,\dots,r+1$. We denote the corresponding sequence of messages sent by such player i at rounds $1,\dots,r$ by:

$$m^i(r)\big(\sigma^{N\backslash T_1}, (m^j(r))_{j\in S}\big) \in M^r.$$

Symmetrically, for i in $N'\backslash T'_1$, r in $\{0,\dots,R-1\}$, given a vector of pure strategies $\sigma^{N'\backslash T'_1} = (\sigma^j)_{j\in N'\backslash T'_1}$ for the players in $N'\backslash T'_1$ and for each j in S' a sequence of messages $m^j(r) = (m^j_1,\dots,m^j_r) \in M^r$, we denote by:

$$m^i(r)\big(\sigma^{N'\backslash T'_1}, (m^j(r))_{j\in S'}\big) \in M^r,$$

the sequence of messages sent by player i at the rounds $r' = 1,\dots,r$ if: each player j in $N'\backslash T'_1$ use σ^j and each player j in S' has sent at each round $r' \le r$ the message $m^j_{r'}$. This definition makes sense because of inclusion (6).

6.1.1. *Construction of* τ^T

We formally construct τ^T as a mixed strategy for the adversary controlling the players in T. To define τ^T, we have to define which message is sent by each player in T at each round. It is particularly simple for the players in $T_2 \cup T''$, but more complicated for the players in T_1. The procedure is the following.

- The adversary first selects, for each player $i \neq a$ in N, a pure strategy σ^i according to the probability $\tilde{\sigma}^i$ and for player a he selects a pure strategy σ^a according to $\tilde{\sigma}^a_{\omega'}$. The idea is that the adversary pretends that the state is ω' and that every player i in N plays according to σ^i.
- Each player in $T_2 \cup T''$ follows a very simple strategy: send the message m_0 at each round, whatever happens.
- Fix some player i in T_1, then $i \in N$. At round 1, i plays according to the selected pure strategy σ^i. Fix now r in $\{1,\dots,R-1\}$ in order to define what is played by player i at round $r+1$. At the end of round r, the adversary knows all previous messages multicast by the players in $G(T)$, which we denote by $(m^j(r))_{j\in G(T)}$. Player i will play at round $r+1$ according to the pure strategy σ^i and multicasts the message $\sigma^i((\hat{m}^j(r))_{j\in G(i)})$, which is the prescription of the pure strategy σ^i at round $r+1$ if the messages previously observed by player i correspond to

$(\hat{m}^j(r))_{j\in G(i)}$. The point is that these messages $(\hat{m}^j(r))_{j\in G(i)}$ are not the messages previously sent by the neighbors of i, but are fictitious messages that we define now.

Fix j in $G(i)$. $i \in N$, so j belongs to $N \vee B \vee T'' \vee T_2' \vee (T_1' \cap G(T))$ by inclusion (1) of Lemma 6.1.

- If j belongs to T_2', the adversary will pretend that j is sending the message m_0 at each round: $\hat{m}^j(r) = (m_0, m_0, \ldots, m_0)$.
- If j belongs to $T_1 \vee B \vee T'' \vee (T_1' \cap G(T))$, the adversary will not cheat on the messages sent by player j: $\hat{m}^j(r) = m^j(r)$.
- If j belongs to $N\backslash T_1$, the adversary will pretend that player j has sent messages corresponding to the case where: (a) the players in $N\backslash T_1$ use $\sigma^{N\backslash T_1} = (\sigma^l)_{l\in N\backslash T_1}$, (b) each player k in $T_1 \vee (T_1' \cap G(T)) \vee T''$ has sent the sequence of messages $l^k(r) = m^k(r)$, which is known by the adversary since in this case $k \in G(T)$, and (c) each player k in T_2' has played at each round the message m_0, i.e. has sent the sequence $l^k(r) = (m_0, \ldots, m_0) \in M^r$. Since $S = T'' \vee T_1 \vee T_2' \vee (T_1' \cap G(T))$, these messages $\hat{m}^j(r)$ correspond to the notation:

$$\hat{m}^j(r) = m^j(r)\big(\sigma^{N\backslash T_1}, (l^k(r))_{k\in S}\big).$$

This concludes the definition of the strategy τ^T of the adversary. The construction of $\bar{\tau}^{T'}$ is perfectly symmetric and is given now for the sake of completeness.

