Communication fiable et sécurisée dans des réseaux

Jérôme Renault

GIS “Sciences de la décision", CMAP et Dpt d'Economie, Ecole Polytechnique

Jeux et Informatique, Chevaleret, 18-02-2009

General context: strategic communication.

Given a communication network, find procedures allowing the players to communicate, in a way that is not manipulable by some "bad" players.

Examples: large computer networks, neural systems.

We want to design protocols (*strategies*) with good properties.

Several goals:
- how to transmit a piece of information (*reliable communication*)
- how to transmit a piece of information in a secrete way (*secure, or private, communication*)
- the information to be transmitted may be exogeneous, or generated by the protocol (*protocols for fault identification*)
- how to generate a common information (*Byzantine agreement problems*)

...

Typically:

• The identities of the bad players are unknown. These players may be *curious*, *malicious*...

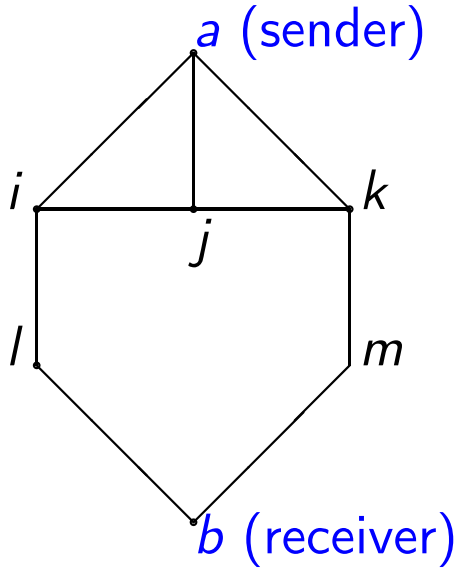
• The communication network is represented by a graph (players=nodes). The communication can be *unicast*, or *multicast*. The graph may be known or unknown.

This talk:

The communication is multicast in a known network.
Player a (the sender) knows some information $\omega \in \{\omega_1, \omega_2\}$, and wants to send ω to player b (the receiver).
At most t malicious bad players.

joint work with T. Tomala, HEC.

• a network $G = (V, E)$ (undirected graph)
- nodes: players. at each round, every player i cand send a finite message and all the neighbors of i receive this message.
- 2 particular players are fixed: a (sender) wants to send some info $\omega \in \{\omega_1, \omega_2\}$ to b (receiver).



• an integer t in $\{0, ..., |V| - 2\}$.
Some malevolent adversary may take the control of t players in $V \backslash \{a, b\}$.
Define $\mathbf{A}_t = \{T \subset V \backslash \{a, b\}, |T| \leq t\}$.

• Reliability: The communication from a to b is t-reliable if no malicious adversary controling t nodes can prevent player a to send the information to player b.

• Security: The communication from a to b is t-secure if no malicious adversary controling t nodes can prevent player a to send privately the information to player b.

References:
- t=1 reliability Renault Tomala GEB 04
- neighbor-disjoint paths. Franklin-Wright, Journal of Cryptology 00
- general case: RT Probabilistic reliability and privacy of communication using multicast in general neighbor networks, Journal of Cryptology 08.

Definitions:

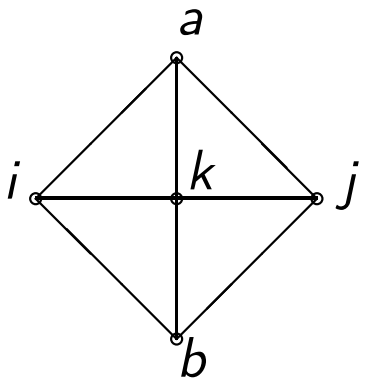
- A communication protocol π is given by:
  - a message space M (finite set),
  - a number of rounds R (positive integer),
  - a vector of behavioral strategies $\sigma = (\sigma^i)_{i \in V}$,
  - and a subset D of histories of length R for player b.

