Crypto Protocol Analysis With Time and Space

D. Aparicio-Sánchez[1], S. Escobar[1], C. Meadows[2], J. Meseguer[3], and J. Sapiña[1]

[1]Universitat Politècnica de València, Spain

[2]Naval Research Laboratory, Washington DC

[3]University of Illinois at Urbana-Champaign, Champaign, USA

Computational Logic Autumn Summit 2022
September 30, 2022

What This Talk is About

- Applying formal methods (model checking) to analysis of cryptographic protocols that rely on time and space constraints
- Use Maude-NPA tool
  - symbolic model checker; uses logical variables and symbolic constraints
- Extend Maude-NPA with timed and located syntax and semantics
- Connect to an SMT solver for non-linear real arithmetic
- Two protocol examples:
  - Brands & Chaum distance bounding
  - Secure localization protocol with beacons

Why Time and Space?

- Security protocols for Internet of Things
- Distance bounding protocols - Can use round trip of a challenge and response to decide whether someone is within k meters from you
- Secure localization- can use time of arrival of signals at different locations to localize a principal
  - Even if it tries to mislead you
- Use this together with cryptography to authenticate the principals to each other

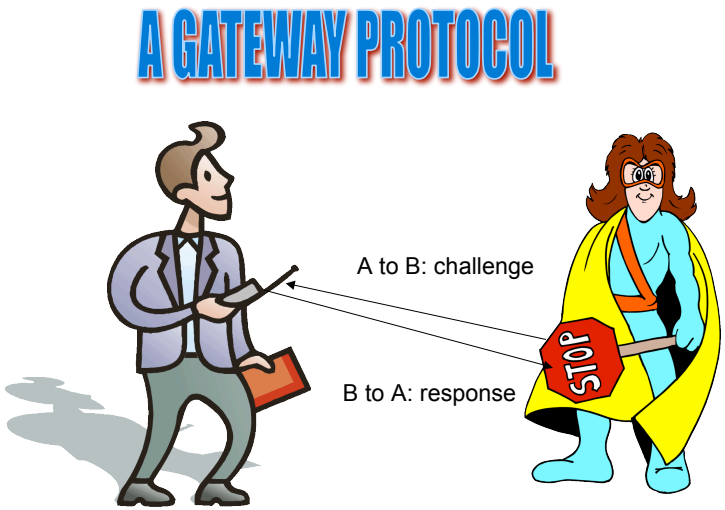
Larger Questions

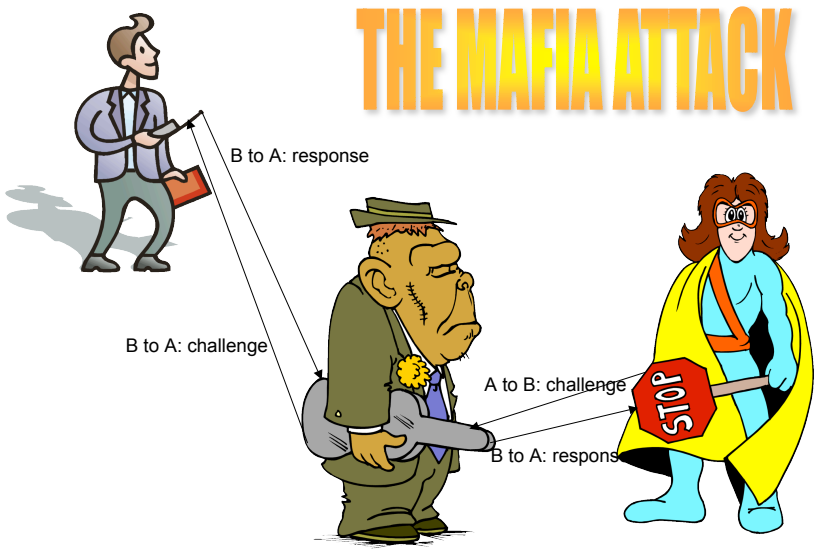
- What kinds of non-linear constraint problems can we analyze symbolically via model checkers?
- What kinds of analyses are practical?
  - State space explosion is always a problem
- What can be done to extend the bounds of what is possible?

