Time-Bounding Needham-Schroeder Public Key Exchange Protocol

Max Kanovich, Queen Mary, University of London, UK
University College London, UCL-CS, UK
Tajana Ban Kirigin, University of Rijeka, HR
Vivek Nigam, Federal University of Paraíba, Brazil
Andre Scedrov, UPENN, USA
National Research University HSE, Russia
Carolyn Talcott, SRI International, USA

LAP 2014.

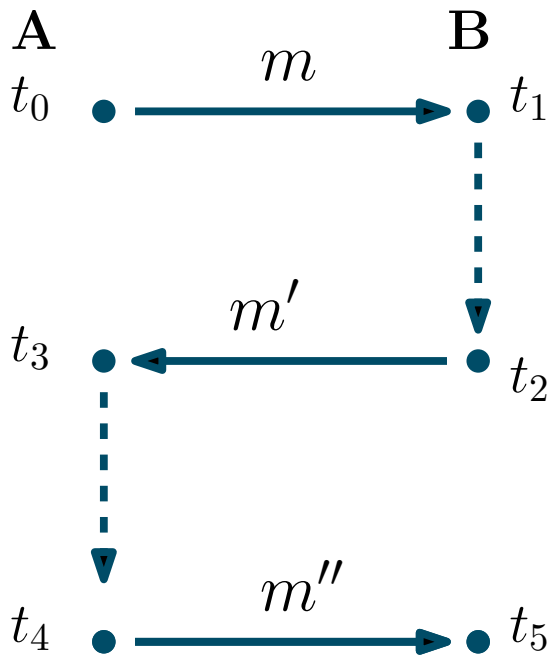
Cyber-Physical Security Protocols

Cyber-Physical Security Protocols are security protocols which rely on the **physical properties** in which its protocol sessions are carried out, such as:

- message transmission takes time
- processing requests takes time
- different transmission channels
- different transmission velocities
- physical and network distances between participants

Cyber-Physical Security Protocols

Example: **Distance Bounding Protocols**

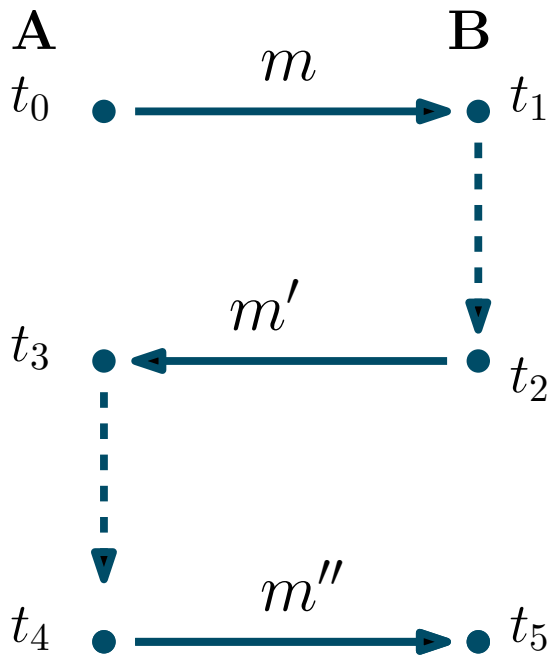


$t_3 - t_0$ is the response time

The round trip time of messages and the transmission velocity is taken into account to infer an upper bound of the distance between two agents.

Cyber-Physical Security Protocols

Example: **Distance Bounding Protocols**



If $t_3 - t_0 \leq R$ for a given **distance bounding time** R, then the verifier A grants the access to its resources to the prover B and sends a confirmation message.

Specification of Distance Bounding Protocols

Standard "Alice-Bob" notation needs to be refined.

$$\begin{aligned} A \longrightarrow B &: \ m \quad \text{at time} \ \ t_0 \\ B \longrightarrow A &: \ m' \quad \text{at time} \ \ t_1 \\ A \longrightarrow B &: \ m'' \quad \text{if} \ \ t_1 - t_0 \leq R \end{aligned}$$

Many **assumptions about time need to be formally specified**, including:

- time requirements for the fulfillment of a protocol session
- assumptions about the network, such as communication mediums and transmission velocities

Protocol verification

Following issues need to be addressed:

- which properties does the protocol ensure
- under which conditions
- against which intruders

Protocol verification

Following issues need to be addressed:

- which properties does the protocol ensure
- under which conditions
- against which intruders

Moreover, the **standard Dolev-Yao intruder** should be ammended with time features in order to make **the physical properties of the system relevant**.

