

Intrusion Tolerance as a Two-Level Game¹

Visit to the University of Melbourne

Kim Hammar

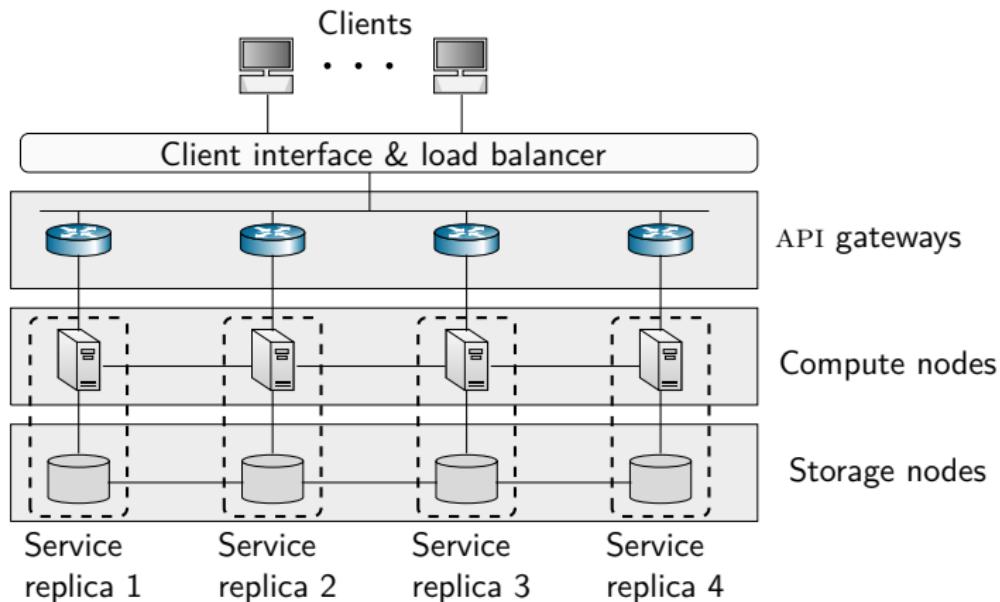
kimham@kth.se
KTH Royal Institute of Technology

June 20, 2024



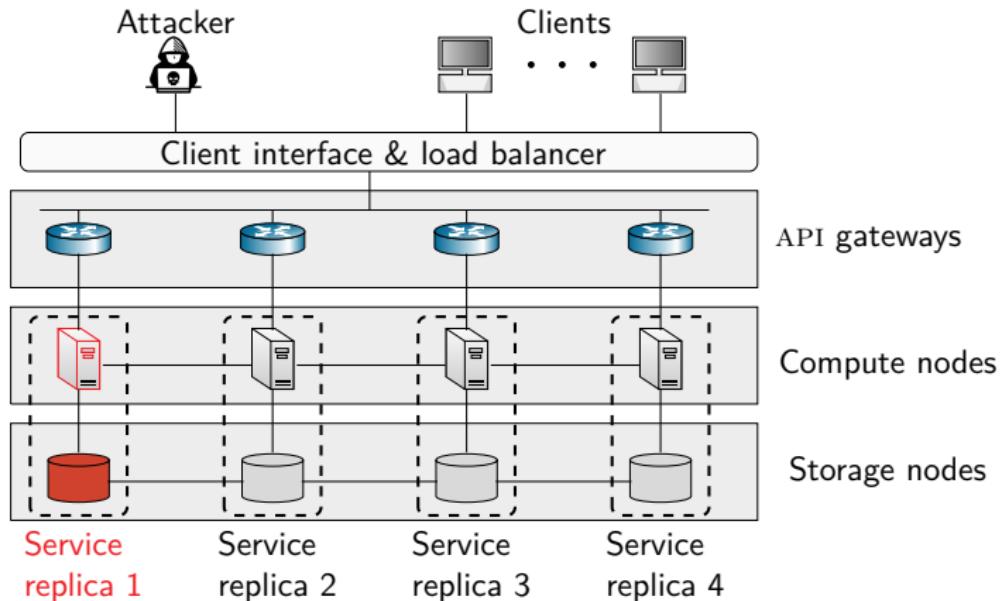
¹Paper to appear in International Conference on Dependable Systems and Networks, IEEE DSN 2024, June 24-27, Brisbane, Australia