Outline

Outline

Mafia Attack





Brands & Chaum

Standard Description

$P \rightarrow V : commit(N_P, S_P)$
//The prover sends his name and a commitment

$V \rightarrow P : N_V$
//The verifier sends a nonce and records the time when this message was sent

$P \rightarrow V : N_P \oplus N_V$
//The verifier checks the answer message arrives within two times a fixed distance

$P \rightarrow V : S_P$
//The prover sends the committed secret and the verifier opens the commitment

$P \rightarrow V : sign_P(N_V; N_P \oplus N_V)$
//The prover signs the two rapid exchange messages

Brands & Chaum

Time & Space Description

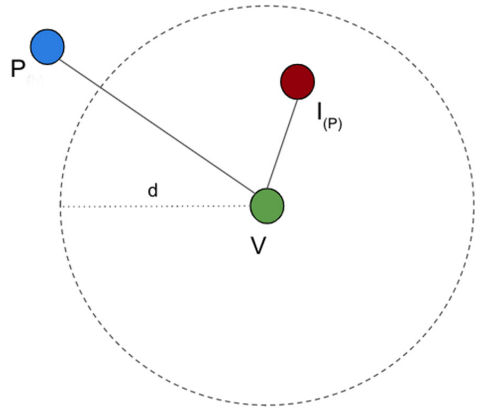
$$
\begin{array}{ll}
P_{t_1} \rightarrow V_{t'_1} : commit(N_P, S_P) & \mid t'_1 = t_1 + d(P,V) \wedge \lfloor d(P,V) \rfloor \\
V_{t_2} \rightarrow P_{t'_2} : N_V & \mid t'_2 = t_2 + d(P,V) \wedge t_2 \geq t'_1 \wedge \lfloor d(P,V) \rfloor \\
P_{t_3} \rightarrow V_{t'_3} : N_P \oplus N_V & \mid t'_3 = t_3 + d(P,V) \wedge t_3 \geq t'_2 \wedge \lfloor d(P,V) \rfloor \\
\qquad V : t'_3 \dot{-} t_2 \leq 2 * d & \\
P_{t_4} \rightarrow V_{t'_4} : S_P & \mid t'_4 = t_4 + d(P,V) \wedge t_4 \geq t_3 \wedge \lfloor d(P,V) \rfloor \\
P_{t_5} \rightarrow V_{t'_5} : sign_P(N_V; N_P \oplus N_V) & \mid t'_5 = t_5 + d(P,V) \wedge t_5 \geq t_4 \wedge \lfloor d(P,V) \rfloor
\end{array}
$$

Time & Space Constraints

$$\lfloor d(A,B) \rfloor := \ (d(A,B) \geq 0 \wedge d(A,B)^2 = (A_x - B_x)^2 + (A_y - B_y)^2 + (A_z - B_z)^2)$$