Discrete vs. Continuous Time

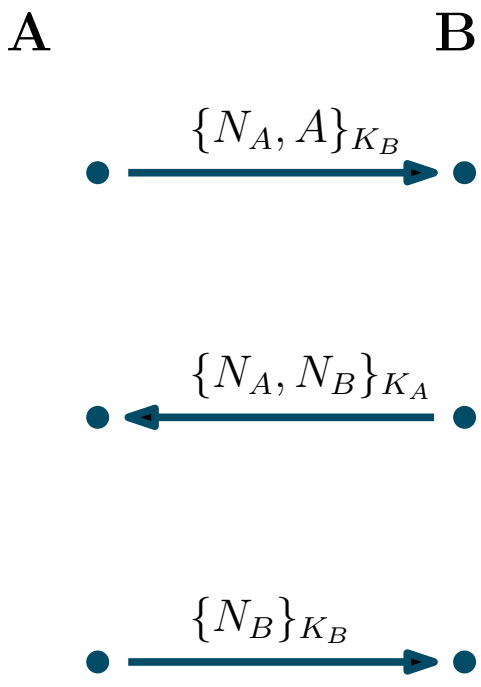
Protocol verification

Discrete Time Models	**Continuous Time Models**

We investigate how the models with **continuous time** relate to models with **discrete time** in protocol verification.

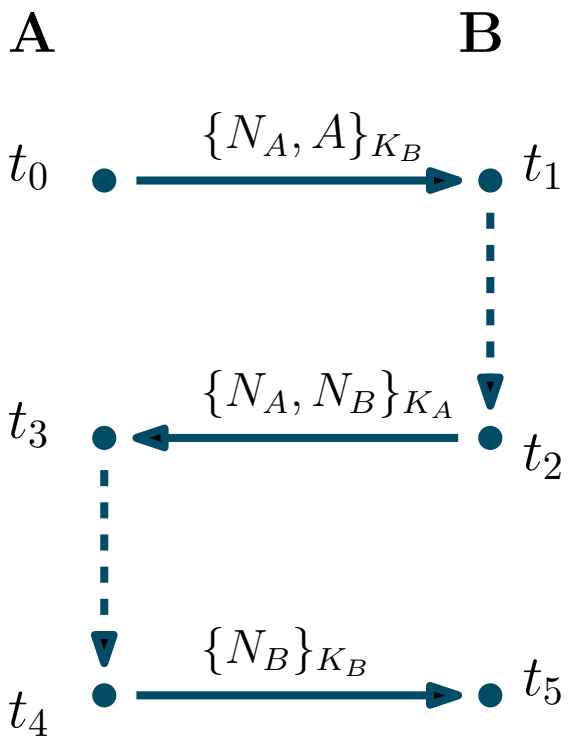
Cyber-Physical Security Protocols

Example: **Original (non-secure) Needham-Schroeder protocol**



Cyber-Physical Security Protocols

Example: **Original (non-secure) Needham-Schroeder protocol**



Can the protocol be fixed by means of **time**
(by some time requirements) ?

Time-Sensitive Features

We need to take into account **time-sensitive features** such as:

Time-Sensitive Features

We need to take into account **time-sensitive features** such as:

- **network delays**

Time-Sensitive Features

We need to take into account **time-sensitive features** such as:

- **network delays**
- participants' **processing time**

Time-Sensitive Features

We need to take into account **time-sensitive features** such as:

- **network delays**
- participants' **processing time**
- protocol execution depends on the round trip time of messages by means of **measuring the response time**

Time-Sensitive Features

Network Delay

A and B communicate through network:

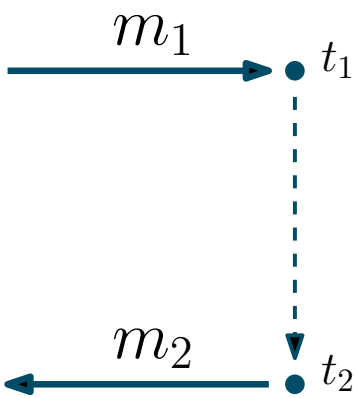
Message m sent at the moment t_0 is received at some **later moment** t_1, i.e. traversal of messages takes non-zero time $t_1 - t_0$.

Time-Sensitive Features

Network Delay

A and B communicate through network:

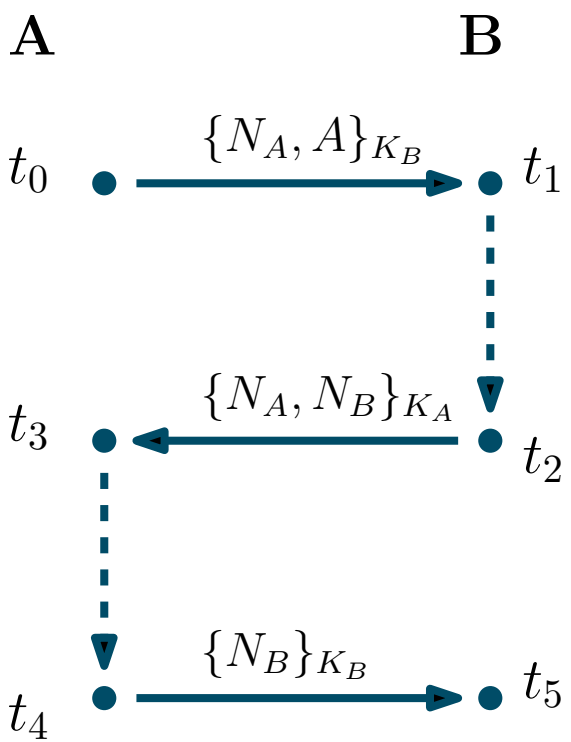
Message m sent at the moment t_0 is received at some **later moment** t_1, i.e. traversal of messages takes non-zero time $t_1 - t_0$.



