ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Fair Exchange with Guardian Angels

Gildas AVOINE & Serge VAUDENAY

http://lasecwww.epfl.ch

Swiss Federal Institute of Technology (EPFL)

This work is supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center supported by the Swiss National Science Foundation.

LASEC

Outline

- Ad Hoc Networks
- Fair Exchange Problem
- Synchronization Problem
- Fair Exchange with Guardian Angels
- Analysis of the Protocol

Security aspects in Ad Hoc Networks

Brave new world

An ad hoc network is not the *Brave new world* described by Aldous Huxley! Here each terminode potentially misbehaves.

- It may cheat in order to maximize his benefits, to save his battery or to harm another terminode.

- It may be corrupted: nobody can be trusted anymore.

Special issues

Ad Hoc networks are more difficult to secure than fixed infrastructures.

- Mobility (e.g. problem to establish security associations).
- Low cost devices (e.g. terminodes cannot be tamper-proof).
- No central trusted party.
- Etc.

No central trusted party

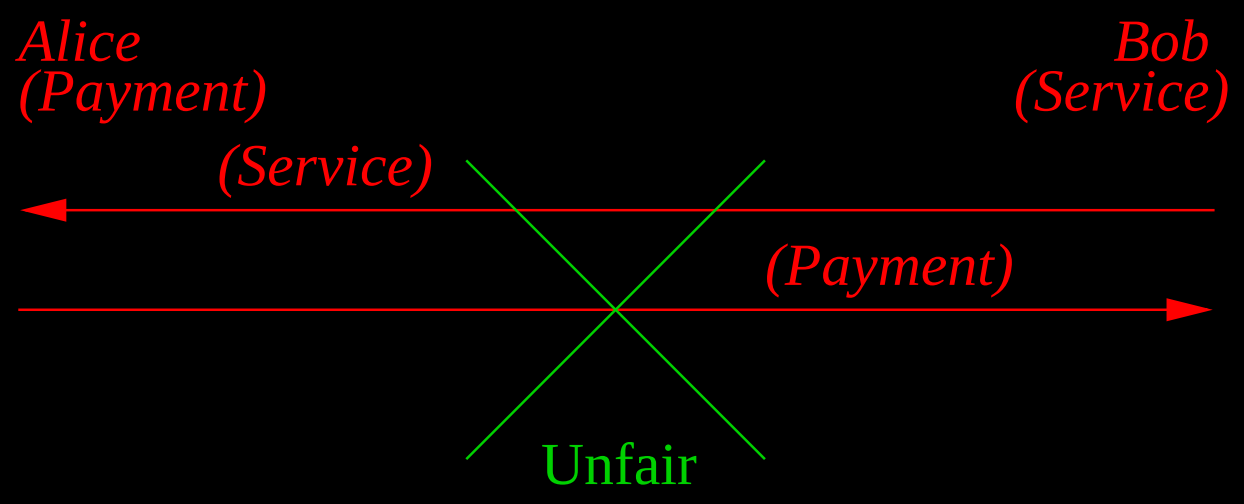
Public Key Management:

- How can you be ensured with whom you communicate if you cannot use public keys authentication?

E-commerce:

- How can you securely exchange a service against a payment without any trusted trader?

E-commerce



Using trusted security modules

One way to mitigate the lack of central trusted party is to add one trusted security module to each terminode.

These modules could be delivered by an authority (provider, manufacturer, government agency, etc.).

Modules are kinds of distributed trusted parties.

Guardian Angels

Security modules are called Guardian Angels (They have to enforce the Terminodes good behavior!).

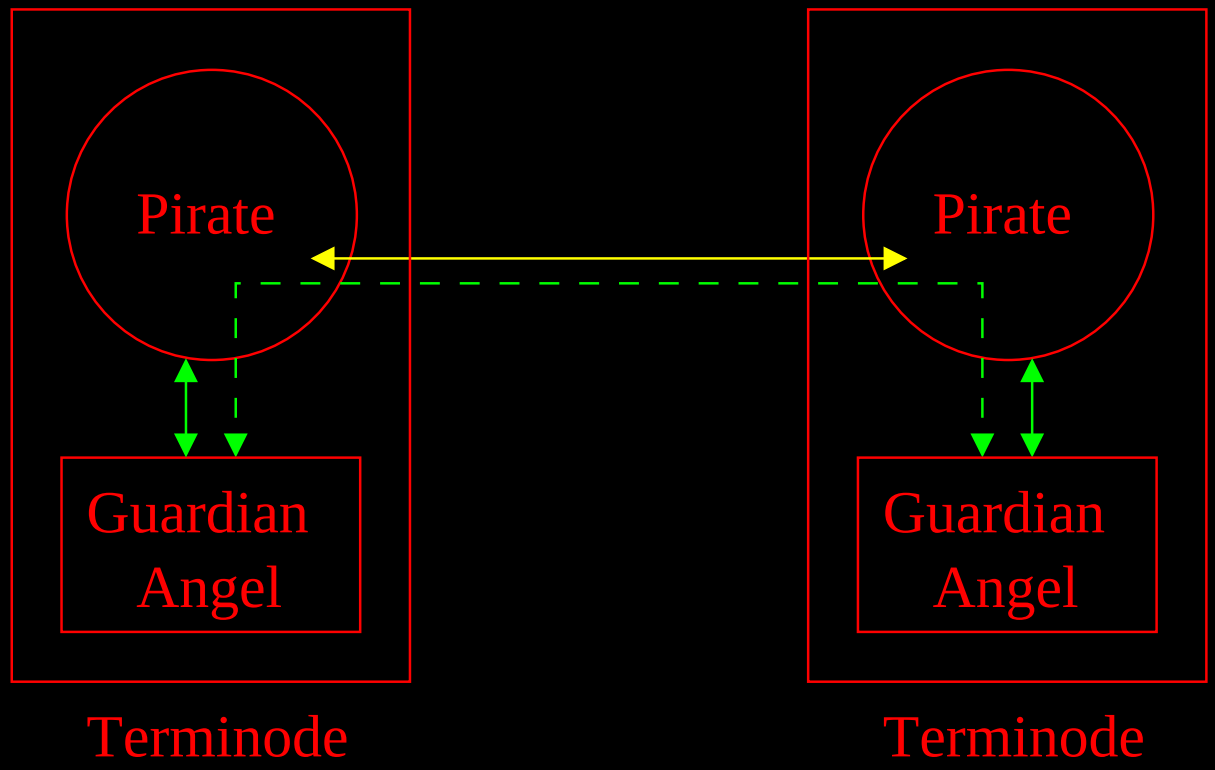
- Tamper-proof (e.g. smartcard)
- Simple and limited (computation, storage)
- Single i/o port (connected to their own device)