6.1.2. *Construction of* $\bar{\tau}^{T'}$

To play according to $\bar{\tau}^{T'}$, the procedure is the following.

- The adversary first selects, for each player $i \neq a$ in N', a pure strategy σ^i according to the probability $\tilde{\sigma}^i$ and for player a he selects a pure strategy σ^a according to $\tilde{\sigma}^a_\omega$. The idea is that the adversary will pretend that the state is ω and that every player i in N' is playing according to σ^i.
- Each player in $T_2' \cup T''$ simply sends at each round the message m_0.
- Fix some player i in $T_1' \subset N'$. At round 1, i plays according to the selected pure strategy σ^i. Fix r in $\{1, \ldots, R-1\}$. At the end of round r, the adversary knows the previous messages sent by the players in $G(T')$, which we denote by $(m^j(r))_{j\in G(T')}$. Player i will play at round $r+1$ according to the pure strategy σ^i, and will send the message $\sigma^i((\hat{m}^j(r))_{j\in G(i)})$, which is the prescription of the pure strategy σ^i at round $r+1$ if the messages previously observed by player i correspond to the quantity $(\hat{m}^j(r))_{j\in G(i)}$, which is defined now.

  Fix j in $G(t)$. j belongs to $N' \vee B \vee T'' \vee T_2 \vee (T_1 \cap G(T'))$ by inclusion (2) of Lemma 6.1.
  - If j belongs to T_2, the adversary will pretend that j is sending the message m_0 at each round: $\hat{m}^j(r) = (m_0, m_0, \ldots, m_0)$.
  - If j belongs to $T_1' \vee B \vee T'' \vee (T_1 \cap G(T'))$, the adversary will not cheat on the messages sent by player j: $\hat{m}^j(r) = m^j(r)$.
  - If j belongs to $N'\backslash T_1'$, we let $\hat{m}^j(r) = m^j(r)(\sigma^{N'\backslash T_1'}, (l^k(r))_{k\in S'})$, where: $\sigma^{N'\backslash T_1'} = (\sigma^l)_{l\in N'\backslash T_1'}$, $l^k(r) = m^k(r)$ for each k in $T_1' \vee (T_1 \cap G(T')) \vee T''$, and $l^k(r) = (m_0, \ldots, m_0) \in M^r$ for each k in T_2.

6.1.3. *Conclusion*

We finally show that player b cannot distinguish between $\{\omega$ is the state, all players in $V\backslash T$ play according to σ and the adversary controls the players in T with $\tau^T\}$ and $\{\omega'$ is the state, all players in $V\backslash T'$ play according to σ and the adversary controls the players in T' with $\bar{\tau}^{T'}\}$. Formally, we prove that $\mathbf{P}_{\omega,\pi,\tau^T}$ and $\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}$ induce the same probability distributions over the messages sent at rounds $1,\dots,R$ by the players in $\overline{B} =_{def} B\vee T_1\vee T_1'\vee T''$. Since $b\in B$ and $G(B)\subset\overline{B}$, this will show that $\mathbf{P}_{\omega,\pi,\tau^T}(D) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(D)$ and conclude the proof.

For each player i in $N\cup N'$, we view $\tilde{\sigma}^i$ ($\tilde{\sigma}^a_\omega$ and $\tilde{\sigma}^a_{\omega'}$ for player a) as a mixed strategy and we think as if player i using $\tilde{\sigma}^i$ ($\tilde{\sigma}^a_\omega$ or $\tilde{\sigma}^a_{\omega'}$ for player a) first selects a pure strategy according to this probability and then plays this pure strategy. If σ^i is a pure strategy of player i, we denote by $\tilde{\sigma}^i(\sigma^i)$ the induced probability to select σ^i. We define, for any vector of pure strategies $\sigma^N = (\sigma^i)_{i\in N}$ and $\bar{\sigma}^{N'} = (\sigma^i)_{i\in N'}$, the following events:

$$\begin{aligned} H_T(\sigma^N,\bar{\sigma}^{N'}) = \{&\text{the adversary } T \text{ playing } \tau^T \text{ first selects } \sigma^N \text{ and}\\ &\text{each player } i \text{ in } N' \text{ playing } \tilde{\sigma}^i \text{ selects } \bar{\sigma}^i\},\\ H_{T'}(\sigma^N,\bar{\sigma}^{N'}) = \{&\text{each player } i \text{ in } N \text{ playing } \tilde{\sigma}^i \text{ selects } \sigma^i, \text{ and}\\ &\text{the adversary } T' \text{ playing } \bar{\tau}^{T'} \text{ first selects } \bar{\sigma}^{N'}\}. \end{aligned}$$