Processing Time

Message m_1 is received at the moment t_1.
Reply m_2 is sent at some **later moment** t_2.
That is, processing takes non-zero time $t_2 - t_1$.

Time-Bounding Needham-Schroeder Protocol



If $t_3 - t_0 \leq R$ for a given **response bounding time** R, then A and sends to Bob the confirmation message $\{N_B\}_{K_B}$.

Time-Bounding Needham-Schroeder Protocol

The protocol is **secure** if the "accepted" N_A and N_B may never be revealed to somebody else except Alice and Bob.

For which response bounding time R is there an attack?

Time-Bounding Needham-Schroeder Protocol

The protocol is **secure** if the "accepted" N_A and N_B may never be revealed to somebody else except Alice and Bob.

For which response bounding time R is there an attack?

- We show that the answer depends on whether time is considered discrete or continuous.

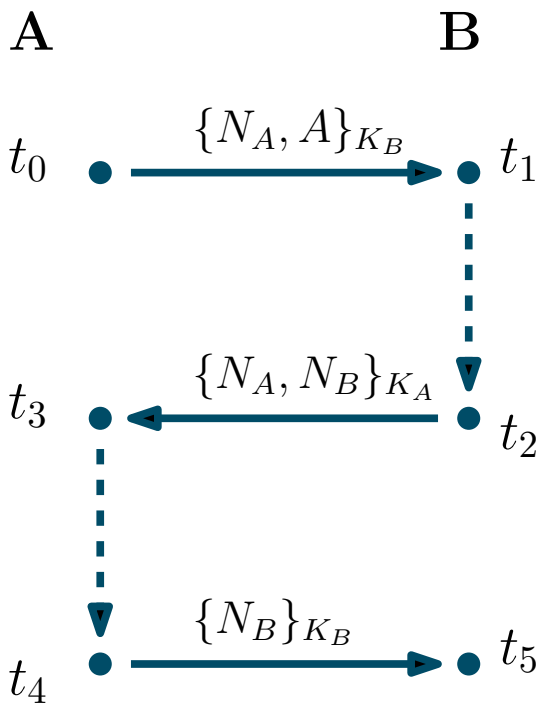
Time-Bounding Needham-Schroeder Protocol

The protocol is **secure** if the "accepted" N_A and N_B may never be revealed to somebody else except Alice and Bob.

For which response bounding time R is there an attack?

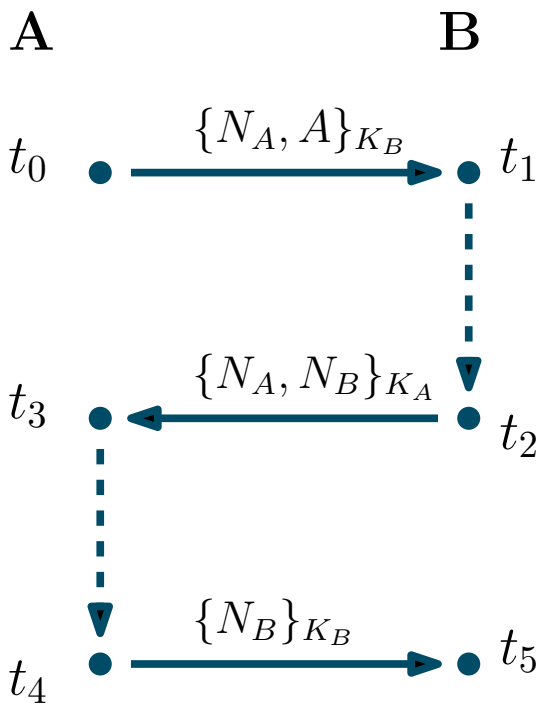
- We show that the answer depends on whether time is considered discrete or continuous.
- We show that the answer also depends on network delay and on internal processing time.