Use Case: Intrusion Tolerance



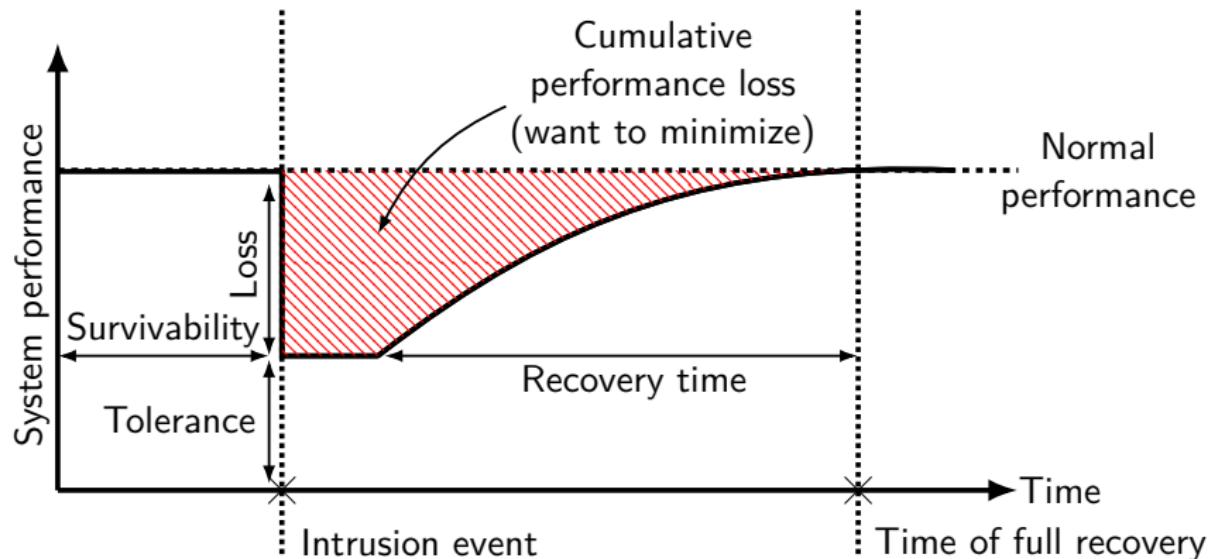
- ▶ A **replicated system** offers a service to a client population.
- ▶ The system should provide **service without disruption**.

Use Case: Intrusion Tolerance



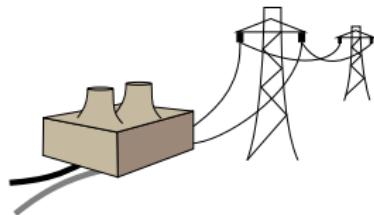
- ▶ An **attacker** seeks to intrude on the system and disrupt service.
- ▶ The system should **tolerate intrusions**.

Intrusion Tolerance (Simplified)



Increasing Demand for Intrusion-Tolerant Systems

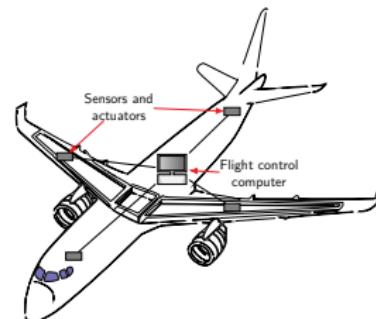
- ▶ As our **reliance on online services grows**, there is an increasing demand for intrusion-tolerant systems.
- ▶ Example applications:



Power grids
e.g., SCADA systems².



Safety-critical IT systems
e.g., banking systems,
e-commerce applications³,
healthcare systems, etc.



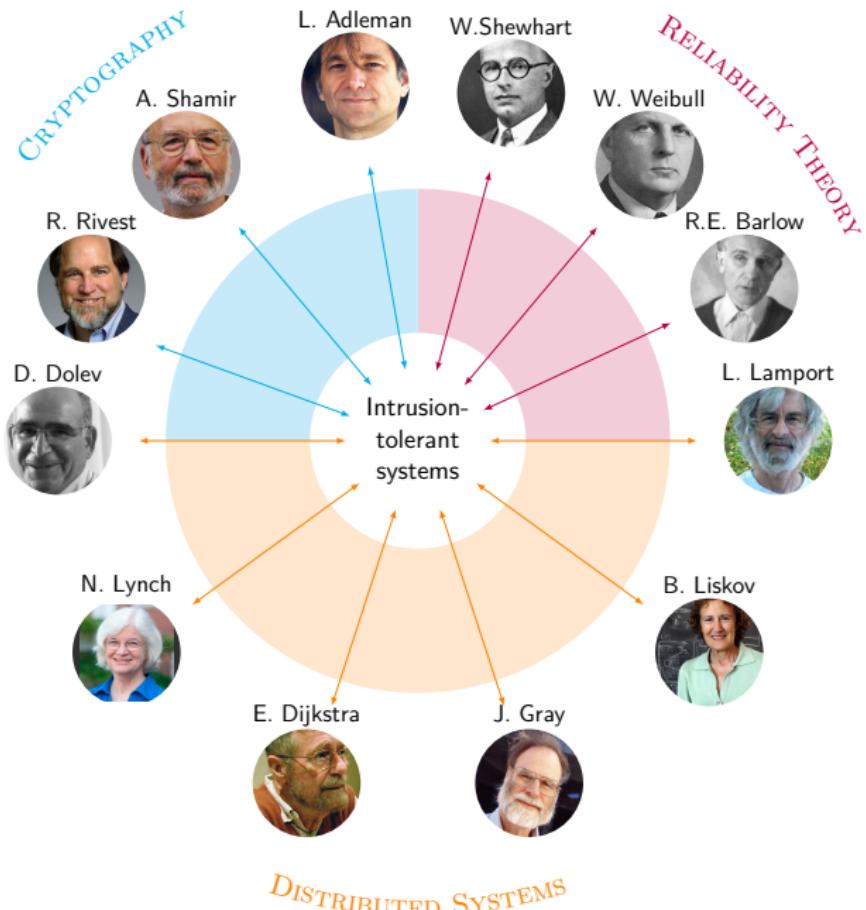
Real-time control systems
e.g., flight control computer⁴.