Pirates

Potentially misbehaving devices are called Pirates (They try to cheat as soon as they want!).

Pirates are powerful in the sense that they are able to communicate with all the other Pirates and their own Guardian Angel.

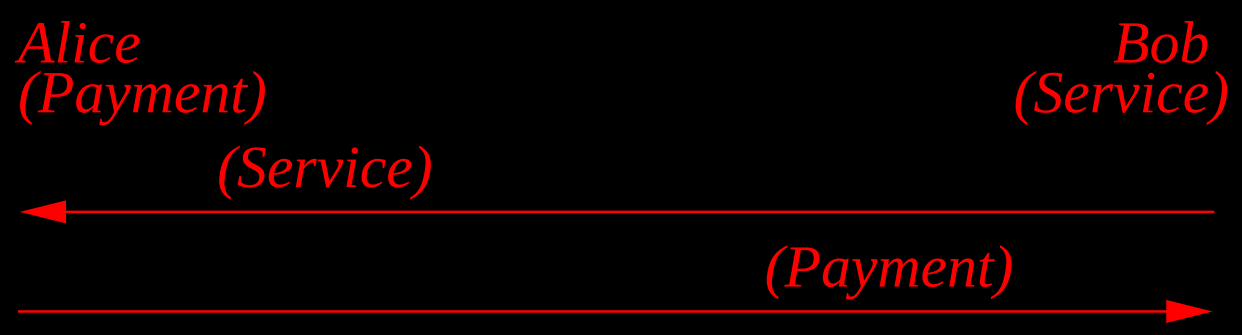
Model


Pirate
Guardian Angel
Terminode
Pirate
Guardian Angel
Terminode

Do GAs solve all problems?

Guardian Angels cannot simulate a central trusted authority in the described model due to the fact that they can only speak through the voice of the Pirates.

But Guardian Angels can help to solve some problems.



Fair Exchange Problem

Fair Exchange: Definitions

An exchange protocol is said to be fair if it ensures that during the exchange of the items, no party involved in the protocol can gain any advantage over the other party, even if the protocol halts for any reason.

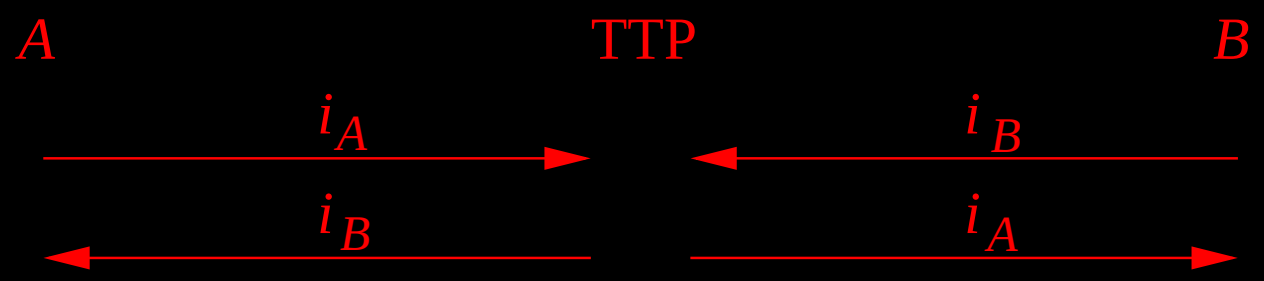
Complete: Both participants always receive the expected items if they are honest.

Timely: The exchange eventually ends.

Fair Exchange: Classification

- Perfect (Using a Trusted Third Party)
  - → On-line
  - → Off-line
- Unperfect
  - → Gradual
  - → Probabilistic