$$d((x,y,z),(x',y',z')) := \ \sqrt{(x-x')^2 + (y-y')^2 + (z-z')^2}$$

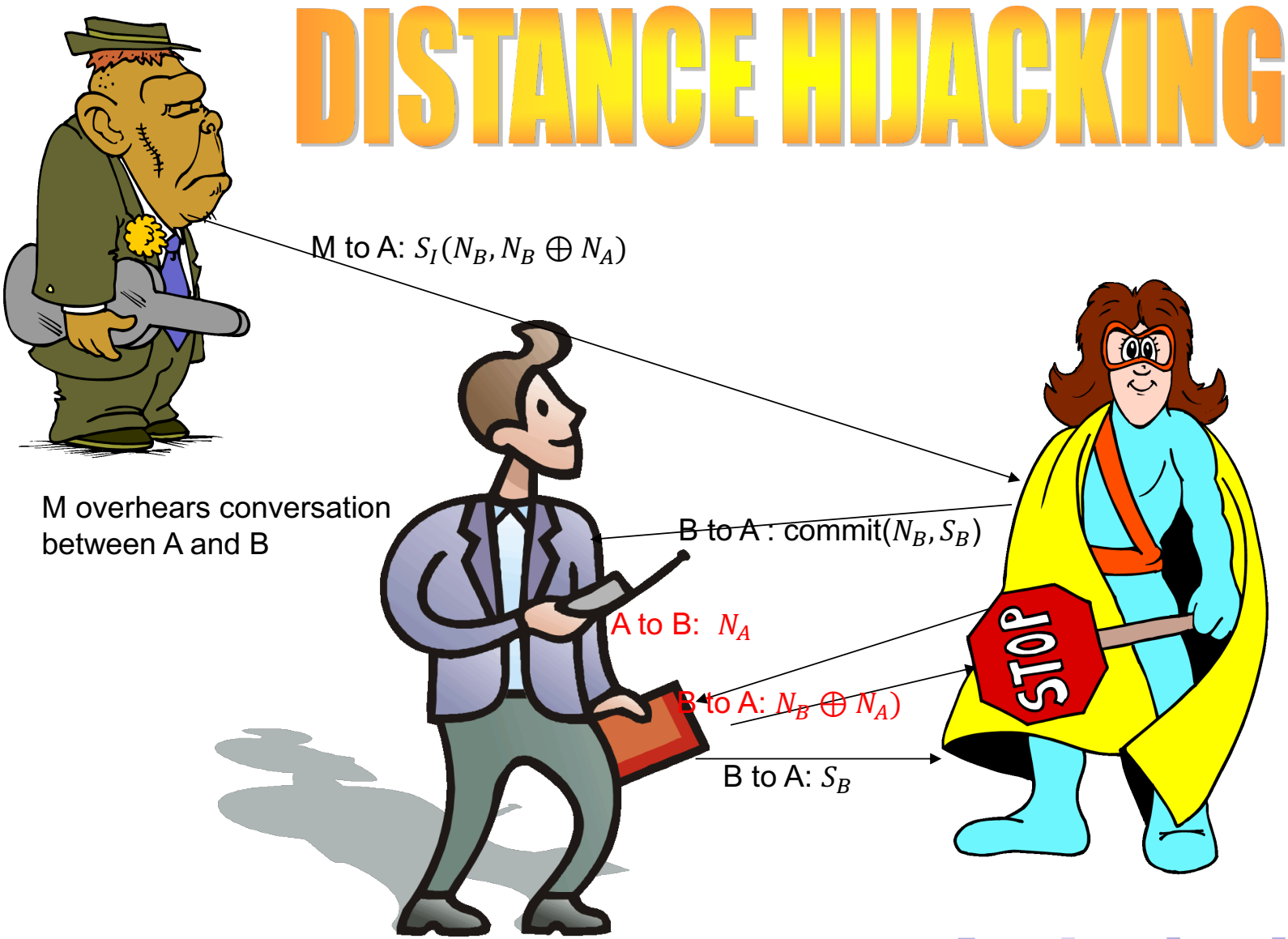
Brands & Chaum (Mafia Fraud - Secure)



$$
\begin{array}{rll}
P_{t_1} \rightarrow I_{t_2} & : commit(N_P, S_P) & \mid t_2 = t_1 + d(P,I) \wedge \lfloor d(P,I) \rfloor \\
I(P)_{t_2} \rightarrow V_{t_3} & : commit(N_P, S_P) & \mid t_3 = t_2 + d(V,I) \wedge \lfloor d(V,I) \rfloor \\
V_{t_3} \rightarrow I(P)_{t_4} & : N_V & \mid t_4 = t_3 + d(V,I) \wedge \lfloor d(V,I) \rfloor \\
I_{t_4} \rightarrow P_{t_5} & : N_V & \mid t_5 = t_4 + d(P,I) \wedge \lfloor d(P,I) \rfloor \\
P_{t_5} \rightarrow I_{t_6} & : N_P \oplus N_V & \mid t_6 = t_5 + d(P,I) \wedge \lfloor d(P,I) \rfloor \\
I(P)_{t_6} \rightarrow V_{t_7} & : N_P \oplus N_V & \mid t_7 = t_6 + d(V,I) \wedge \lfloor d(V,I) \rfloor \\
V & : t_7 \dot{-} t_3 \leq 2 * d & \\
P_{t_8} \rightarrow I_{t_9} & : S_P & \mid t_9 = t_8 + d(P,I) \wedge t_8 \geq t_5 \wedge \lfloor d(P,I) \rfloor \\
I(P)_{t_{10}} \rightarrow V_{t_{11}} & : S_P & \mid t_{11} = t_{10} + d(V,I) \wedge t_{11} \geq t_7 \wedge \lfloor d(V,I) \rfloor \\
I(P)_{t_{12}} \rightarrow V_{t_{13}} & : sign_P(N_V; N_P \oplus N_V) & \mid t_{13} = t_{12} + d(V,I) \wedge t_{13} \geq t_{11} \wedge \lfloor d(V,I) \rfloor
\end{array}
$$