²Amy Babay et al. "Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid". In: *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 2018, pp. 255–266. DOI: [10.1109/DSN.2018.00036](https://doi.org/10.1109/DSN.2018.00036).

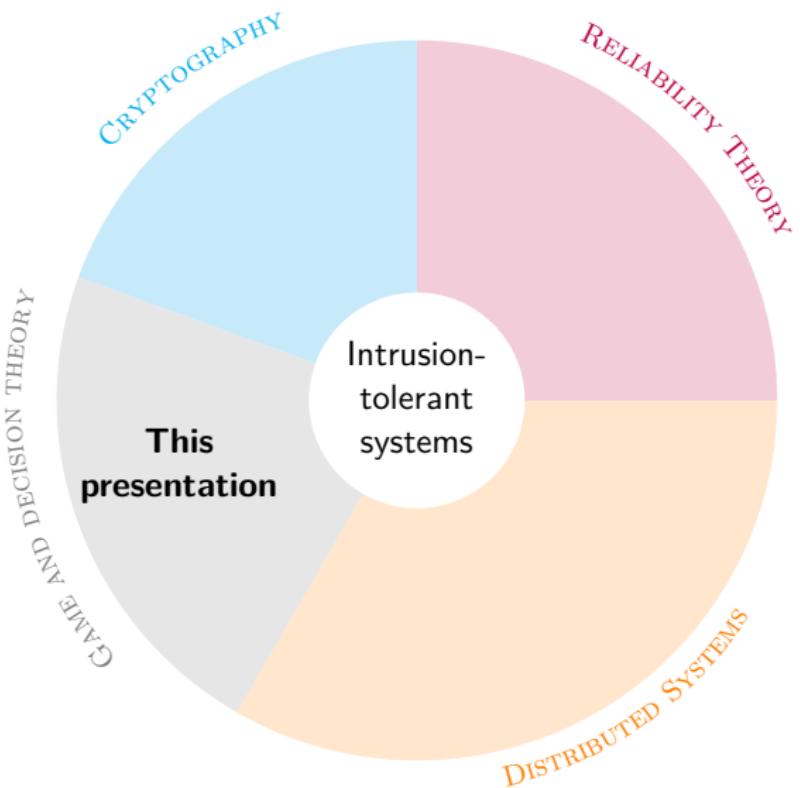
³Jukka Soikkeli et al. "Redundancy Planning for Cost Efficient Resilience to Cyber Attacks". In: *IEEE Transactions on Dependable and Secure Computing* 20.2 (2023), pp. 1154–1168. DOI: [10.1109/TDSC.2022.3151462](https://doi.org/10.1109/TDSC.2022.3151462).

⁴J.H. Wensley et al. "SIFT: Design and analysis of a fault-tolerant computer for aircraft control". In: *Proceedings of the IEEE* 66.10 (1978), pp. 1240–1255. DOI: [10.1109/PROC.1978.11114](https://doi.org/10.1109/PROC.1978.11114).