- The communication from a to b is t-reliable if for every $\varepsilon > 0$, there exists a protocol π such that: $\forall T \in \mathbf{A}_t$, $\forall \tau^T$ correlated strategy of the players in T, we have:

$$I\!P_{\omega_1,\pi,\tau^T}(D) \geq 1 - \varepsilon, \text{ and } I\!P_{\omega_2,\pi,\tau^T}(D) \leq \varepsilon.$$

Examples with $t = 1$

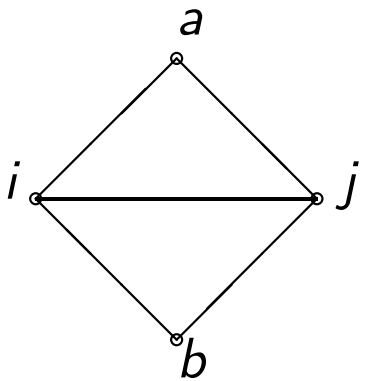
Example 1:



1-reliable

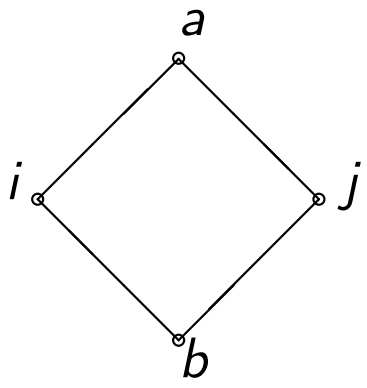
$M = \{\omega_1, \omega_2\}, R = 2$.
round 1: player a sends the true value ω_1 or ω_2.
round 2: every player i, j, k, repeats the announce of a.
$D = \{$ histories of player b where at least 2 players among i, j, k announce ω_1 at round 2$\}$.

Example 2:



not 1-reliable

Example 3:



1-reliable

Take $M = F_q$ large field.

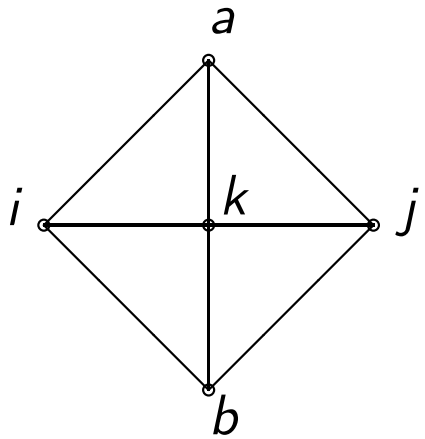
• round 1: players i (resp. j) selects m^i (resp. m^j) uniformly in M, and announces m^i (resp. m^j).
• round 2: if $\omega = \omega_1$, player a announces the sum $m^i + m^j$. if $\omega = \omega_2$, player a selects a message uniformly in M, and announces it.
• round 3: players i and j repeat the message announced at round 2 by player a.

$D = \{$ the message announced by i or by j at round 3 is $m^i + m^j\}$.
For $T = \{i\}$ or $T = \{j\}$, $I\!P_{\omega_1,\pi,\tau_T}(D) = 1$, and $I\!P_{\omega_2,\pi,\tau_T}(D) \leq 2/q$.

Theorem: Reliability, $t = 1$

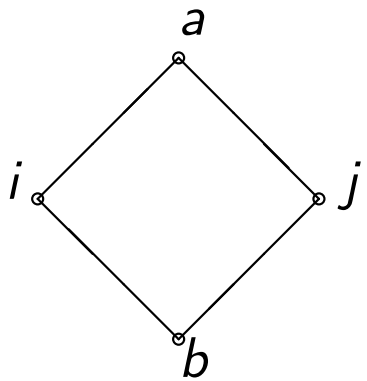
The communication from a to b is 1-reliable if and only if for every i and j in $V \backslash \{a, b\}$:

- there exists a path from a to b in $V \backslash \{i, j\}$,



or

- there exists a path from a to b not going through i, there exists a path from a to b not going through j, and i and j are not neighbours.