In addition $d(P,V) > d$, $d(I,V) \leq d$, $d(P,V) \leq d(I,V) + d(I,P)$

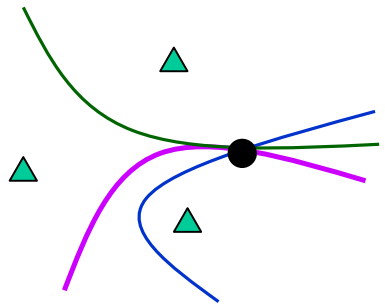
Hijacking Attack



Outline

Secure Localization

Standard Description



$D \rightarrow Be^i : timestamp$
//The device broadcasts a timestamp, maybe different to its
//actual time to appear farther or closer than its true location

$Be^i \rightarrow Ba : timediff\ ;\ Be^i_x\ ;\ Be^i_y$
//Each beacon sends to a base station the difference between
//the received timestamp and the actual reception time plus
//her position.

The base station takes the intersection of four different circles, each center = Beacon's location, and radius = Beacon's timediff

The intersection is the location of the device

Secure Localization

Time & Space Description

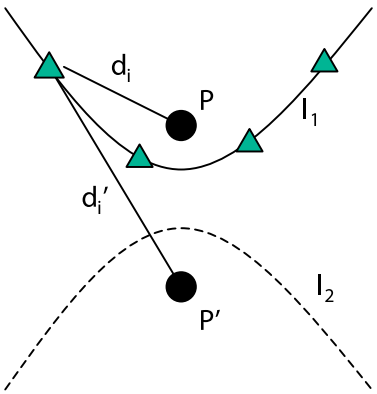
$$
\begin{aligned}
D_{t_1} \rightarrow Be^i_{t'_1} &: t && \mid t'_1 = t_1 + d(D, Be^i) \wedge \lfloor d(D, Be^i) \rfloor \\
Be^i &: \bar{t} = t \dot{-} t'_1 && \mid \bar{t} \geq 0 \\
Be^i_{t_2} \rightarrow Ba_{t'_2} &: \bar{t}\ ;\ Be^i_x\ ;\ Be^i_y && \mid t'_2 = t_2 + d(Be^i, Ba) \wedge \lfloor d(Be^i, Ba) \rfloor \\
Ba &: \bar{t}^2 = (D^1_x - Be^1_x)^2 + (D^1_y - Be^1_y)^2 \\
&\vdots \\
Ba &: \bar{t}^2 = (D^n_x - Be^n_x)^2 + (D^n_y - Be^n_y)^2 \\
Ba &: D^1_x = \cdots = D^n_x \wedge D^1_y = \cdots = D^n_y
\end{aligned}
$$

Time & Space Constraints

$$\lfloor d(A,B) \rfloor := \ (d(A,B) \geq 0 \wedge d(A,B)^2 = (A_x - B_x)^2 + (A_y - B_y)^2 + (A_z - B_z)^2)$$

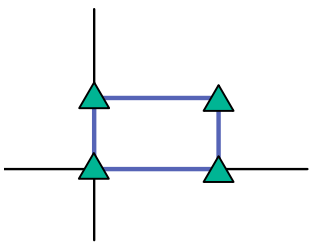
$$d((x,y,z),(x',y',z')) := \ \sqrt{(x-x')^2 + (y-y')^2 + (z-z')^2}$$

Secure Localization Attack (Shmatikov and Wang, 2007)



Definition (Insecure configuration)

If the beacons are in the same lobe of a hyperbola, it is possible for a malicious device at the P to choose a timestamp to pretend to be at position P', where P and P' are the foci



Definition (Secure configuration)

If there are four beacons and they form a rectangle, then it can be proved that they never lie on the same lobe of a hyberbola.