FE with an on-line TTP



FE with an on-line TTP

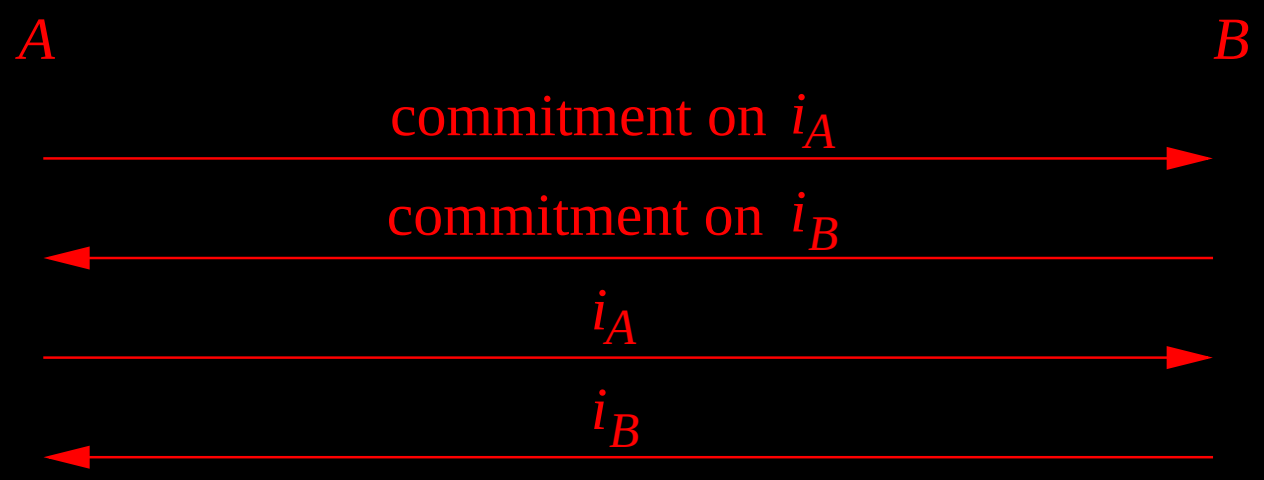
Advantage:

- Can be used to exchange arbitrary types of items.

Drawbacks:

- Having an online Third Party is a strong requirement.
- The Third Party needs to be trusted.
- The Third Party becomes a bottleneck.

FE with an off-line TTP



FE with an off-line TTP

Advantage:

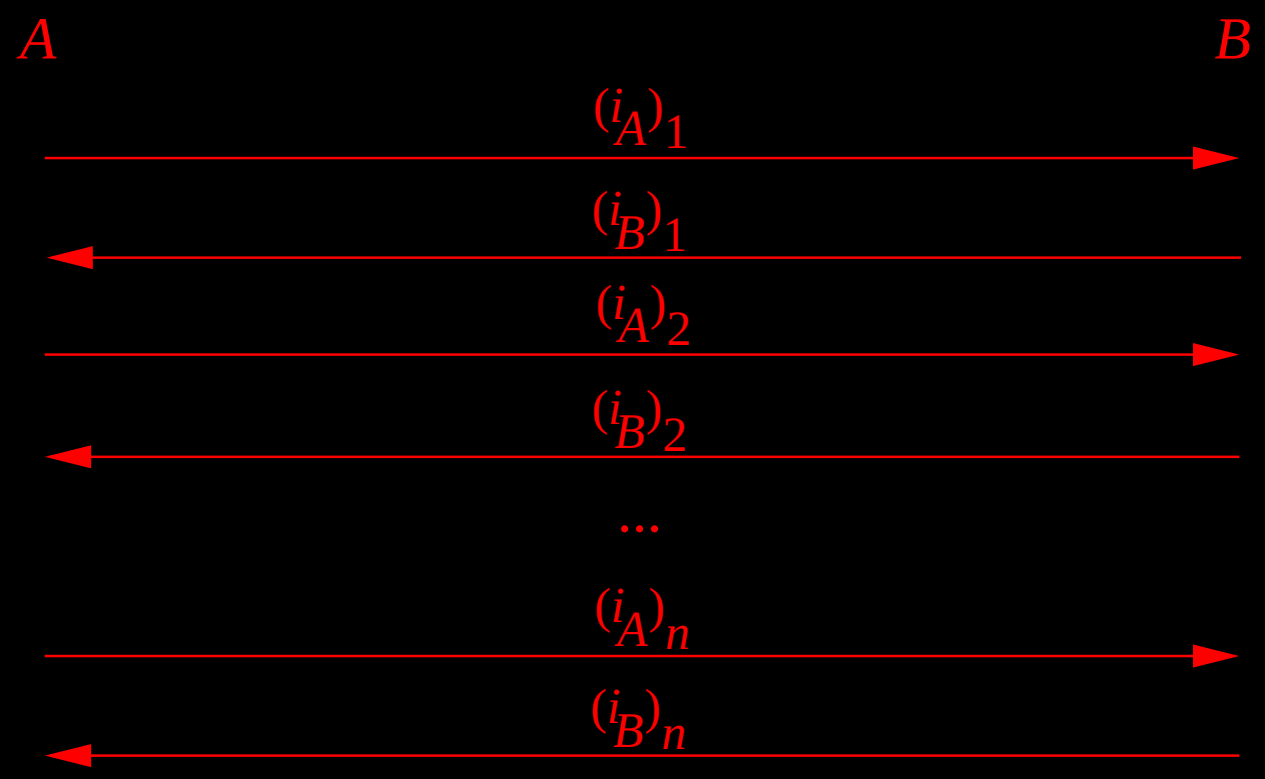
- The TTP is required only in case of conflict.

Drawbacks:

- Having a Third Party is sometimes difficult to achieve (even off-line)
- The Third Party needs to be trusted.
- The items must be revocable or generatable.

Gradual FE

Each entity alternatively transmits successive pieces of the items to exchange until the last piece of each item is sent.



Gradual FE

Advantage:

- This model does not require a TTP.

Drawbacks:

- High communication overhead.
- Difficult to determine if $(i_X)_j$ is really a part of i_X.
- The two participants must have the same computational power.
- Fairness is not ensured during the protocol.

Probabilistic FE

The fairness of the exchange is only ensured in a probabilistic way.

We aim to design such a protocol. To achieve this task, we are going to reduce the Fair Exchange Problem to the Synchronization Problem.