Notice that:

$$\begin{aligned} \mathbf{P}_{\omega,\pi,\tau^T}(H_T(\sigma^N,\bar{\sigma}^{N'})) &= \prod_{i\in N, i\neq a}\tilde{\sigma}^i(\sigma^i)\times\tilde{\sigma}^a_{\omega'}(\sigma^a)\times\prod_{i\in N', i\neq a}\tilde{\sigma}^i(\bar{\sigma}^i)\times\tilde{\sigma}^a_{\omega}(\bar{\sigma}^a)\\ &= \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}(H_{T'}(\sigma^N,\bar{\sigma}^{N'})). \end{aligned}$$

Fix now any sequence of messages $(m^i(R))_{i\in\overline{B}}$, where for each i, $m^i(R) = (m^i_1,\dots,m^i_R)\in M^R$ corresponds to the messages played by player i at rounds $1,\dots,R$. If for all pairs $(\sigma^N,\bar{\sigma}^{N'})$ we show that,

$$\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i(R)_{i\in\overline{B}})|H_T(\sigma^N,\bar{\sigma}^{N'})\big) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i(R)_{i\in\overline{B}})|H_{T'}(\sigma^N,\bar{\sigma}^{N'})\big),$$

then we obtain $\mathbf{P}_{\omega,\pi,\tau^T}((m^i(R)_{i\in\overline{B}})) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}((m^i(R)_{i\in\overline{B}}))$, which concludes the proof. We fix then a pair $(\sigma^N,\bar{\sigma}^{N'})$. To prove that:

$$\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i(R)_{i\in\overline{B}})|H_T(\sigma^N,\bar{\sigma}^{N'})\big) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i(R)_{i\in\overline{B}})|H_{T'}(\sigma^N,\bar{\sigma}^{N'})\big),$$

we proceed by induction on R. It is then sufficient to prove the following lemma.

Lemma 6.2. *For each r in $\{0,\dots,R-1\}$,*

$$\begin{aligned} &\mathbf{P}_{\omega,\pi,\tau^T}\big((m^i_{r+1})_{i\in\overline{B}}|H_T(\sigma^N,\bar{\sigma}^{N'}),(m^i(r))_{i\in\overline{B}}\big)\\ &\quad= \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\big((m^i_{r+1})_{i\in\overline{B}}|H_{T'}(\sigma^N,\bar{\sigma}^{N'}),(m^i(r))_{i\in\overline{B}}\big), \end{aligned}$$

where by convention the equality for $r = 0$ is:

$$\mathbf{P}_{\omega,\pi,\tau^T}\left((m_1^i)_{i\in\overline{B}}|H_T(\sigma^N,\bar{\sigma}^{N'})\right) = \mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\left((m_1^i)_{i\in\overline{B}}|H_{T'}(\sigma^N,\bar{\sigma}^{N'})\right).$$

Proof of Lemma 6.2. We compute $\mathbf{P}_{\omega,\pi,\tau^T}((m_{r+1}^i)_{i\in\overline{B}}|H_T(\sigma^N,\bar{\sigma}^{N'}),(m^i(r))_{i\in\overline{B}})$. We thus assume that: ω is the state, the adversary controls T, plays τ^T and has selected σ^N, the players in N' play according to the pure strategy $\bar{\sigma}^{N'}$ and at the first r rounds the messages really sent by each player i in $\overline{B}$ corresponds to $m^i(r)$. What is played by the players in $\overline{B} = B \vee T_1 \vee T_1' \vee T''$ at round $r+1$?