Time-Bounding Needham-Schroeder Protocol



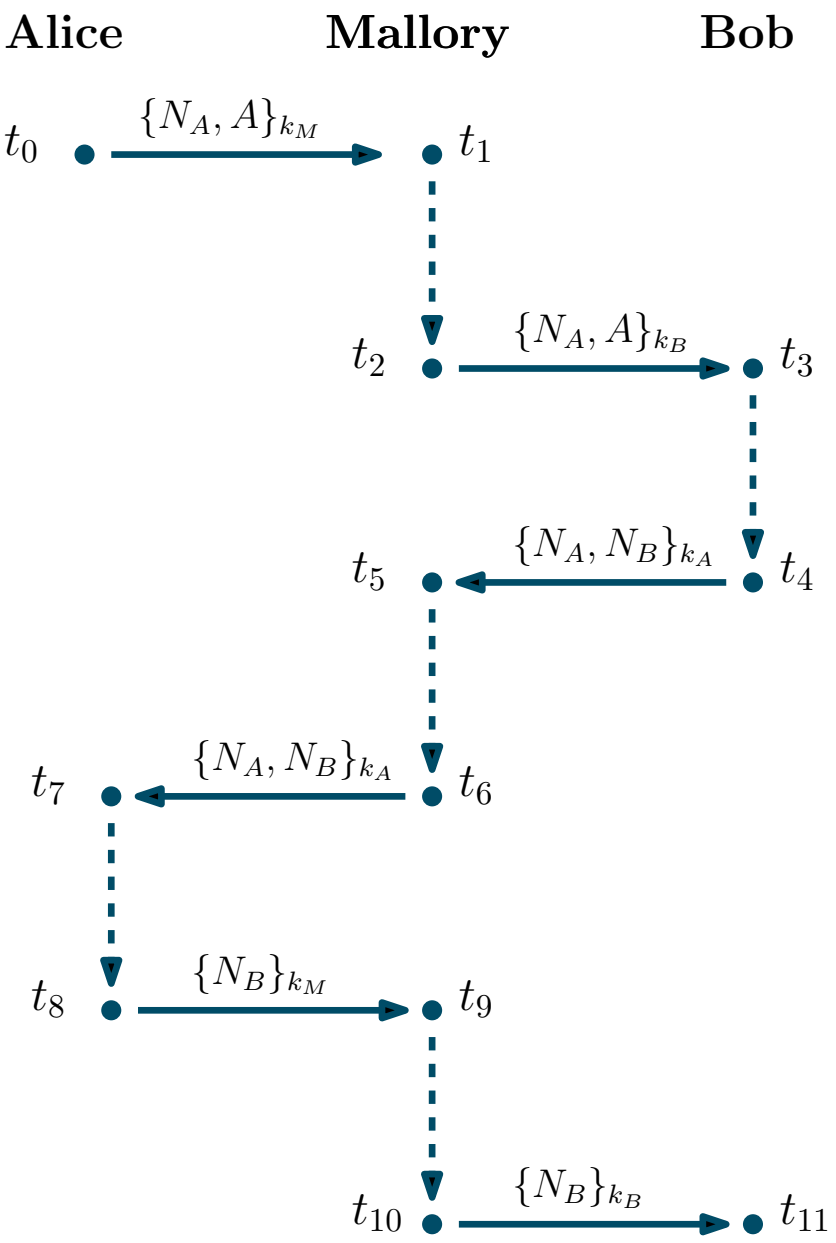
- The protocol is **safe** with an appropriate response bounding time R when using a model with discrete time : **no attack can be found.**

Time-Bounding Needham-Schroeder Protocol



- The protocol is **safe** with an appropriate response bounding time R when using a model with discrete time : **no attack can be found.**
- The protocol is **insecure** for any response bounding time R in the case of continuous time : **there is a timed version of Lowe attack.**