Synchronization Problem

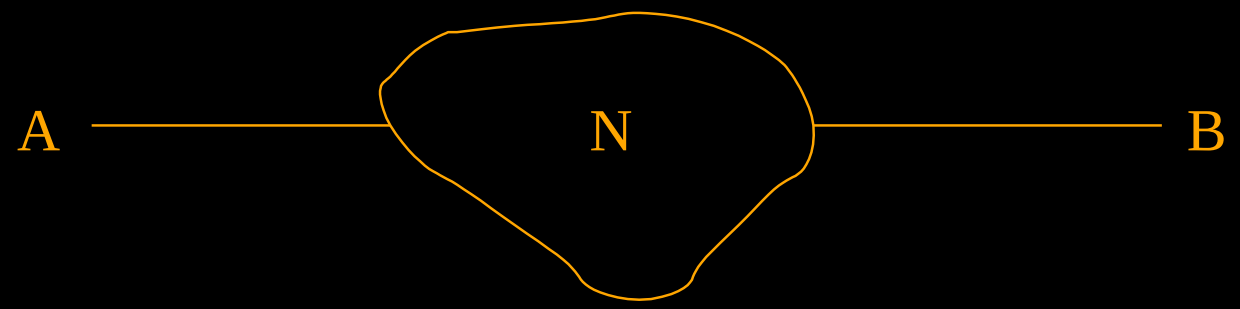
Synchronization: Definition

A synchronization protocol between A and B is a protocol which eventually ends with A and B on two possible terminal states, either success or failure.

Complete: A and B always end on the success state when there is no malicious misbehavior.
Fair: A and B always end on the same state even in case of misbehavior.
Timely: A and B eventually end.

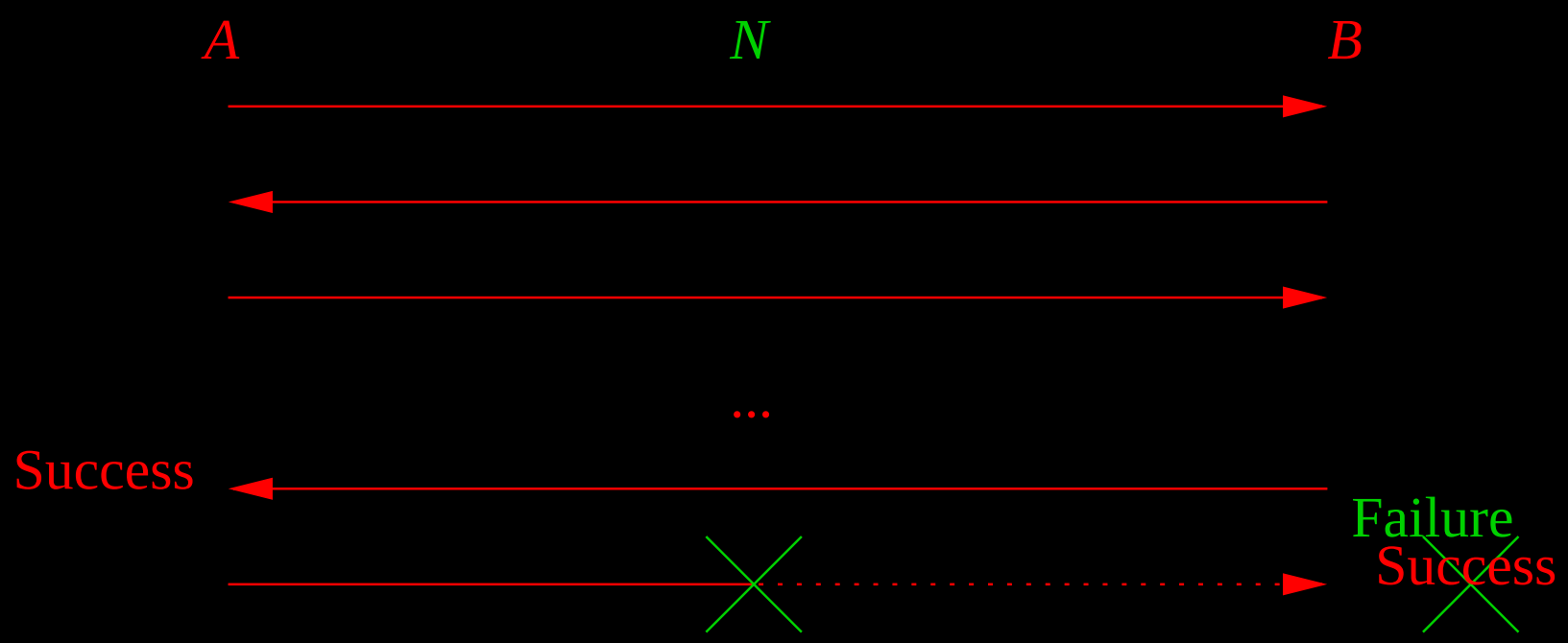
Synchronization Problem

How can two honest participants A and B achieve a synchronization through a malicious network N which may want to harm A or B?



