Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

SAT-based Verifiction of NSPKT Protocol Including Delays in the Network

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Czestochowa University of Technology
Cardinal Stefan Wyszynski University

MMFT2017

Ministerstwo Nauki i Szkolnictwa Wyższego

Organizacja IX Konferencji Modelowanie Matematyczne w Fizyce i Technice (MMFT 2017)
- zadanie finansowane w ramach umowy 829/P-DUN/2017 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

1 Introduction
2 State of Research
3 Our Approach
4 SAT-testing
5 Summary
6 References

Importance of Security Protocols

- Key point of security systems
- Used in many areas
- Errors in: structure, operations, security
- Specification and verification importance
- Need for the complete formal model
- IT market development sets new requirements

New Challenges

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

- Detailed analysis of the protocol
- "Tailor-made" security
- The importance of time

World Leaders

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

- AVISPA
- ProVerif
- Scyther
- VerIcs
- PRISM

Basic elements

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Protocol definition (with time aspect)

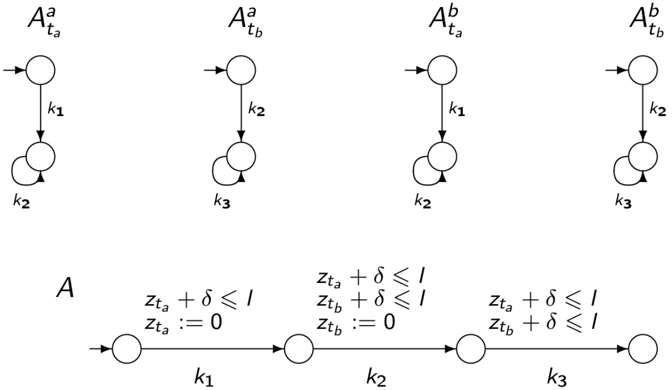
$$\begin{aligned} \alpha^1 &= (S_{\rightarrow}, R_{\leftarrow}, L), \\ \alpha^2 &= (\tau, D, X, G, tc) \end{aligned} \tag{1}$$

Example: Needham-Schroeder Public Key Protocol

$$
\begin{aligned}
\alpha_1 &= (\alpha_1^1, \alpha_1^2),\\
\alpha_1^1 &= (\mathcal{A}; \mathcal{B}; \langle \tau_\mathcal{A} \cdot \mathcal{I}_\mathcal{A} \rangle_{\mathcal{K}_\mathcal{B}}),\\
\alpha_1^2 &= (\tau_1; D_1; \{\tau_\mathcal{A}, \mathcal{I}_\mathcal{A}, \mathcal{K}_\mathcal{B}\}; \{\tau_\mathcal{A}\}; \tau_1 + \mathcal{D}_1 - \tau_\mathcal{A} \leqslant \mathcal{L}),\\
\\
\alpha_2 &= (\alpha_2^1, \alpha_2^2),\\
\alpha_2^1 &= (\mathcal{B}; \mathcal{A}; \langle \tau_\mathcal{B} \cdot \tau_\mathcal{A} \rangle_{\mathcal{K}_\mathcal{A}}),\\
\alpha_2^2 &= (\tau_2; \mathcal{D}_2; \{\tau_\mathcal{B}, \tau_\mathcal{A}, \mathcal{K}_\mathcal{A}\}; \{\tau_\mathcal{B}\}; \tau_2 + \mathcal{D}_2 - \tau_\mathcal{A} \leqslant \mathcal{L} \wedge \tau_2 + \mathcal{D}_2 - \tau_\mathcal{B} \leqslant \mathcal{L}),\\
\\
\alpha_3 &= (\alpha_3^1, \alpha_3^2),\\
\alpha_3^1 &= (\mathcal{A}; \mathcal{B}; \langle \tau_\mathcal{B} \rangle_{\mathcal{K}_\mathcal{B}}),\\
\alpha_3^2 &= (\tau_3; \mathcal{D}_3; \{\tau_\mathcal{A}, \mathcal{K}_\mathcal{B}\}; \{\emptyset\}; \tau_3 + \mathcal{D}_3 - \tau_\mathcal{A} \leqslant \mathcal{L} \wedge \tau_3 + \mathcal{D}_3 - \tau_\mathcal{B} \leqslant \mathcal{L}).
\end{aligned}
$$