Attack on Time-Bounding Needham-Schroeder Protocol

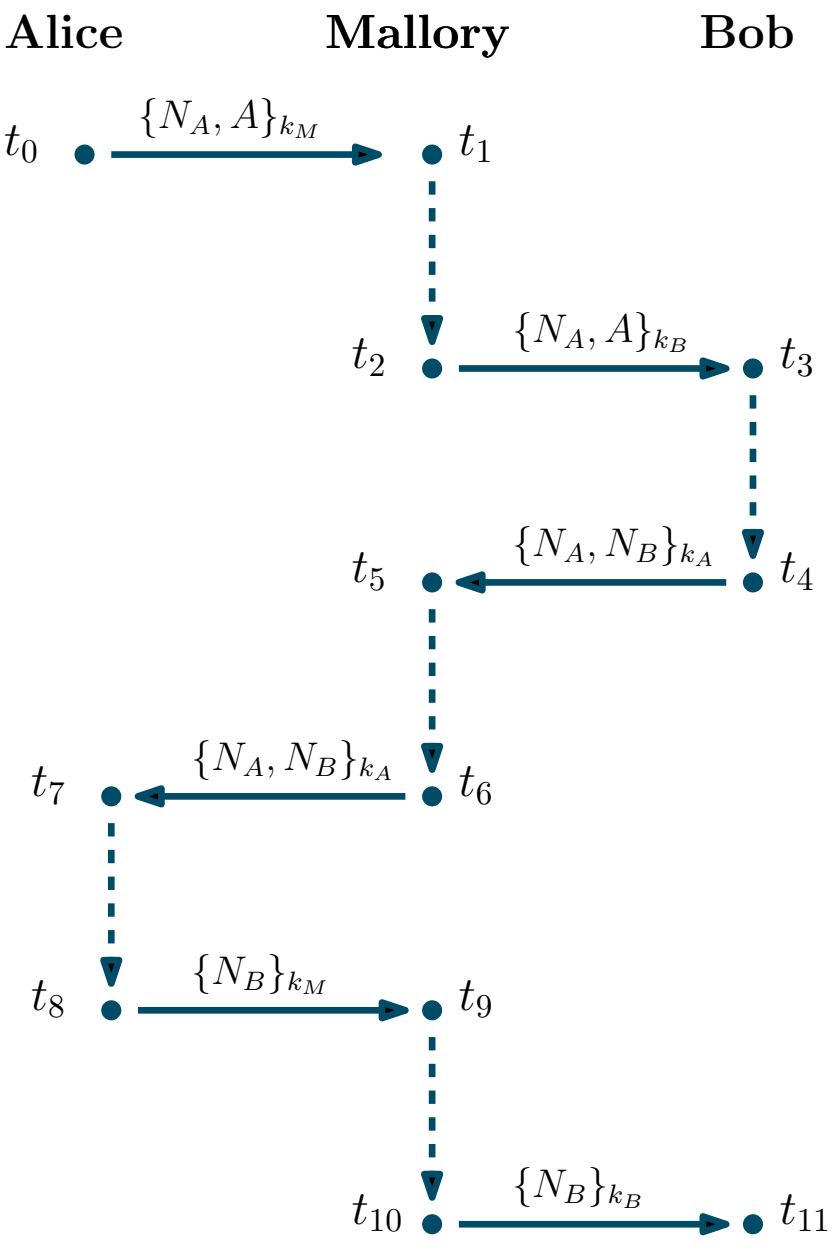


Lowe-style attack

Mallory forces Bob to believe that he communicated with Alice, and that only Alice learned Bob's nonce N_B.

Actually, Bob communicated with Mallory, and Mallory learned N_B.

Attack on Time-Bounding Needham-Schroeder Protocol



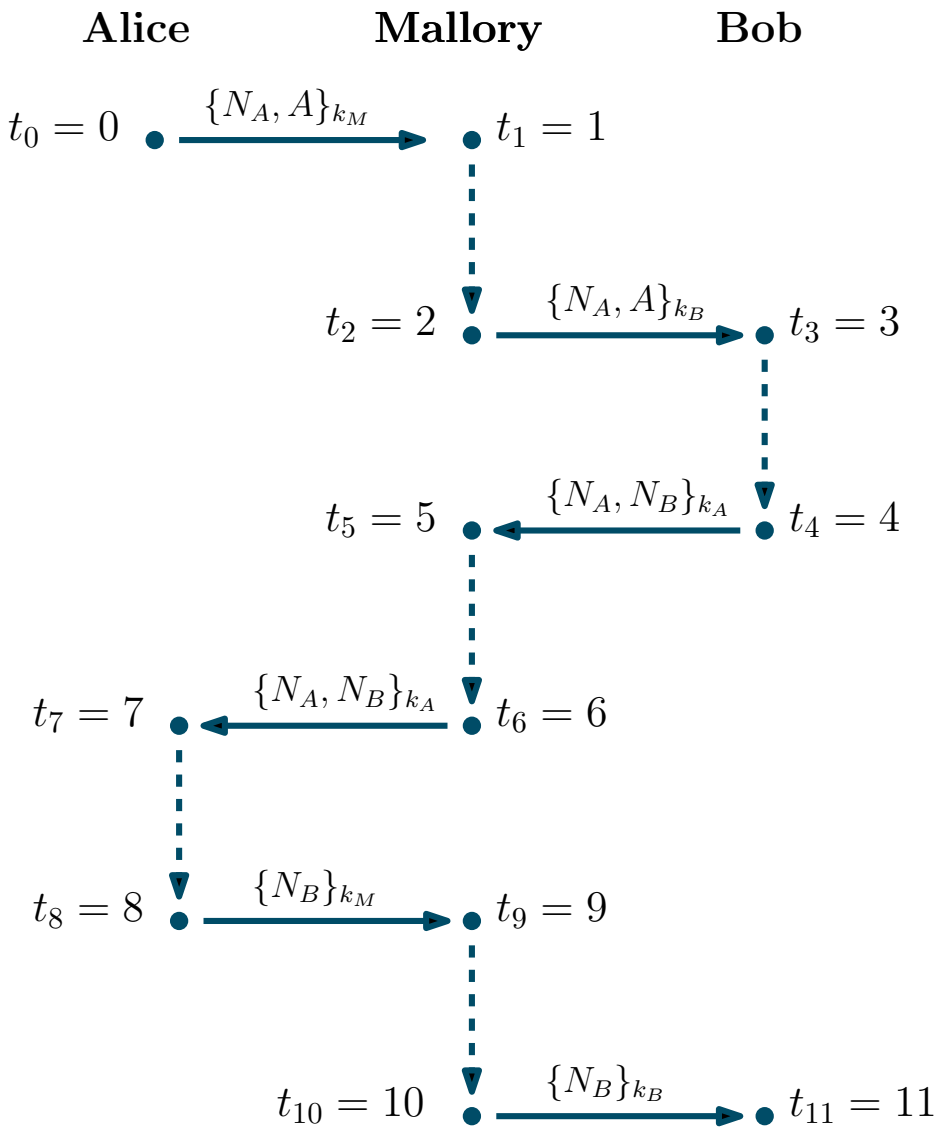
Lowe-style attack

Mallory forces Bob to believe that he communicated with Alice, and that only Alice learned Bob's nonce N_B.