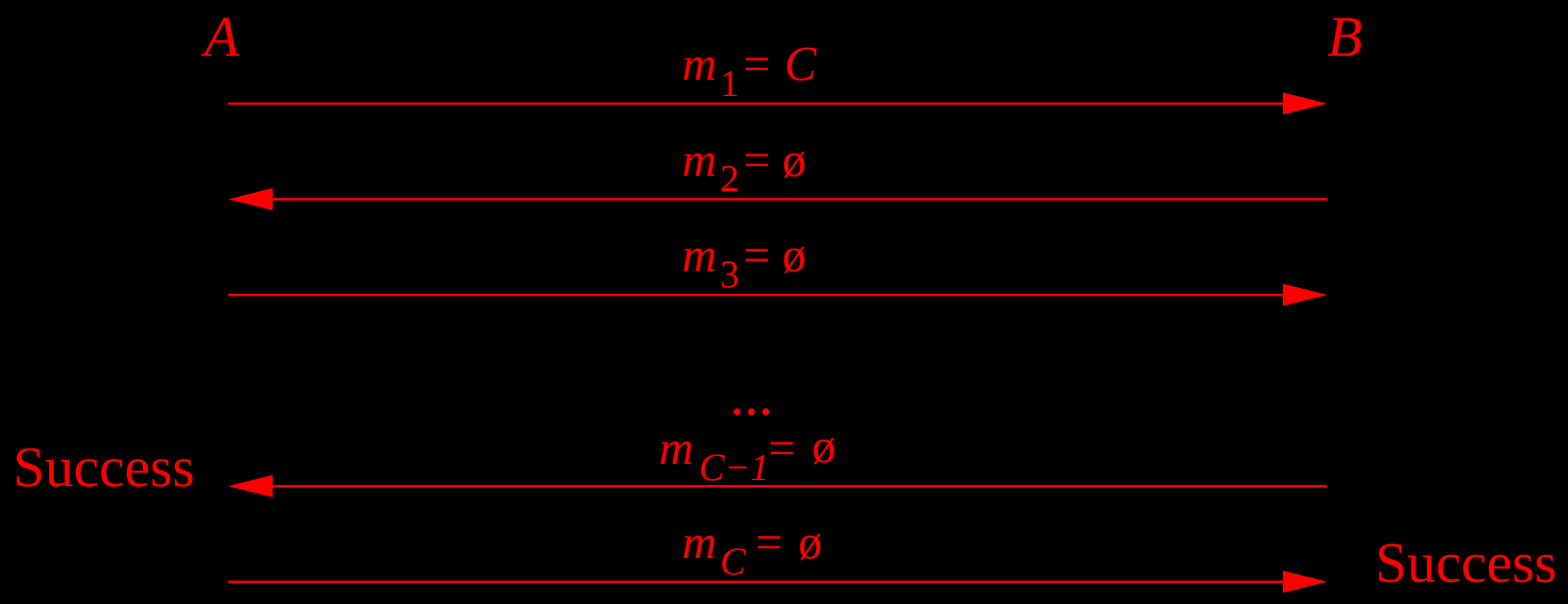
A and B are able to establish a secure channel providing confidentiality, authenticity, integrity, and sequentiality (but no timeliness).

Synchronization



If N knows the number of expected messages, C, then it can break the fairness of the protocol with probability 1. So N should not know the value of C.

Our Synchronization Protocol



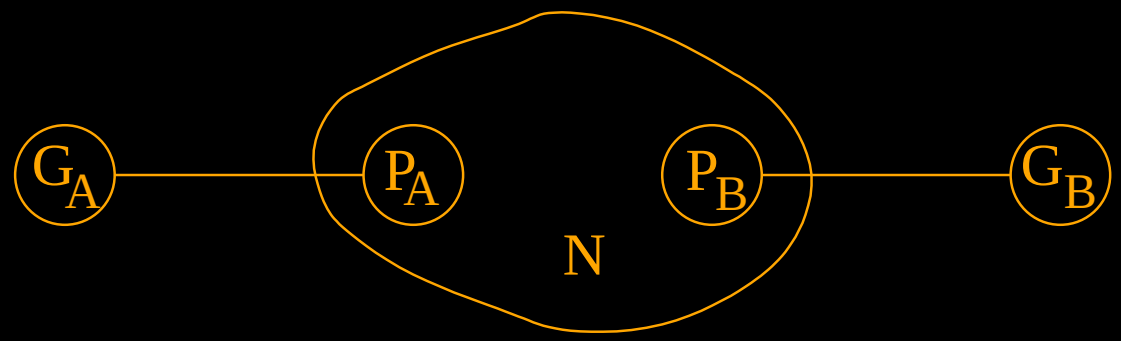
Synchronization

Here A and B were honest: this frame is not the common one for the fair exchange problem!