- Each player i in B plays $\tilde{\sigma}^i$ and has received the messages $(m^j(r))_{j\in G(i)}$, so he sends at round $r+1$ his message according to the probability $\tilde{\sigma}^i(m^j(r))_{j\in G(i)}$.
- Each player i in T'' plays m_0 at each round, so he sends (with probability one) the message m_0 at round $r+1$.
- Consider a player i in T_1', i belongs to $N'\backslash(T\cup N)$ thus to $N'\backslash T$ so i uses the pure strategy $\bar{\sigma}^i$. At round $r+1$ he sends the message $\bar{\sigma}^i((\bar{m}^j(r))_{j\in G(i)})$, where for each j in $G(i)$, $\bar{m}^j(r)$ denotes the stream of messages really sent by player j at the first r rounds. For each j in $G(i)$, we compute $\bar{m}^j(r)$. We have $j\in G(i)\subset G(N')\subset (N'\backslash T_1')\vee T_1'\vee B\vee T''\vee T_2\vee(T_1\cap G(T'))$ by inclusion (2) of Lemma 6.1.
  - If $j\in T_1'\vee B\vee T''\vee(T_1\cap G(T'))$, j belongs to $\overline{B}$ so $\bar{m}^j(r)=m^j(r)$.
  - If $j\in T_2$, by definition of τ^T, player j plays m_0 at each round: $\bar{m}^j(r)=(m_0,\ldots,m_0)$.
  - If $j\in N'\backslash T_1'$, we also need to compute $\bar{m}^j(r)$. The players in $N'\backslash T_1'$ are using the pure strategy $\bar{\sigma}^{N'\backslash T_1'}$, each player k in $T_1'\vee T''\vee(T_1\cap G(T'))\subset\overline{B}$ has played $m^k(r)$ and each player k in T_2 is controlled by the adversary and has played m_0 at each round. So $\bar{m}^j(r)$ is exactly what we have defined as: $m^j(r)(\bar{\sigma}^{N'\backslash T_1'},(l^k(r))_{k\in S'})$, with $l^k(r)=m^k(r)$ if $k\in T_1'\vee T''\vee(T_1\cap G(T'))$ and $l^k(r)=(m_0,\ldots,m_0)$ if $k\in T_2$.
- Consider finally a player i in T_1. Player i is controlled by the adversary so he plays according to the pure strategy σ^i and at round $r+1$ he sends the message $\sigma^i(\hat{m}^j(r))_{j\in G(i)})$, where for each j in $G(i)$, $\hat{m}^j(r)$ is defined as follows by the strategy τ^T.
  - If $j\in T_1\vee B\vee(T_1'\cap G(T))\vee T''$, $\hat{m}^j(r)=m^j(r)$.
  - If $j\in T_2'$, $\hat{m}^j(r)=(m_0,\ldots,m_0)$.
  - If $j\in N\backslash T_1$, $\hat{m}^j(r)=m^j(r)(\sigma^{N\backslash T_1},(l^k(r))_{k\in S})$ with $l^k(r)=m^k(r)$ if $k\in T_1\vee(T_1'\cap G(T))\vee T''$ and $l^k(r)=(m_0,\ldots,m_0)$ if $k\in T_2'$.

We have computed, for each player i in $\overline{B}$, the probability that he plays m_{r+1}^i at round $r+1$.

$$\mathbf{P}_{\omega,\pi,\tau^T}\left((m_{r+1}^i)_{i\in\overline{B}}|H_T(\sigma^N,\bar{\sigma}^{N'}),(m^i(r))_{i\in\overline{B}}\right)$$

is nothing but the product of these probabilities and one can check that it is a symmetric expression of (T,σ^N), $(T',\bar{\sigma}^{N'})$. So this equals

$$\mathbf{P}_{\omega',\pi,\bar{\tau}^{T'}}\left((m_{r+1}^i)_{i\in\overline{B}}|H_{T'}(\sigma^N,\bar{\sigma}^{N'}),(m^i(r))_{i\in\overline{B}}\right)$$

and the proof of the first case is complete. □

6.2. *Second Case*

The second case is when all paths from A to B go through T or when all paths from A to B go through T'. By symmetry, it is sufficient to assume that all paths from A to B go through T. The idea is that T separates A from B and it suffices for the adversary controlling T to pretend that the state is ω' and that there is no adversary. This case is easier than the previous one and we just define τ^T and $\bar{\tau}^{T'}$ without going into computations.