Actually, Bob communicated with Mallory, and Mallory learned N_B.

Under which time conditions is the attack possible?

Attack on Time-Bounding Needham-Schroeder Protocol

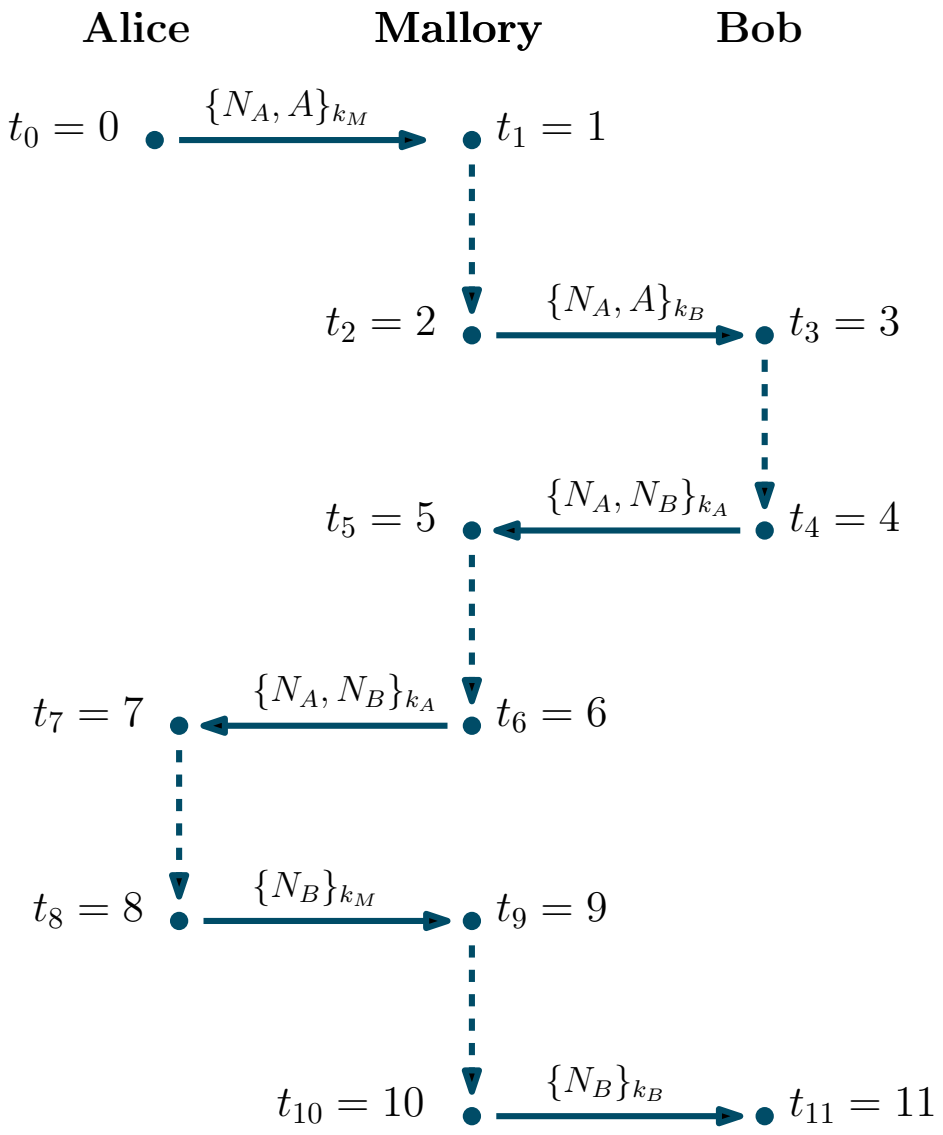


Lowe-style attack

Discrete time model

Since both network delay and processing take at least 1 time unit, attack can be performed only for response bounding time $R \geq 7$.