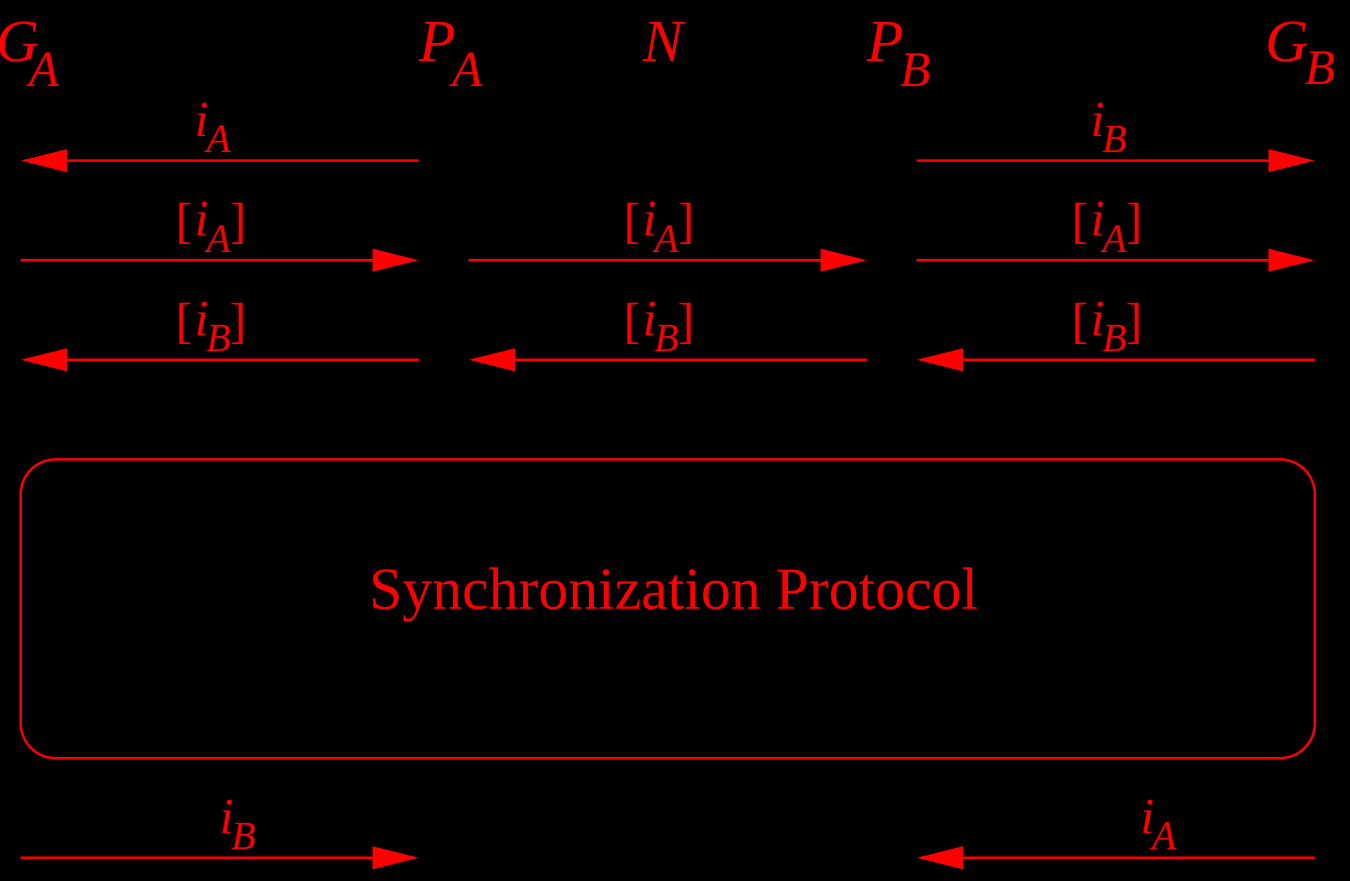
We reduce the Fair Exchange problem between two Guardian Angels to the Synchronization problem between two Pirates.

Fair Exchange with Guardian Angels

Fair Exchange to Synchronization



Our FE Protocol



Analysis of the Protocol

Complexity

When P_A and P_B are honest, the complexity in terms of exchanged messages is exactly equal to C.

When someone misbehaves, the complexity is smaller.

Let p_i be the probability $\Pr[C = i]$; by definition, the average complexity is