Outline

Original Maude-NPA

- State is a set of communicating processes
- Instead of communicating with each other, communicate with a single intruder who can
  - Read messages
  - Apply functions to messages it's received (e.g. encryption/decrypton)
  - Send messages
  - Block messages
- Supplied with an Intruder Knowledge constraint set
- Maude-NPA executes backwards from a description of an insecure state
- As Maude-NPA executes, constraints are introduced to the constraint set

Timed and Located Maude-NPA

- State in Maude-NPA is again a set of communicating processes
- Each process is assumed to have a fixed location with coordinates x, y, and z
- Each action (sending or receiving) takes place at a time t
- We designate a sent message M by $M@(ro, i) : x, y, z, t \rightarrow AS$, where AS stands for a set of recipients of the form $B : t$
  - B denotes a principal, t denotes the time it receives a message
- These are added to a Network constraint set

Timed Send

$$\{(ro, i, j, x, y, z)\ (+M@t \cdot P)\ \&\ PS \mid \{Net\} \mid \bar{t}\}$$
$$\longrightarrow_{(ro,i,j,+(M\sigma'),0,\bar{t})}$$
$$\{(ro, i, j+1, x, y, z)\ P\sigma'\ \&\ PS \mid \{(M\sigma'@(ro, i) : x, y, z, \bar{t} \to \emptyset), Net\} \mid \bar{t}\}$$
$$\textit{if}\ (M\sigma' : (ro, i) : x, y, z, \bar{t} \to \emptyset) \notin Net$$
where σ *is a ground substitution binding choice variables in* M
$$\textit{and}\ \sigma' = \sigma \uplus \{t \mapsto \bar{t}\} \qquad \text{(TPA++)}$$

Timed Receive

$$\{(ro, i, j, x, y, z)\ (-(M@t) \cdot P)\ \&\ PS \mid \{(M'@((ro', k) : x', y', z', t' \to AS)), Net\} \mid \bar{t}\}$$

$$\longrightarrow_{(ro, i, j, -(M\sigma'), 0, \bar{t})}$$

$$\{(ro, i, j+1, x, y, z)\ P\sigma'\ \&\ PS \mid \{(M'@((ro', k) : x', y', z', t' \to (AS \uplus (ro, i) : \bar{t})), Net\} \mid \bar{t}\}$$

IF $\exists \sigma : M' =_{E_{\mathcal{P}}} M\sigma, \bar{t} = t' + d((x, y, z), (x', y', z')), \sigma' = \sigma \uplus \{t \mapsto \hat{t}\}$

(TPA-)

Further Constraints

General Time and Space

- Constraints on distance:
  $d(A, A) = 0, d(A, B) = d(B, A), d(A, B) \leq d(A, C) + d(B, C)$
- For every message $M@A : t \rightarrow AS$ stored in the network,
  $t' = t + d(A, B)$ for any $B : t'$ in AS

Constraints Specific to Problem

- Wireless Line-of-Sight Constraint
  - If $M@A : t \rightarrow AS$, and $(B, t') \in AS$, then
    if $((d(A, C) \leq d(A, B)$, then $(C, t'') \in AS$ for some $t'')$

All constraints on space and time sent to SMT solver

Outline

Experiments (1/3)

- Brands & Chaum: Shown secure against Mafia fraud- fully symbolic, bounded number of principals

```
smt(((dai +=+ dbi) > d) and (dbi > 0/1) and (dab > 0/1) and (dai > 0/1) and
   ((dab *=* dab) === ((((ax -=- bx) *=* (ax -=- bx)) +=+ ((ay -=- by) *=* (ay -=- by)))
                                      +=+ ((az -=- bz) *=* (az -=- bz)))))
```