Attack on Time-Bounding Needham-Schroeder Protocol



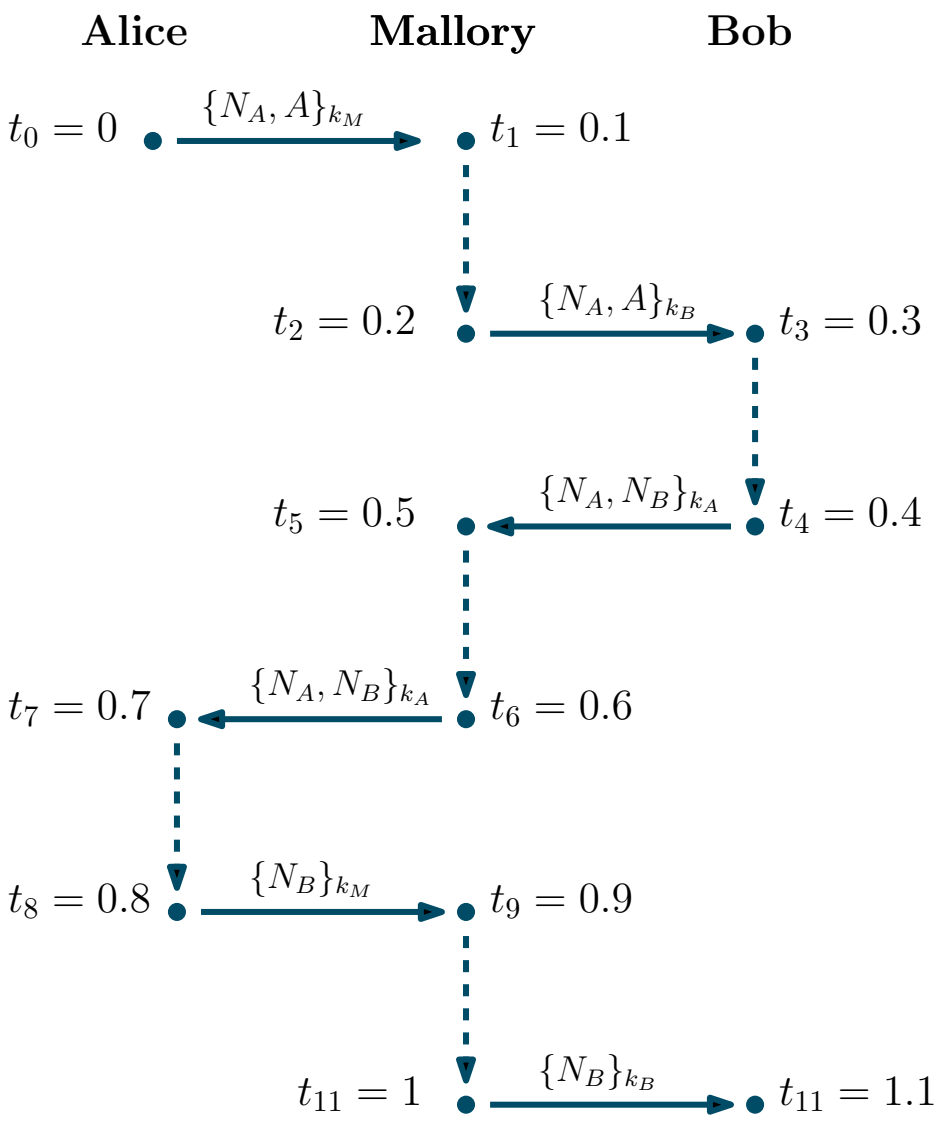
Lowe-style attack

Discrete time model

Since both network delay and processing take at least 1 time unit, attack can be performed only for response bounding time $R \geq 7$.

There is **no attack** for $R < 7$.

Attack on Time-Bounding Needham-Schroeder Protocol



Lowe-style attack

Continuous time model

Attack is possible for every response bounding time

$$R > 0$$

Discrete vs. Continuous Time

The existance of the attack depends on whether time is considered discrete or continuous.

No rescaling of discrete time units removes this issue:

For **any discretisation of time**, such as days, seconds or any other infinitesimal time unit, there is a protocol, for which

- **there exists an attack with continuous time**, and
- **no attack is possible in the discrete case**.

Discrete vs. Continuous Time

The existance of the attack depends on whether time is considered discrete or continuous.

No rescaling of discrete time units removes this issue:

For **any discretisation of time**, such as days, seconds or any other infinitesimal time unit, there is a protocol, for which

- **there exists an attack with continuous time**, and
- **no attack is possible in the discrete case**.

Between moments t_i and t_j only a finite number of acts can happen within discrete time, whereas an **unbounded number of timed events** are possible within continuous time.

Specification of Cyber-Physical Security Protocols

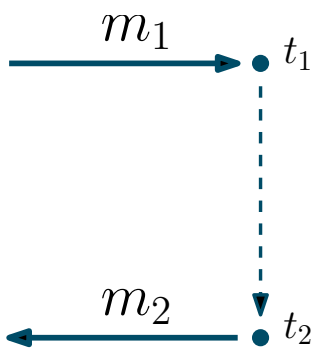
Lower bounds for passing messages and processing requests

a - strict lower bound for passing messages
b - strict lower bound for processing messages