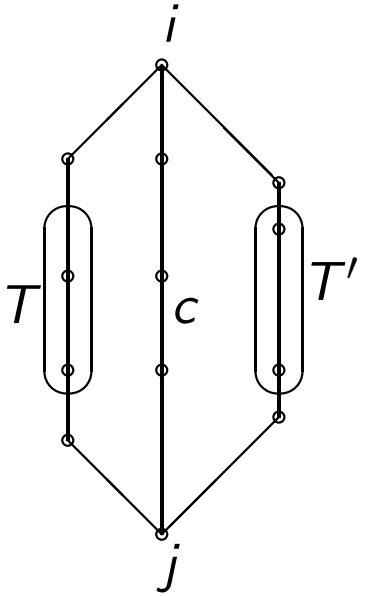


Reliability: general case

Fix T and T' in $\mathbf{A}_t$. Define a binary relation $\Gamma_{T,T'}$ on $V \backslash (T \cup T')$:

$\Gamma_{T,T'}(i,j)$ holds if:

(1) There is a path c from i to j with $c \subset V \backslash (T \cup T')$



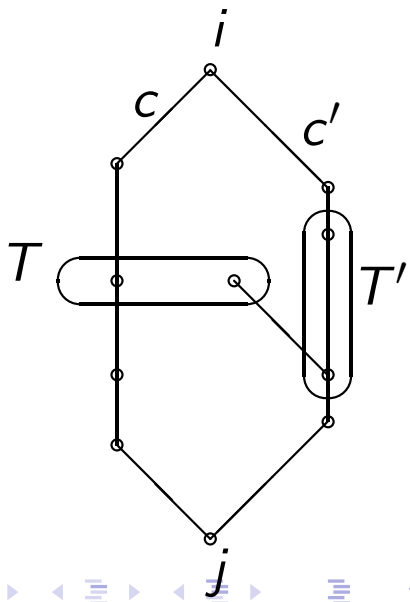
Or

(2) There is a pair of paths c, c' from i to j such that:

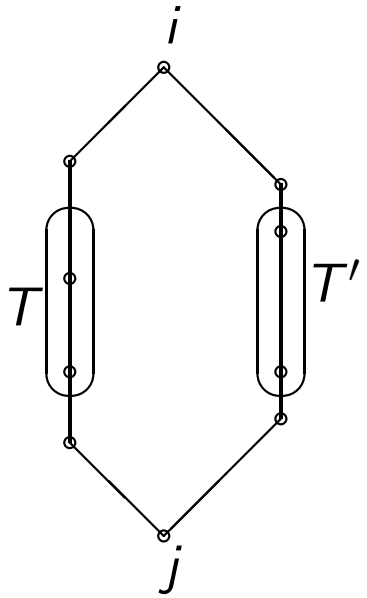
(i) $c \subset V \backslash T'$, $c' \subset V \backslash T$ and

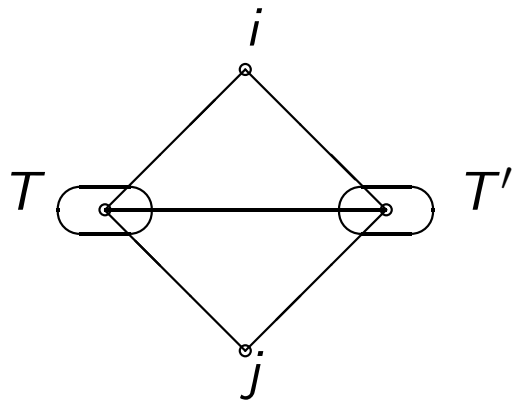
(ii) ($c \cap T$ is a singleton not seen by T')

or ($c \cap T'$ is a singleton not seen by T)



Examples without $\Gamma_{T,T'}(i,j)$:





$\Gamma_{T,T'}$ is reflexive, symetric but need not be transitive. Denote by $C_{T,T'}$ its transitive closure (associated equivalence).