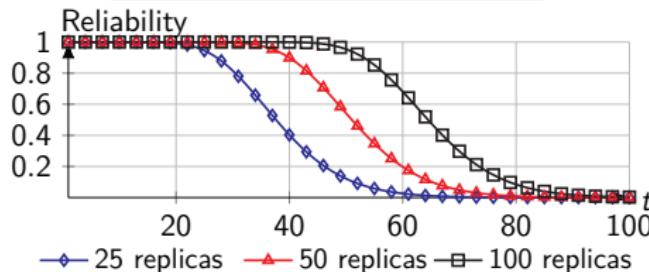
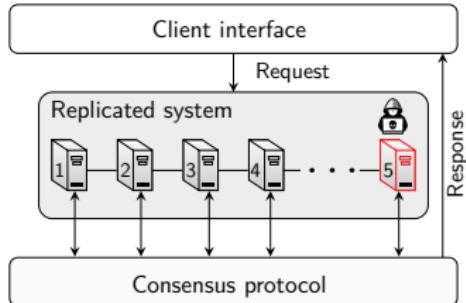
Theoretical Foundations of Intrusion Tolerance



Our Contribution



Building Blocks of An Intrusion-Tolerant System

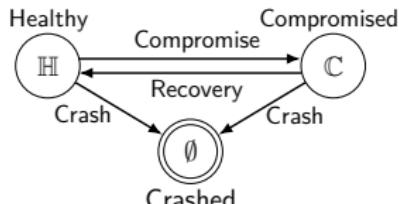


1. Intrusion-tolerant consensus protocol

A quorum needs to reach agreement to tolerate f compromised replicas.

2. Replication strategy

Cost-reliability trade-off.



3. Recovery strategy

Compromises will occur as $t \rightarrow \infty$.

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

Abstract. Rampart is a toolkit of protocols to facilitate the development of *high-integrity* services, i.e., distributed systems that provide availability and correctness despite the malicious behavior of up to t component servers by an attacker. At the core of Rampart are a set of protocols that solve several basic problems in distributed systems, including asynchronous group membership, reliable broadcast, consensus (e.g., leader election and atomic agreement), and atomic multicast. Using these primitives, Rampart supports the development of high-integrity services via *replication* and *machine replication*, and also extends this technique with a new approach to server output voting. In this paper we give a brief overview of Rampart, focusing primarily on its protocol architecture. We also sketch its performance in our prototype implementation and ongoing work.

Published 1995

- Fixed number of replicas
- No recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
xmitter@research.att.com

Abstract. RAMPAN is a toolkit of protocols to facilitate the development of high-integrity services, i.e., distributed services that retain their integrity even in the presence of a malicious component. It provides a framework for specifying and implementing protocols that serve several basic problems in distributed computing, including asynchronous group membership, reliable multichannel (Byzantine) agreement, and atomic multicast. Using these protocols, RAMPAN supports the development of high-integrity services via the techniques of static machine realization, and also extends the techniques with a new approach called *realization with partial knowledge*. The latter approach allows us to focus primarily on security issues, while leaving the details of performance optimization to the system implementer. We also sketch how RAMPAN can be used to implement distributed systems with strong consistency guarantees.

The SecureRing Protocols for Securing Group Communication*

Kim Potter Kihlstrom, L. E. Moser, P. M. Melliar-Smith

*Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106*

kimk@alpha.ece.ucsb.edu, moser@ece.ucsb.edu, pmms@ece.ucsb.edu

Abstract

The SecureRing group communication protocols provide reliable ordered message delivery and group members services despite Byzantine faults such as might be caused by modifications to the programs of a group member following illicit access to, or capture of, a group member.

Published 1998

- Fixed number of replicas
 - No recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication*

Kim Potter Kuhlstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@alpha.ece.ucsb.edu, moser@ece.ucsb.edu, pmms@ece.ucsb.edu

Abstract

The Securing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modifications to the programs of a group member following illicit access to, or capture of, a group member. The

protocols within an asynchronous distributed system impose a common total order on messages, and i consistent group membership.

The approach adopted by SecuringRing to protect Byzantine faults is to optimize the performance mal (fault-free) operation and to pay a performance

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO

Microsoft Research
and

BARBARA LISKOV
MIT Laboratory for Computer Science

Published 2002

Our growing reliance on online services that provide correct service with malicious attacks are a major cause of error, that is, Byzantine faults. This article used to build highly available systems to implement real services: it performs Internet, it incorporates mechanisms replicas proactively. The recovery mechani

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
rampart@research.att.com

The SecureRing Protocols for Securing Group Communication*

Kim Potter Kuhlstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@csba.ece.acsl.edu, moser@ece.acsl.edu, pmms@ece.acsl.edu

Abstract

The SecuringRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modifications to the programs of a group member following illicit access to, or capture of, a group member. The

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

Our growing reliance on online services accessible on the Internet demands highly available systems that can tolerate failures, with increasing concern regarding security and malicious attacks as a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement replicated services; it performs well, it is safe in asymptotic terms, and safe in the Internet, it incorporates mechanisms to defend against Byzantine-faulty clients, and it recovers replicas proactively. The recovery mechanism allows the algorithm to tolerate any number of faults

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
{R.J.Stroud,J.P.Warne,Peter.Ryan}@ncl.ac.uk
Ian.Welch@mcs.vt.edu

Published 2004

Abstract

MAFTIA was a three-year European research project that explored the use of fault-tolerant techniques to build intrusion-tolerant systems. The MAFTIA architecture embodies a number of key design

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication*

Kim Putter Kibrström, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@eipha.ece.ucsb.edu, moser@ece.acsh.edu, pmms@ece.acsh.edu

Abstract

The SecuringRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modifications to the programs of a group member following illicit access to, or capture of, a group member. The

processors within an asynchronous distributed system have a consistent total order on messages, and i consistent group memberships.