Automata Model

Network of synchronized timed automata for NSPK protocol

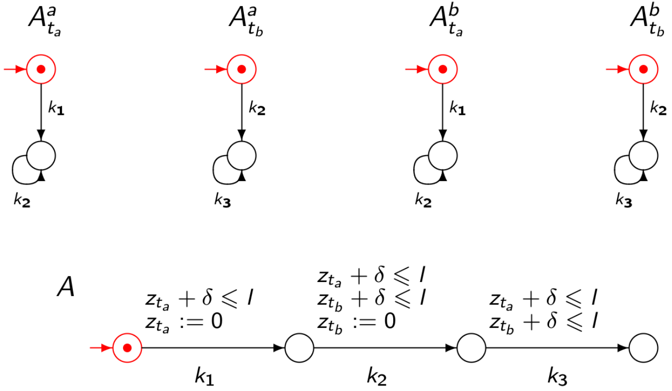


Automata Model

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

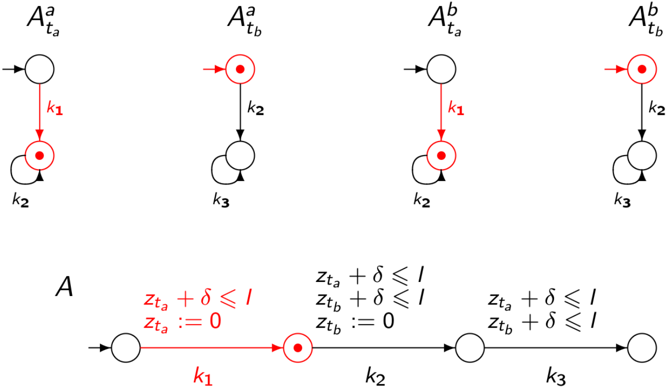
Network of synchronized timed automata for NSPK protocol



Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Network of synchronized timed automata for NSPK protocol

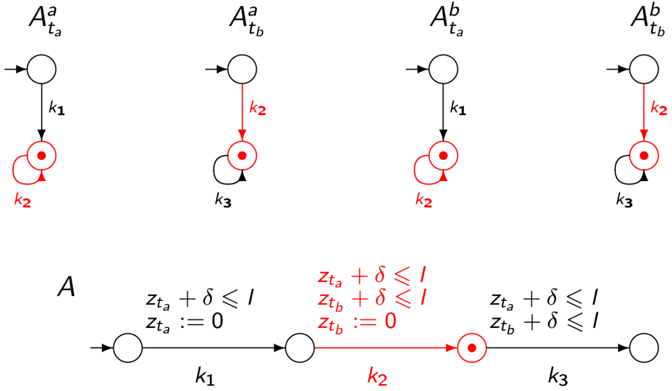


Automata Model

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

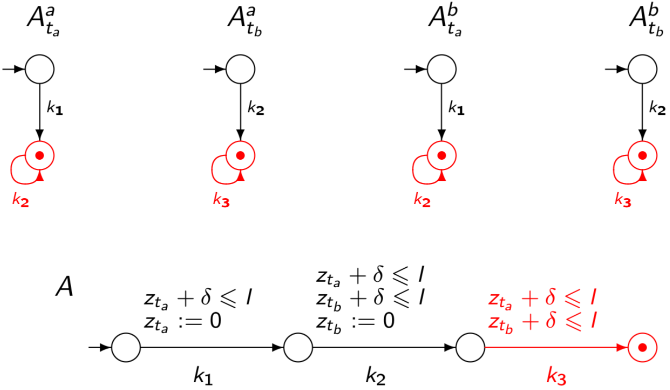
Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Network of synchronized timed automata for NSPK protocol



Automata Model

Network of synchronized timed automata for NSPK protocol



Time dependencies

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Message composing time

$$T_c = T_{sz} + T_g \tag{2}$$

Duration of k-step

$$T_k = T_{sz} + T_g + D + T_{dsz} \tag{3}$$

$$T_k^{min} = T_{sz} + T_g + D_{min} + T_{dsz} \tag{4}$$

$$T_k^{max} = T_{sz} + T_g + D_{max} + T_{dsz} \tag{5}$$

Time dependencies

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Session time

$$T_{ses} = \sum_{k=1}^{n} T_k \tag{6}$$

$$T_{ses}^{min} = \sum_{k=1}^{n} T_k^{min} \tag{7}$$

$$T_{ses}^{max} = \sum_{k=1}^{n} T_k^{max} \tag{8}$$

Time dependencies

Lifetime in single step

$$T_k^{out} = \sum_{i=k}^{n} T_i^{max} \tag{9}$$

where:

- k – step number,
- n – number of all steps in protocol,
- T_i^{max} – maximum time of step execution.