- Brands & Chaum:Shown insecure against hijacking attack - fully symbolic, bounded number of principals

```
smt( (dai > d) and (dab <= d))
```

Experiments (2/3)

- Secure Localization: Hyperbola attack - one specific configuration

```
smt( --- hyperbola with a^2 = 4, b^2 = 5, c^2 = 9
(t > t0) and (t0 === 0/1) and (z1 === 0/1) and
(be1z === 0/1) and (be2z === 0/1) and (be3z === 0/1) and
(be4z === 0/1) and (baz === 0/1) and
((be1x === 3/1) and (be1y === 5/2)) and
((be2x === 3/1) and (be2y === -(5/2))) and
((be3x === 4/1) and ((be3y *=* be3y) === 60/4) and (be3y > 0/1)) and
((be4x === 4/1) and ((be4y *=* be4y) === 60/4) and (be4y < 0/1)) and
(x1 === -(3/1)) and (dx === 3/1) and (dy === y1) and (y1 === 0/1))
```

First Try at Solving Constraints for Beacons in a Rectangle (fully symbolic)

- Assume beacons at $(0,0),(0,w),(h,0),(w,h)$
- Attacker can only fake its distance by the same amount d for each beacon
  - This can be deduced from the constraints of the problem
- Constraints as follows
  1. $w > 0, h > 0, d \neq 0$
  2. All distance, real and fake, are positive (8 constraints)
  3. 2 quadratic equations for each beacon, one with the real distance as radius and real location as a solution, one with the fake distance and fake location
- Total of 11 inequalities, and 8 quadratic equations
- Every single SMT solver we tried it on tanked

Second Try

- Manually simplified the equations by addition, subtraction, and multiplication
- Wound up with the following, which only Mathematica could handle

```
In[8]:= Solve[w > 0 && h > 0 && d != 0 && d1 > 0 && d2 > 0 && d3 > 0 && d4 > 0 && (d1-d) > 0 && (d2 - d) > 0 &&
    (d3 - d) > 0 && (d4 - d) > 0 && (((d1 == d2) && (d2 == d4)) || ((d1 == d3) && d2 == d4)) &&
   x == (1 / 2) * w && y == ((((d1 ^ 2) - (d3 ^ 2)) + (w ^ 2)) / (2 * w)) && x ^ 2 + y ^ 2 == d1 ^ 2 &&
   (((2 * d * (d3 - d1)) / h) * y) ^ 2 + (d * ((d3 - d1) / h)) ^ 2 + (2 * d1 * d) - d ^ 2 == 0, {d}, Reals]

Out[8]= { }
```

Outline

Conclusion

- We've shown how it is possible to use symbolic methods to reason about crypto protocols that rely on properties of time and space
- Still easy to run into issues that limit the ability to perform fully symbolic reasoning
- Number of ways in which we can explore this further
  - Concentrate on specific classes of problems where solutions and methodologies can be reused
    - This has already been done to some extent for distance bounding
  - Develop ways of breaking down problems so that they can be better handled by available tools
    - Did this to some extent for secure localization
- There's a lot to explore out there!

References

- Damian Aparicio-Sanchez, Santiago Escobar, Catherine A. Meadows, Jose Meseguer, Julia Sapina: Protocol Analysis with Time. INDOCRYPT 2020: 128-150
- Damian Aparicio-Sanchez, Santiago Escobar, Catherine A. Meadows, Jose Meseguer, Julia Sapina: Protocol Analysis with Time and Space. Protocols, Strands, and Logic 2021: 22-49
- Stefan Brands, David Chaum: Distance-Bounding Protocols (Extended Abstract). EUROCRYPT 1993: 344-359
- Vitaly Shmatikov, Ming-Hsiu Wang: Secure Verification of Location Claims with Simultaneous Distance Modification. ASIAN 2007: 181-195
- Link to Experiments: http://personales.upv.es/sanesro/guttman2021