The approach adopted by SecuringRing to prevent Byzantine faults is to optimize the performance mal (fault-free) operation and to pay a performance

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
(R.J.Stroud, J.P.Warne, Peter.Ryan)@ncl.ac.uk
Ian.Welch@mcs.vuw.ac.nz

Abstract

MAFTIA was a three-year European research project that explored the use of fault-tolerance techniques to build intrusion-tolerant systems. The MAFTIA architecture embodies a number of key design

presence of malicious faults, i.e., deliberate attack the security of the system by both insiders outsiders. Such faults are perpetrated by attackers and unauthorized users who try to access and/or destroy information in a system and/or to render system unreliable or unusable. Attacks are facilitated by vulnerabilities and a successful attack results

An architecture for adaptive intrusion-tolerant applications

Partha Pal^{1,*} and Paul Rubel¹, Michael Atighetchi¹, Franklin Webber¹, William H. Sanders², Mouna Seri², HariGovind Ramasamy³, James Lyons², Tod Courtney³, Adnan Agbaria², Michel Cukier³, Jeanna Gossett⁴, Idit Keidar⁵

¹ BBN Technologies, Cambridge, Massachusetts. {ppal, prubel, matighet, fwebber}@bbn.com

² University of Illinois at Urbana-Champaign. {whs, seri, ramasamy, jlyons, tod, adnan}@crhc.uiuc.edu

³ University of Maryland at College Park, Maryland. mckukier@eng.umd.edu ⁴ The Boeing Company. jeanna.m.gossett@boeing.com ⁵ Electrical Engineering.

Published 2006

- Adaptive replication based on heuristics
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Potter Kuhlstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@ece.ucsb.edu, moser@ece.ucsb.edu, pmiss@ece.ucsb.edu

Abstract

The SecureRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modifications to the programs of a group member following illicit access to, or capture of, a group member. The

processors within an asynchronous distributed system pose a consistent total order on messages, and i

consist group memberships.

The approach adopted by SecureRing to protect

Byzantine faults is to optimize the performance

of (fault-free) operation and to pay a performance

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
{R.J.Stroud, J.P.Warne, Peter.Ryan}@ncl.ac.uk
Ian.Welch@mcs.vuw.ac.nz

Abstract

MAFTIA was a three-year European research project that explored the use of fault-tolerance techniques to build intrusion-tolerant systems. The MAFTIA architecture embodies a number of key design

presence of malicious faults, i.e., deliberate attack the security of the system by both insiders and outsiders. Such faults are perpetrated by attackers making unauthorised attempts to access, modify or destroy information in a system, and/or to render system unreliable or unusable. Attacks are facilitated by vulnerabilities and a chosen set of attack methods

An architecture for adaptive intrusion-tolerant applications

Partha Pal^{1,*} and Paul Ruhel¹, Michael Atighetchi¹, Franklin Webber¹, William H. Sanders², Monia Seri², HarGovind Ramasamy³, James Lyons², Tod Courtney⁴, Adnan Agbaria⁵, Michel Cukier⁶, Joanna Gossett⁷, Ilti Keldar⁸

¹ IBM Technologies, Cambridge, Massachusetts. <http://sysc.prakel.mitgat.net/pal/>

² University of Illinois at Urbana-Champaign. <http://sysc.prakel.mitgat.net/pal/>

³ Department of Computer Science, University of College Park, Maryland. <http://sysc.prakel.mitgat.net/pal/>

⁴ The Boeing Company. <http://sysc.prakel.mitgat.net/pal/>

⁵ Department of Electrical Engineering, Technion - Israel Institute of Technology. <http://sysc.prakel.mitgat.net/pal/>

⁶ Department of Electrical Engineering, Tel Aviv University. <http://sysc.prakel.mitgat.net/pal/>

⁷ Department of Electrical Engineering, Tel Aviv University. <http://sysc.prakel.mitgat.net/pal/>

⁸ Department of Electrical Engineering, Tel Aviv University. <http://sysc.prakel.mitgat.net/pal/>