$$E(C) = \sum_{i=1}^{+\infty} i p_i.$$

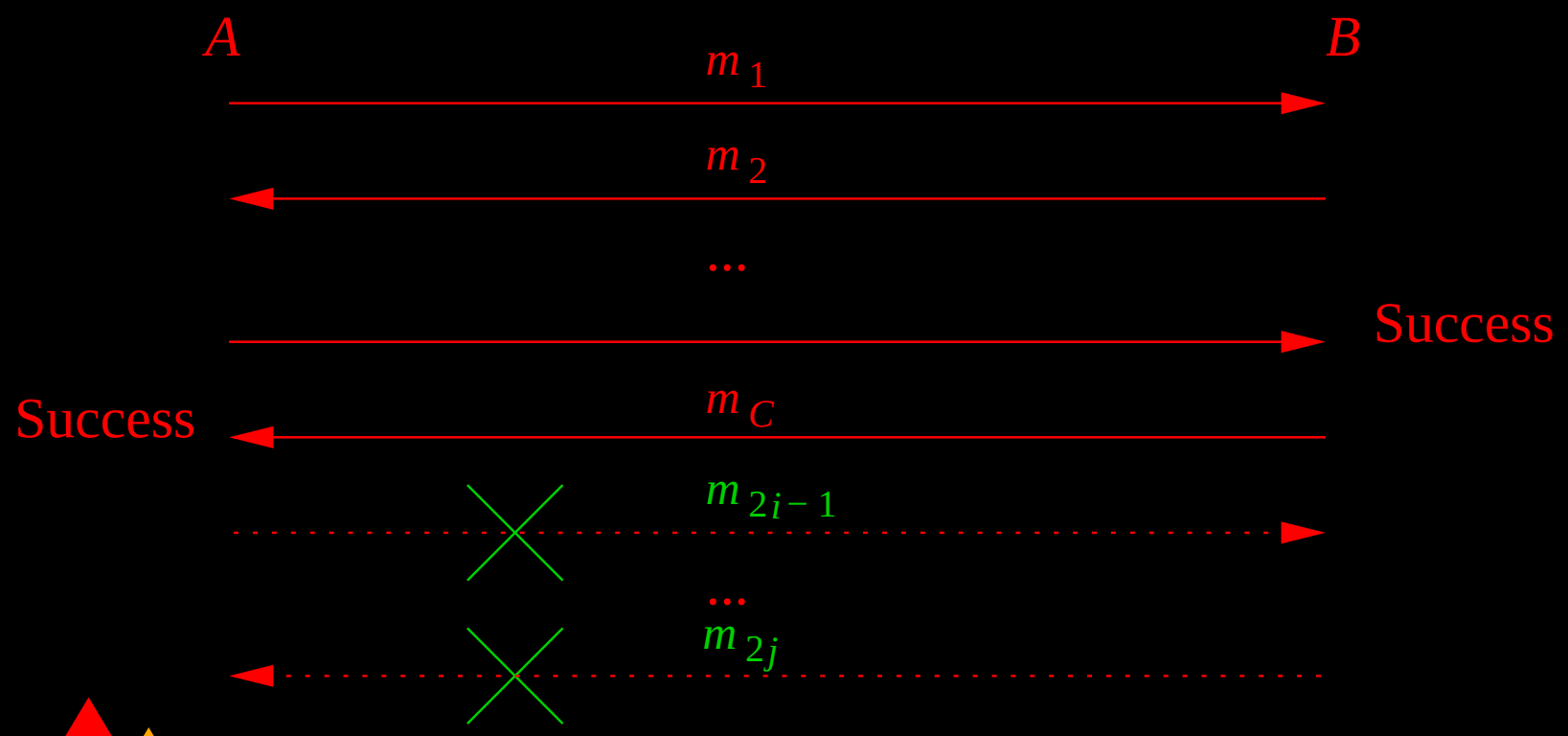
Probabilities

P_u (probability of unfairness) is the maximum of the probability that the protocol ends on an unfair state (over all possible misbehaviors of N).

P_c (probability that crime pays) is the maximum of the conditional probability that the protocol ends on an unfair state conditioned on N deviating from the protocol (over all possible misbehavior of N).

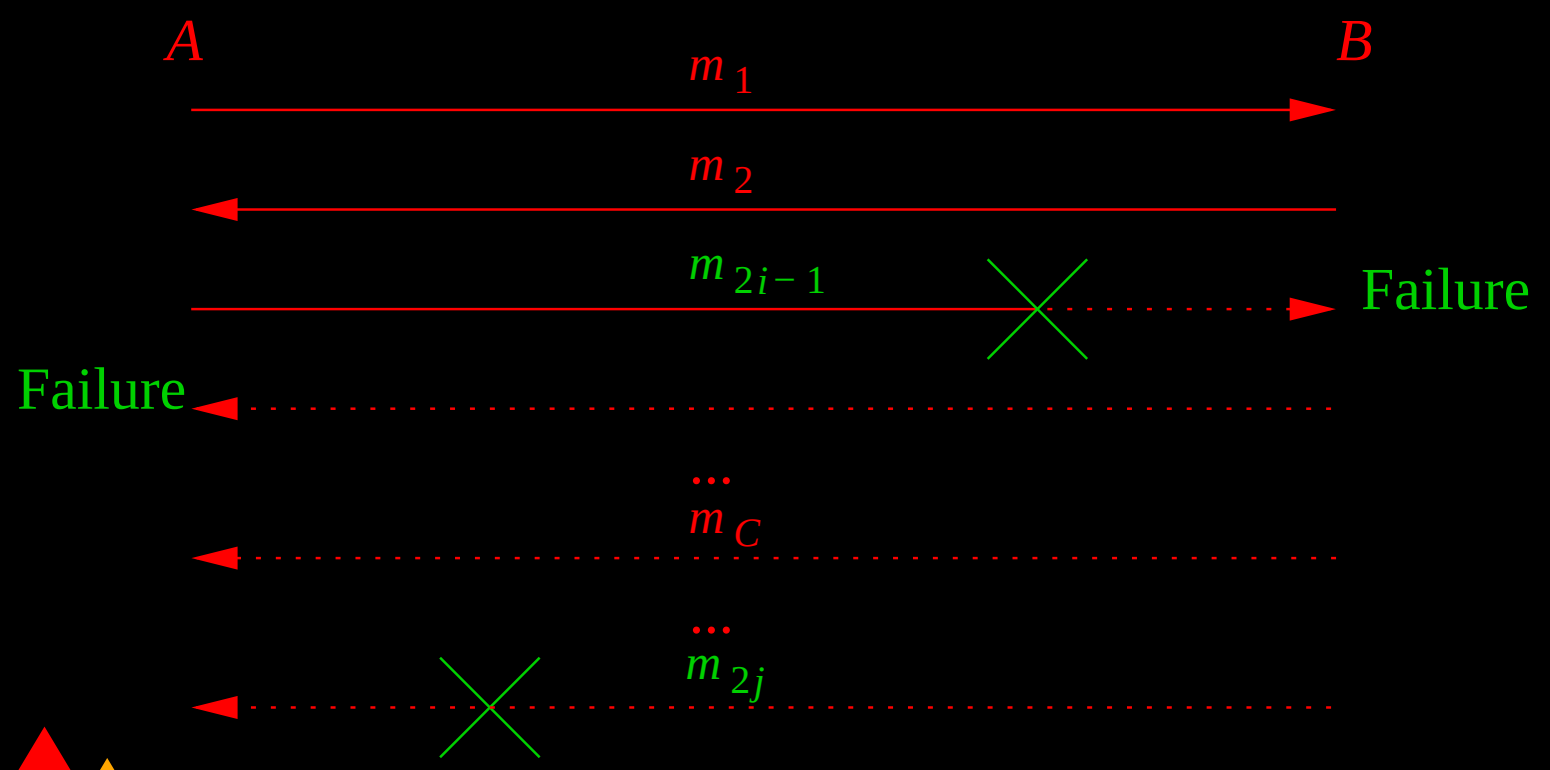
Probability of unfairness (1)

If $C < 2i - 1$ and $C < 2j$ then the misbehavior of P_A and P_B have no influence and the protocol fairly succeeds.