Steps of Procedure

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

- Writing protocol in ProToc language.
- Generating a set of protocol executions.
- Generating a network of timed automata.
- Generating a formulas for SAT-Solver.
- SAT-Solver testing.
- Saving results to a file.

Selected SAT-solvers

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Protocols	Mini-SAT	Lingeling	Clasp	Glucose	Treengeling
Memory [MB]					
NSPK	2,95	2,99	3,01	3,2	4
$NSPK_{Lowe}$	3,95	4,4	4,02	4,23	5
Time [ms]					
NSPK	48	56	60	200	260
$NSPK_{Lowe}$	360	400	370	560	430

Experimental results for NSPK protocol

Length of path	Variables	Clauses	Memory [MB]	Time [ms]	Result
2	6087	15781	2,19	8	UNSAT
3	7322	18829	2,19	8	UNSAT
4	13873	34298	2,48	20	UNSAT
5	15051	37188	2,55	28	UNSAT
6	21849	53246	2,95	48	SAT

Time assumptions:

- Delays in $D = 0,15[tu]$,
- lifetime $Lf = 2[tu]$

Susceptibility to Attack

Protocol NSPK will be vulnerable to attack if

- in the first step: $D \leqslant Lf$
- in the second step: $D \leqslant Lf/4$
- in the last step: $D \leqslant Lf/5$

Experimental results for NSPK protocol, with time restrictions

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

Length of path	Variables	Clauses	Memory [MB]	Time [ms]	Result
2	6216	16118	2,19	8	UNSAT
3	7533	19366	2,18	12	UNSAT
4	14177	35054	2,48	32	UNSAT
5	15431	38130	2,55	28	UNSAT
6	22334	54435	2,95	80	UNSAT

Time assumptions:

- Delay in the following steps $D_1 = 10,1[tu]$, $D_2 = 2,6[tu]$, $D_3 = 2,1[tu]$,
- lifetime $Lf = 10[tu]$

Summary

Sabina Szymoniak, Olga Siedlecka-Lamch, Mirosław Kurkowski

Introduction
State of Research
Our Approach
SAT-testing
Summary
References

- Presented method can be used for fast and simple protocol verification.
- With the implemented tool, we can not only find the attack on the protocol, but also check if the protocol makes sense.
- Shown time constraints, enable us to determine the protocol time frame in which it is vulnerable to attack.
- This is one of the steps to accurately show the strengths and weaknesses of security protocols.

References I

Armando, A., et. al.: The AVISPA tool for the automated validation of internet security protocols and applications. In: Proc. of 17th Int. Conf. on Computer Aided Verification (CAV'05), vol. 3576 of LNCS, pp. 281–285, Springer (2005)

Burrows M., Abadi M., Needham R.: A Logic of Authentication, In: Proceedings of the Royal Society of London A, vol. 426, pp. 233–271, (1989)

Cremers, C.: The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols, In: Proceedings of the 20th International Conference on Computer Aided Verification, Princeton, USA, pp 414–418 (2008)

Dolev, D. and Yao, A.: On the security of public key protocols. In: IEEE Transactions on Information Theory, 29(2), pp. 198–207 (1983)

Kurkowski M., Penczek W.: Applying Timed Automata to Model Checking of Security Protocols, in ed. J. Wang, Handbook of Finite State Based Models and Applications, pp. 223–254, CRC Press, Boca Raton, USA (2012)

Lowe, G.: Breaking and Fixing the Needham-Schroeder Public-key Protocol Using fdr., In:TACAS, LNCS, Springer, pp. 147–166 (1996)

Needham, R. M., Schroeder, M.D.: Using encryption for authentication in large networks of computers. Commun. ACM, 21(12), 993–999 (1978)

Paulson L.: Inductive Analysis of the Internet Protocol TLS, TR440, University of Cambridge, Computer Laboratory (1998)