Worm-IT – A wormhole-based intrusion-tolerant group communication system

Miguel Correia ^{a,*}, Nuno Ferreira Neves ^a, Lau Cheuk Lung ^b, Paulo Veríssimo ^a

^a Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C6, Piso 3, 1749-016 Lisboa, Portugal
^b Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, PR, Brazil

Received 26 October 2005; r

Published 2006

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Potter Kihlstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@cs.ucsb.edu, moser@ece.ucsb.edu, pmms@ece.ucsb.edu

Abstract

The *SecureRing* group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modification to the programs of a group member following illicit access to, or capture of, a group member. The

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
(R.J.Stroud, J.P.Warne, Peter.Ryan)@ncl.ac.uk
ian.Welch@ncl.vuw.ac.nz

Worm-IT – A wormhole-based intrusion-tolerant group communication system

Miguel Correia ^{a,*}, Nuno Ferreira Neves ^a, Lau Cheuk Lung ^b, Paulo Veríssimo ^a

^a Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Edifício C8, Piso 3, 1749-002 Lisboa, Portugal
^b Programa de Pós-Graduação em Tecnologia Aplicada, Pontifícia Universidade Católica do Paraná, Rua General Conde, 1155, 80215-900, Brazil

Received 26 October 2005; revised 10 March 2006; accepted 30 March 2006

An architecture for adaptive intrusion-tolerant applications

Partha Pol^{1,*} and Paul Rubel¹, Michael Atighehchi¹, Franklin Webber¹, William H. Sanders², Monna Seri², HarGovind Ramaswamy³, James Lyons², Tod Courtney⁴, Adina Aguirre⁵, Michel Culier⁵, Jerome Gosset⁴, Idit Keidar³

¹ IBM Technologies, Cambridge, Massachusetts, {ppol, prubel, matighechi, franklin}@ibm.com

² University of Illinois at Urbana-Champaign, {whs, seri, rama}@uiuc.edu

³ University of Maryland at College Park, Maryland, mculier@engr.umd.edu⁴ The Boeing Company, jones.o.gosset@FW Boeing.com⁵ Department of Electrical Engineering,

Technion, Israel Institute of Technology, idit@technion.ac.il

Resilient Intrusion Tolerance through Proactive and Reactive Recovery*

Paulo Sousa Alysson Neves Bessani Miguel Correia
Nuno Ferreira Neves Paulo Veríssimo
LASIGE, Faculdade de Ciências da Universidade de Lisboa – Portugal
{pj.sousa, bessani, mpc, nuno, pjv}@di.fc.ul.pt

Published 2007

- Fixed number of replicas
- **Supports both periodic and reactive recoveries**
- Does not provide reactive recovery strategies

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Potter Kuhlstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@ece.ucsb.edu, moser@ece.ucsb.edu, pmms@ece.ucsb

Abstract

The SecureRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by modification to the programs of a group member following illicit access to, or capture of, a group member. The

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welsh¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
(R.J.Stroud, J.P.Warne, Peter.Ryan)@ncl.ac.uk
ian.Welch@cs.nwu.ac.nz

Worm-IT – A wormhole-based intrusion-tolerant group communication system

Miguel Correia^{a,*}, Nuno Ferreira Neves^b, Lau Cheuk Lung^b, Paulo Veríssimo^a

^a Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Piso 3, 1749-002 Lisboa, Portugal
^b Programa de Pós-Graduação em Ciências da Computação, Pontifícia Universidade Católica do Paraná, Rua Joaquim Nabuco, 1155, 80215-900, Brazil

Received 26 October 2005; revised 10 March 2006; accepted 30 March 2006

An architecture for adaptive intrusion-tolerant applications

Partha Pol^{1,*} and Paul Rubel¹, Michael Atighetechi¹, Franklin Webber¹, William H. Sanders², Monna Serf², HarGovind Ramaswamy³, James Lyons², Tod Courtney⁴, Adina Agustini⁵, Michel Calher⁵, Jerome Gossett⁴, Idit Keidar⁵

¹ IBM Technologies, Cambridge, Massachusetts, {ppol, prubel, matighet, frankweb}@ibm.com

² University of Illinois at Urbana-Champaign, {whs, serf, ramasw, jlyons, tod}

gossett}@uiuc.edu

³ Department of College Park, Maryland, rams@engr.wisc.edu⁴ The Boeing

Company, jessica.o.gossett@FW Boeing.com⁵ Department of Electrical Engineering,

Tel Aviv – Israel Institute of Technology, idit@tx.tau.ac.il

Resilient Intrusion Tolerance through Proactive and Reactive Recovery^{*}

Paulo Sousa Alysson Neves Bessani Miguel Correia

Nuno Ferreira Neves Paulo Veríssimo

LASIGE, Faculdade de Ciências da Universidade de Lisboa – Portugal

{pj.sousa, bessani, mpc, nuno, pnv}@di.fc.ul.pt

State Transfer for Hypervisor-Based Proactive Recovery of Heterogeneous Replicated Services

Tobias Distler Rüdiger Kapitz

Friedrich-Alexander University
Erlangen-Nuremberg, Germany

{distler,rrkapitz}@cs.fau.de

Hans P. Reiser

LASIGE
Universidade de Lisboa, Portugal
hans@di.fc.ul.pt

Published 2011

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Potter Kuhlmann, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kimk@cs.ucsb.edu, moser@ece.ucsb.edu, pmm@ece.ucsb.