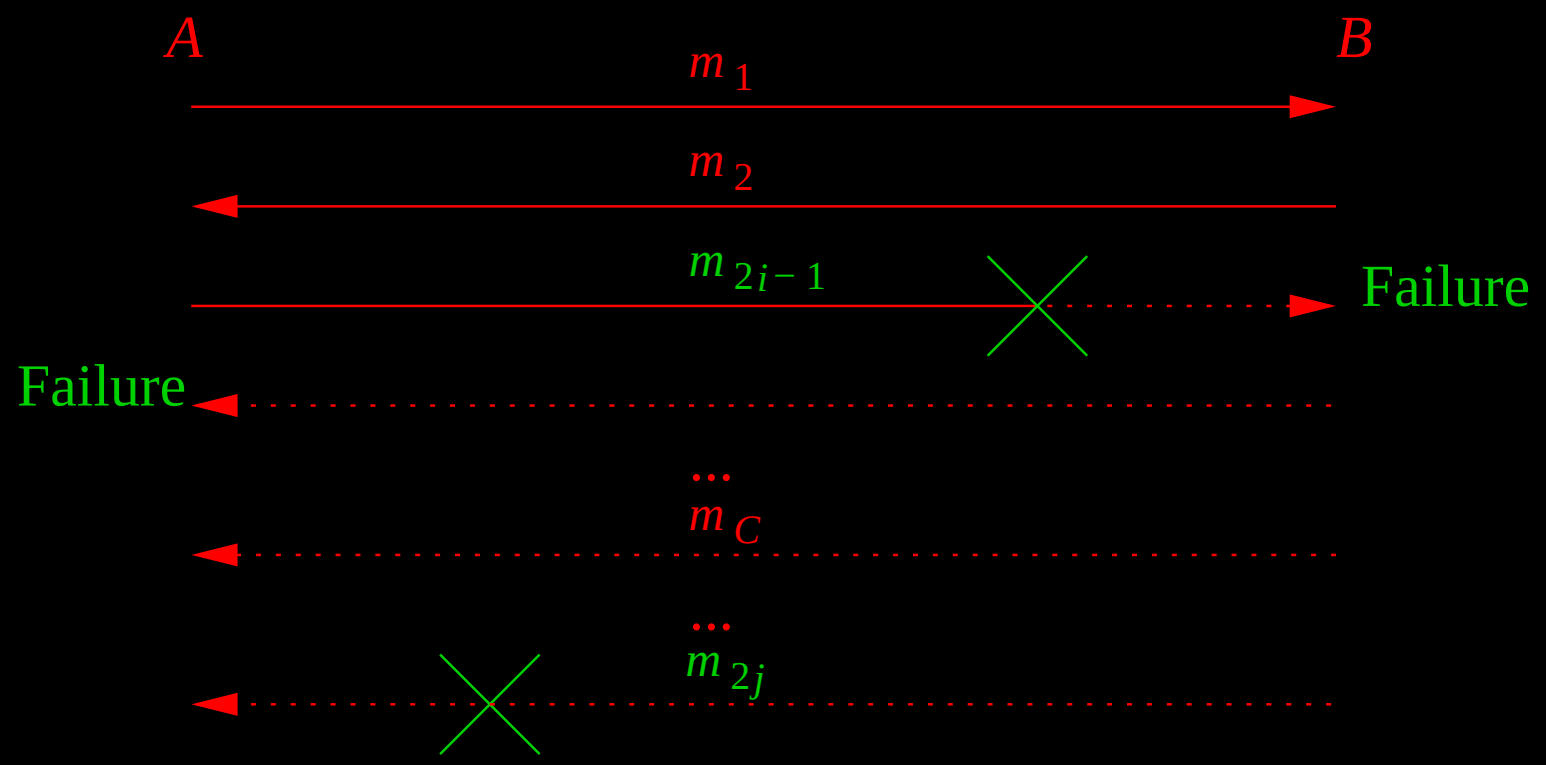
Probability of unfairness (2)

If $2i-1 < 2j$ and $2i-1 \leq C$, then the misbehavior of P_B has no influence since G_B is expecting the $(2i-1)$th message.



Probability of unfairness (3)

If $C > 2i - 1$ then the protocol "fairly" fails since G_A is also expecting a message.



Probability of unfairness (4)

Hence, if $2i - 1 < 2j$ then the protocol is unfair if and only if $2i - 1 = C$, then it is unfair with probability p_{2i-1}.

Conversely, if $2i-1 > 2j$ then the protocol is unfair with probability p_{2j}.

Therefore we have

$$P_u = \max_i p_i.$$

Probability that crime pays...

When a misbehavior drops the message i, the conditional probability that the crime pays is

$$\Pr[C = i / C \geq i].$$

Hence we have

$$P_c = \max_i \frac{p_i}{\sum_{j \geq i} p_j}.$$

e.g. 1: Uniform distribution

If $p_1 = \ldots = p_n = \frac{1}{n}$ and $p_i = 0$ for $i > n$ then

$E(C) = \frac{n+1}{2}, P_u = \frac{1}{n}$, and $P_c = 1$(for $i = n$).

If the Pirate who is assumed to send the nth message does not forward it, then his risk is void since this is the last message for sure. Hence the protocol is unfair with probability $\frac{1}{n}$ but with no risk at all for Pirates.

e.g. 2: Geometric distribution

If $p_i = (1-p)^{i-1}p$ for $i > 0$ then

$$E(C) = \frac{1}{p}, P_u = p, \text{ and } P_c = p.$$

This example is equivalent to the case where each Guardian Angel flips a coin in order to send the last message with probability p in every step.

Conclusion

We have designed a Fair Exchange protocol which

- Does not require a TTP.
- Does not rely on computational assumptions.
- Provides arbitrarily low unfairness.

General conclusion

Even if security modules cannot replace central trusted authority, embedding such modules in the devices seems to be a good way to enforce security in ad hoc networks.

This leads to some interesting questions related to economical aspects of ad hoc networks.