Network Delay

Traversal of messages is greater then a :

$$t_1 - t_0 > a$$



Processing Time

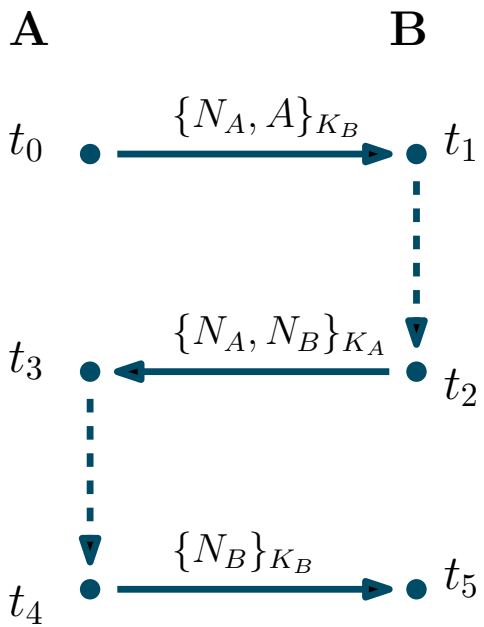
Internal processing is greater then b :

$$t_2 - t_1 > b$$

Time-Bounding Needham-Schroeder Protocol

Lower bounds for passing messages and processing requests

a - strict lower bound for passing messages
b - strict lower bound for processing messages

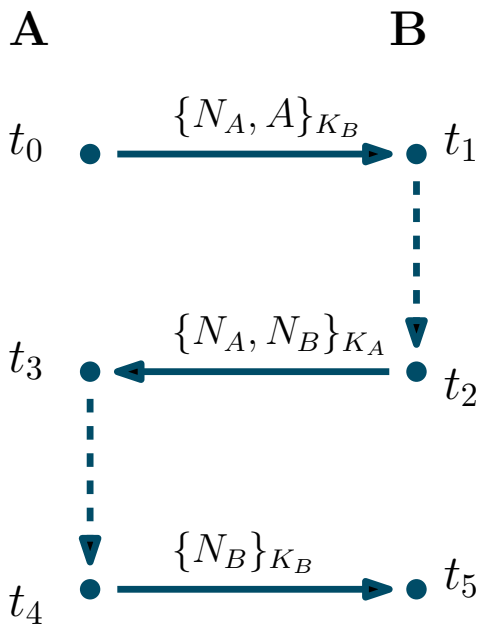


For which R the protocol is safe?
For which R there is an attack?

Time-Bounding Needham-Schroeder Protocol

Lower bounds for passing messages and processing requests

a - strict lower bound for passing messages
b - strict lower bound for processing messages



For which R the protocol is safe?
For which R there is an attack?

Given explicit lower bounds we can provide precise results.

Time-Bounding Needham-Schroeder Protocol

Lower bounds for passing messages and processing requests

a - strict lower bound for passing messages
b - strict lower bound for processing messages

In case $a > 0$ or $b > 0$, for non-negative integers a, b,

- For **discrete time**, there is **no Dolev-Yao attack** on the time-bounding Needham-Schroeder protocol with response bounding time $R < 4a + 3b + 7$.
- For **continuous time**, there is **no Dolev-Yao attack** on the time-bounding Needham-Schroeder protocol with the response bounding time $R < 4a + 3b$.

Discrete vs. Continuous Time

Protocol verification

Discrete Time Models	**Continuous Time Models**

There is a difference !

There are protocols for which there is no attack in the discrete time model, but there is an attack in the continuous time model.

Discrete vs. Continuous Time

Protocol verification

Discrete Time Models	**Continuous Time Models**

There is a difference !

There are protocols for which there is no attack in the discrete time model, but there is an attack in the continuous time model.

One should be aware of this difference in **cyber-physical security protocol verification**.

Complexity results

Planning Problem \ Reachability Problem		
Balanced actions	Untimed system	**PSPACE-complete** [Kanovich et al., FAST'10]
	System with discrete time	**PSPACE-complete** [Kanovich et al.,RTA'12]
	System with real time	**PSPACE-complete** new
Actions not necessarily balanced		**Undecidable**

Though the nonce updates cause a potentially infinite number of states, the PSPACE membership is given for the timed systems with **fresh values (nonces)**.

Future Work

- Investigating the power of our intruder model:
  how much damage can be done under which conditions
- Alternative Intruder and Protocol Models
  e.g. agents allowed to move, not static
- Implementation of our model in automated tools e.g. Maude:
  verifying cyber-physical protocols
- Specification of asynchronous systems
  Time synchronization mechanisms
  Network Time Protocols
- Analysis of security protocols
  e.g. timestamps, timing channels

Related Work

- Durgin, Lincoln, Mitchell, Scedrov. Multiset rewriting and the complexity of bounded security protocols. 1999.
- Kanovich, Okada, Scedrov. Specifying real-time finite-state systems in linear logic, 1998.
- Alur, Dill. A theory of timed automata, 1994.
- Brands, Chaum. Distance-bounding protocols, 1993.
- Meadows, Poovendran, Pavlovic, Chang, Syverson. Distance bounding protocols: Authentication logic analysis and collusion attacks, 2007.
- Lanotte, Maggiolo-Schettini, Troina. Reachability results for timed automata with unbounded data structures, 2010.
- Malladi, Bruhadeshwar, Kothapalli. Automatic analysis of distance bounding protocols, 2010.