Formally, $\bar{\tau}^{T'}$ is just "do not deviate", i.e. in order to play according to $\bar{\tau}^{T'}$, each player i in T' just uses $\tilde{\sigma}^i$. In order to construct τ^T, we define:

$$\overline{A} = \{i \in V \backslash T, \text{ there exists a path from } a \text{ to } i \text{ in } V \backslash T\} \quad \text{and} \quad \overline{B} = V \backslash (\overline{A} \cup T).$$

We have $V = \overline{A} \vee T \vee \overline{B}$, $A \subset \overline{A}$, $B \subset \overline{B}$, $G(\overline{A}) \subset \overline{A} \cup T$ and $G(\overline{B}) \subset \overline{B} \cup T$. To play according to τ^T:

- the adversary first selects a pure strategy σ^a according to $\tilde{\sigma}^a_{\omega'}$ and for each player $i \neq a$ in $\overline{A} \cup T$ a pure strategy σ^i according to $\tilde{\sigma}^i$.
- fix i in T, and r in $\{0, \ldots, R-1\}$. At the end of stage r, the adversary knows the sequence of messages $m^j(r) \in M^r$ sent by each player j in $G(T)$ at the rounds $1, \ldots, r$. Player i will play at round $r+1$ the message $\sigma^i((\hat{m}^j(r))_{j \in G(i)})$, where: for j in $\overline{B} \cup T$, $\hat{m}^j(r) = m^j(r)$ and for j in $\overline{A}$, $\hat{m}^j(r)$ is the sequence of messages that j would have sent at the rounds $1, \ldots, r$ if each player k in $\overline{A}$ plays σ^k whereas each player k in T has sent messages according to $m^k(r)$.

One can show that (ω, π, τ^T) and $(\omega', \pi, \bar{\tau}^{T'})$ induce the same distributions over the messages sent by the players in $\overline{B} \cup T$. The proof is similar to that of the first case (one can consider, for each vector of pure strategies $\sigma^{\overline{A} \cup T} = (\sigma^i)_{i \in \overline{A} \cup T}$, the hypotheses: $H_T(\sigma^{\overline{A} \cup T}) = \{$the adversary playing τ^T has first selected σ^i for each player i in $\overline{A} \cup T\}$ and $H_{T'}(\sigma^{\overline{A} \cup T}) = \{$every player i in $\overline{A} \cup T$ playing $\tilde{\sigma}^i$ selects $\sigma^i\}$). Since $b \in \overline{B}$ and $G(\overline{B}) \subset \overline{B} \cup T$, this is sufficient to conclude this second case.

Acknowledgements

We wish to thank two anonymous referees for helpful remarks and comments. This work was done while Tristan Tomala was at CEREMADE.

References

[1] R.J. Aumann, L.S. Shapley, Long-term competition—a game theoretic analysis, in *Essays on Game Theory*, ed. by N. Megiddo (Springer, New York, 1994), pp. 1–15.

[2] A. Beimel, M. Franklin, Reliable communication over partially authenticated networks. *Theor. Comput. Sci.* **220**, 185–210 (1999)

[3] A. Beimel, L. Malka, Efficient reliable communication over partially authenticated networks, in *Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing* (2003), pp. 233–242

[4] E. Ben-Porath, M. Kahneman, Communication in repeated games with private monitoring. *J. Econ. Theory* **70**, 281–297 (1996)

[5] Y. Desmedt, Y. Wang, Secure communication in multicast channels: the answer to Franklin and Wright's question. *J. Cryptol.* **14**(2), 121–135 (2001)

[6] D. Dolev, The Byzantine general strikes again. *J. Algorithms* **3**, 14–30 (1982)
[7] D. Dolev, C. Dwork, O. Waarts, M. Yung, Perfectly secure message transmission. *J. Assoc. Comput. Mach.* **40**(1), 17–47 (1993)
[8] H.W. Kuhn, Extensive games and the problem of information, in *Contributions to the Theory of Games,* vol. II, ed. by Kuhn and Tucker, Annals of Mathematic Study, vol. 28 (Princeton University Press, Princeton, 1953)
[9] M. Franklin, R.N. Wright, Secure communication in minimal connectivity models. *J. Cryptol.* **13**(1), 9–30 (2000)
[10] M. Franklin, M. Yung, Secure hypergraphs: privacy from partial broadcast, in *Proceedings of the 27th ACM Symposium on the Theory of Computing* (1995), pp. 36–44
[11] J. Renault, T. Tomala, Repeated proximity games. *Int. J. Game Theory* **27**, 539–559 (1998)
[12] J. Renault, T. Tomala, Learning the state of nature in repeated game with incomplete information and signals. *Games Econ. Behav.* **47**, 124–156 (2004)
[13] K. Srinathan, C. Pandu Rangan, Possibility and complexity of probabilistic reliable communication in directed networks, in *PODC'06*, July 2006