Abstract

The *Securing* group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by malfunctions in programs of a group member. *Joining* is implicit access to, or capture of, a group member. The

processors within an asynchronous distributed system pose a consistent total order on messages, and i consistence group memberships.

The approach adopted by *Securing* to protect Byzantine faults is to operate the performance (fault-free) operation and to pay a performance

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTIA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
{R.J.Stroud, J.P.Warne, Peter.Ryan}@ncl.ac.uk
ian.Welch@mcs.vuw.ac.nz

Worm-IT – A wormhole-based intrusion-tolerant group communication system

Miguel Correia ^{a,*}, Nuno Ferreira Neves ^a, Lau Cheuk Lung ^b, Paulo Verissimo ^a

^a Faculdade de Ciéncias da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Piso 3, 1749-016 Lisboa, Portugal
^b Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rue Imbuassuza Conceição, 1155, 80.215-907, Brazil

Received 28 October 2005; received in revised form 28 March 2006; accepted 30 March 2006

An architecture for adaptive intrusion-tolerant applications

Partha Pal^{1,*} and Paul Rubeil¹, Michael Atighetchi¹,
William H. Sanders², Mouna Seri², HarGovind Ramu
Tod Courtney³, Adnan Agbaria³, Michel Cukier³, Jos
Tobias Distler⁴, Rüdiger Kapitz⁴
¹ BBN Technologies, Cambridge, Massachusetts, {ppal, grbel, mihal, whs, mseri, mramu, tdistler, rkapitz}@bbn.com
² University of Illinois at Urbana-Champaign, {tobias, rkapitz}@uiuc.edu
³ University of Maryland at College Park, Maryland, mca@cs.umd.edu
⁴ Computer Science, mca@cfir.BMPC.Boeing.com, Department of Electrical Engineering,
Technion - Israel Institute of Technology, idk@technion.ac.il

State Transfer for Hypervisor-Based Proactive Recovery of Heterogeneous Replicated Services

Hans P. Reiser
Universidade de Lisboa, Portugal
hans@di.fc.ul.pt

Resilient Intrusion Tolerance through Proactive and Reactive Recovery*

Paulo Souto^a Alysson Neves Bessani^a Miguel Correia^a
Nuno Ferreira Neves^a Paulo Verissimo^a
LASIGE, Faculdade de Ciéncias da Universidade de Lisboa - Portugal
{pjsoouto, bessani, mpc, nuno, pnv}@fc.ul.pt

Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid

Amy Babay^a, Thomas Tantillo^a, Trevor Aron, Marco Platania, and Yair Amir
Johns Hopkins University — {babay, tantillo, taron1, yairamir}@cs.jhu.edu
AT&T Labs — {platania}@research.att.com
Spread Concepts LLC — {yairamir}@spreadconcepts.com

Published 2018

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Potter Kuhlstrom¹, L. E. Moser², P. M. Melliar-Smith³
¹ Department of Electrical and Computer Engineering
² University of California, Santa Barbara, CA 93106
kirk@ece.ece.ucsb.edu, moser@ece.ucsb.edu, pmms@ece.ucsb.

Abstract

The SecureRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by malicious users or faulty hardware. Following a failure, they offer access to, or capture of, a group member. The

processes within an asynchronous distributed system

pose a consistent total order on messages, and i

consistent group memberships.

The approach adopted by SecureRing to prevent

Byzantine faults is to optimize the performance

and fault-tolerance of a group of nodes.