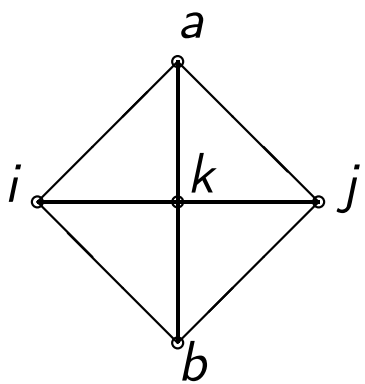
Theorem

The communication from a to b is t-reliable if and only if we have $C_{T,T'}(a,b)$ for every T, T' in $\mathbf{A}_t$.

Definition:
The communication from a to b is t-secure if for every $\varepsilon > 0$, there exists a protocol π such that: $\forall T \in \mathbf{A}_t$, $\forall \tau^T$ correlated strategy of the players in T, we have:
(i) $I\!P_{\omega_1,\pi,\tau^T}(D) \geq 1-\varepsilon$, and $I\!P_{\omega_2,\pi,\tau^T}(D) \leq \varepsilon$. (*reliability*),
and
(ii) $\|P^T_{\omega_1,\pi,\tau^T} - P^T_{\omega_2,\pi,\tau^T}\|_1 \leq \varepsilon$ (*privacy*), where P^T_{ω,π,τ^T} is the marginal distribution of P_{ω,π,τ^T} on the set of R-histories of players in T.

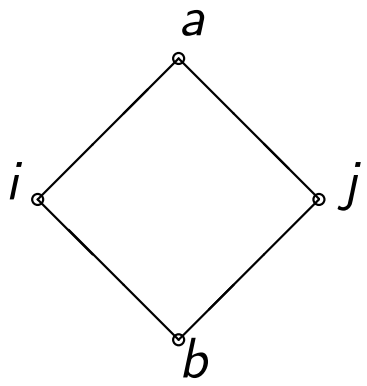
$$\textit{secure} \Longrightarrow \textit{reliable}$$

Example 1:



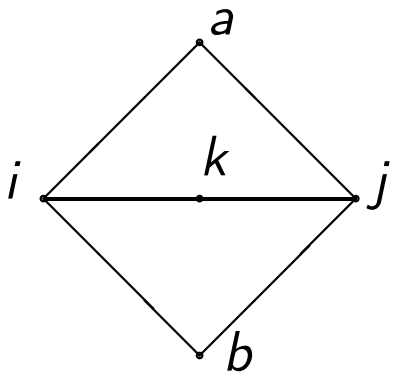
1-reliable, but not 1-secure

Example 3:



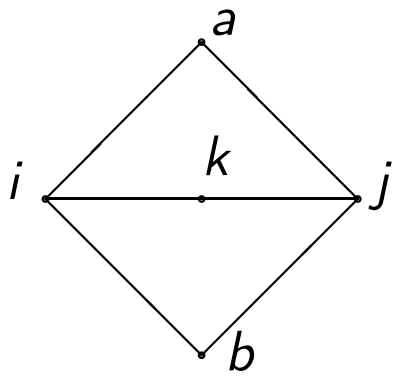
1-reliable and 1-secure

Example 4:



Can player a send
a private message to player b ?

Yes ! 1-secure.



Sketch of Proof: $M = F_q$ large field. $V := \{i, j, k\}$ set of possible adversaries.

Sub-protocol $\{l\}$, for l in V: player a sends a message $m^l \in M$ to player b, keeping it secret from l.
example for $l = k$.
round 1: a selects and announces m^a uniformly in M, whereas b selects and announces m^b uniformly in M.
round 2: j announces $m^a + m^b$
Player b can then compute $(m^a + m^b) - m^b = m^a$, player k can not.

but this can be manipulated by player j.

A reliable and private protocol:

(1) for every l in V, player a selects a message $m_l^a = (c_l^a, d_l^a)$ uniformly in M^2, and sends it to b, *keeping it secret from* l. $m_l^b = (c_l^b, d_l^b)$ received by b.

(2) for every l in V, b selects r_l uniformly in M, compute $s_l = c_l^b r_l + d_l^b$, and sends r_l and s_l *in a reliable way* to a.

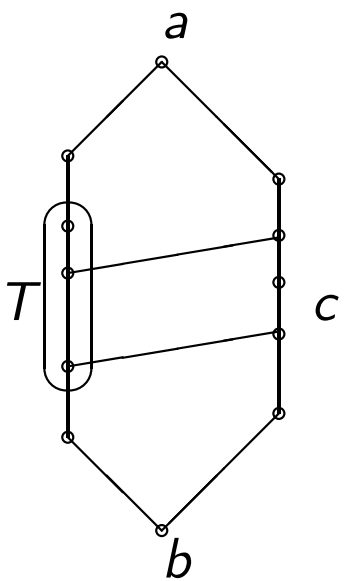
(3) a computes and announces to b *in a reliable way*:
$W = \{l \in V, s_l = c_l^a r_l + d_l^a\}$, and $z = \omega + \sum_{l \in W} c_l^a$.

$$\text{Finally, } b \text{ computes } \hat{\omega} = z - \sum_{l \in W} c_l^b.$$

Idea: suppose that j is deviating in a way such that $m_k^a \neq m_k^b$, and $m_i^a = m_i^b$.
Then $m_j^a = m_j^b$, and with high proba $W = \{i, j\}$, and $z = \omega + c_i^a + c_j^a$.
$c_l^a = c_l^b$ for l in W, so $\omega = \hat{\omega}$, player b gets the info.
j knows at most $z = \omega + c_i^a + c_j^a$ and c_i^a, but not c_j^a.

Theorem

The communication from a to b is t-secure if and only if:
1) it is t-reliable, and
2) for each T in $\mathbf{A}_t$, there is a path c from a to b in $V \setminus T$ such that T has no consecutive neighbors in c .



Remarks:

- the proof generalizes to the case when the set of bad players belongs to a given family.
- unicast communication: seems to decrease the reliability and security here.
- directed graphs: open, even for $t = 1$.
- what if the graph is unknown ?
- efficiency regarding the number of rounds, minimal graphs ?

A. Beimel and M. Franklin.
Reliable communication over partially authenticated networks,
Theoretical computer science, 220: 185-210, 1999.

A. Beimel and L. Malka.
Efficient reliable communication over partially authenticated networks,
In
Proc. of the 22nd ACM symp. on Principles of Distributed Computing, 233-242, 2003.

Y. Desmedt and Y. Wang.
Secure Communication in multicast channels: The answer to Franklin and Wright's question,
J. of Cryptology,14(2):121-135 (2001).

D. Dolev,
The Byzantine general strikes again,
J. Algorithms,3:14-30, 1982.

D. Dolev, C. Dwork, O. Waarts and M. Yung.
Perfectly secure message transmission,
J. Association for Computing Machinery,40(1):17–47, 1993.


M. Franklin and R.N. Wright.
Secure Communication in minimal connectivity models.
Journal of Cryptology, 13, 9–30, 2000.


] M. Franklin and M. Yung.
Secure hypergraphs: Privacy from partial broadcast,
Proc. of the 27th ACM symp. on the theory of Computing, 36-44, 1995.


N. Linial.
Game-Theoretic aspects of computing,
Handbook of Game Theory, vol.2, chapter 38. Aumann and Hart editors, 1994.


J. Renault and T. Tomala.
Repeated proximity games,
International Journal of Game Theory, 27:539–559, 1998.


J. Renault.
Learning sets in state dependent signalling game forms: a characterization,
Mathematics of Operations Research, 26, 832–850, 2001.


J. Renault and T. Tomala.
Learning the state of nature in repeated games with incomplete information and signals,
Games and Economic Behavior, 47:124–156, 2004.


J. Renault and T. Tomala.
Probabilistic reliability and privacy of communication using multicast in general neighbor networks,
Journal of Cryptology, volume 21, 250-279, 2008.


K. Srinathan and C. Pandu Rangan.
Possibility and complexity of probabilistic reliable communication in directed networks,
PODC'06, July 2006.


T. Tomala.
Protocols for Fault Identification in partially known networks.
Discussion paper, https://studies2.hec.fr/jahia/Jahia/lang/fr/pid/2327
2008.