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV
MIT Laboratory for Computer Science

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
/R.J.Stroud, J.P.Warne, Peter.Ryan@ncl.ac.uk
Ian.Welch@nccs.vuw.ac.nz

Worm-IT – A wormhole-based intrusion-tolerant group communication system

Miguel Correia ^{a,*}, Nuno Ferreira Neves ^a, Lau Cheuk Lung ^b, Paulo Veríssimo ^a

^a Faculdade de Ciéncias da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Piso 3, 1749-016 Lisboa, Portugal
^b Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rua Imaculada Conceição, 1155, 80.215-901, Brazil

Received 28 October 2005; received in revised form 28 March 2006; accepted 30 March 2006

An architecture for adaptive intrusion-tolerant applications

Partha Pal^{1,*} and Paul Rubel², Michael Atighechi³,
William H. Sanders², Monna Seri², Hartmut Raun
Tom Courtney⁴, Adina Agarwal⁵, Michel Olsker⁵, Joe

¹ BBN Technologies, Cambridge, Massachusetts [ppal, prosh]
² University of Illinois at Urbana-Champaign [whs, seri, vers]
³ University of Maryland at College Park, Maryland, northwestern
Computer Science, jessica.cs.umd.edu/HW.Boring.com² Department of Electrical
Engineering, Israel Institute of Technology, shaf@technion.ac.il

State Transfer for Hypervisor-Based Proactive Recovery of Heterogeneous Replicated Services

Tobias Distler ¹ Rüdiger Kapitzka ¹

Friedrich-Alexander University
Erlangen-Nürnberg, Germany
¹ distler, rkapitzka @fse.fau.de

Hans P. Reiser ²

Universidade de Lisboa, Portugal
hans@fc.ul.pt

Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid

Aug Baker¹, Thomas Baillie², Trevor Attie, Martin Plataniotis, and Yair Arad
¹ John Hopkins University — {dbaker, tsbaillie, tattie, mplataniotis}@cs.jhu.edu
² AT&T Labs — {plattaniotis}@research.att.com
Special Concepts LLC — {yairad}@specialconcepts.com

Resilient Intrusion Tolerance through Proactive a

Pando Souza ¹ Alysson Neves Bassani ¹ Mig
Nuno Ferreira Neves ¹ Paulo Veríssimo ¹
LASIGE, Faculdade de Ciéncias da Universidade de Lisboa — e-mail:
{pjsousa, bassani, nmc, nuno, pvt}@fc.ul.pt

Skynet: a Cyber-Aware Intrusion Tolerant Overseer

Tadeu Freitas, João Soares, Manuel E. Correia, Rolando Martins
Department of Computer Science, Faculty of Science, University of Porto
Email: {tadeufreitas, joao.soares, mdcorrei, rmartins} @fc.up.pt

Published 2023

- Fixed number of replicas
- Periodic recoveries

Prior Work on Intrusion-Tolerant Systems

The Rampart Toolkit for Building High-Integrity Services

Michael K. Reiter

AT&T Bell Laboratories, Holmdel, New Jersey, USA
reiter@research.att.com

The SecureRing Protocols for Securing Group Communication

Kim Foster Kiltzstrom, L. E. Moser, P. M. Melliar-Smith
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
kim@alpha.ece.ucsb.edu, moser@ece.ucsb.edu, pm@ece.ucsb.edu

Abstract
The SecuringRing group communication protocols provide reliable ordered message delivery and group membership services despite Byzantine faults such as might be caused by

An architecture for adaptive intrusion-tolerant applications

Pantelis Paliogianni¹ and Paul Bubel², Michael Albrecht²,
William H. Sanders², Monica Sey³, Hartmut Klaue³,
Tom Courtney³, Adams Agius³, Miguel Cukier³, Jon

¹ IBM Technologies, Cambridge, Massachusetts, USA, paul.paliogianni@us.ibm.com
² University of Regensburg, Department of Computer Science, D-93040 Regensburg, Germany
³ University of Maryland at College Park, Department of Computer Science, 3400 Computer and Space Sciences Building, College Park, MD 20742, USA

State Transfer for Hypervisor-Based Proactive Recovery of Heterogeneous Replicated Services

Tobias Dietrich¹, Rüdiger Kapitza²
Friedrich-Alexander University
Erlangen-Nürnberg, Germany
(tobias.dietrich)@fau.de

Hans P. Reiter¹,
LARGE
Universidade de Lisboa, Portugal
hans@lx.it.pt

-

Network-Attack-Resilient Intrusion-Tolerant SCADA for the Power Grid

Amy Baker¹, Thomas Taft¹, Trevor Arai, Mario Palusz, and Yair Arad
Johns Hopkins University — {tbaker, mopalusz, yarad}@cs.jhu.edu

Special Committee LLC — {trevor}@specialcommittee.com

Can we do better by leveraging game-theoretic strategies?

A Quantitative Analysis of the Intrusion-Tolerance Capabilities of the MAFTA Architecture

Robert Stroud, Ian Welch¹, John Warne, Peter Ryan,
School of Computing Science, University of Newcastle upon Tyne, UK
(R.J.Stroud, J.P.Warne, Peter.Ryan)@ncl.ac.uk
Ian.Welch@ncl.ac.uk

Worm-IT – A wormhole-based intrusion-tolerant group communication system

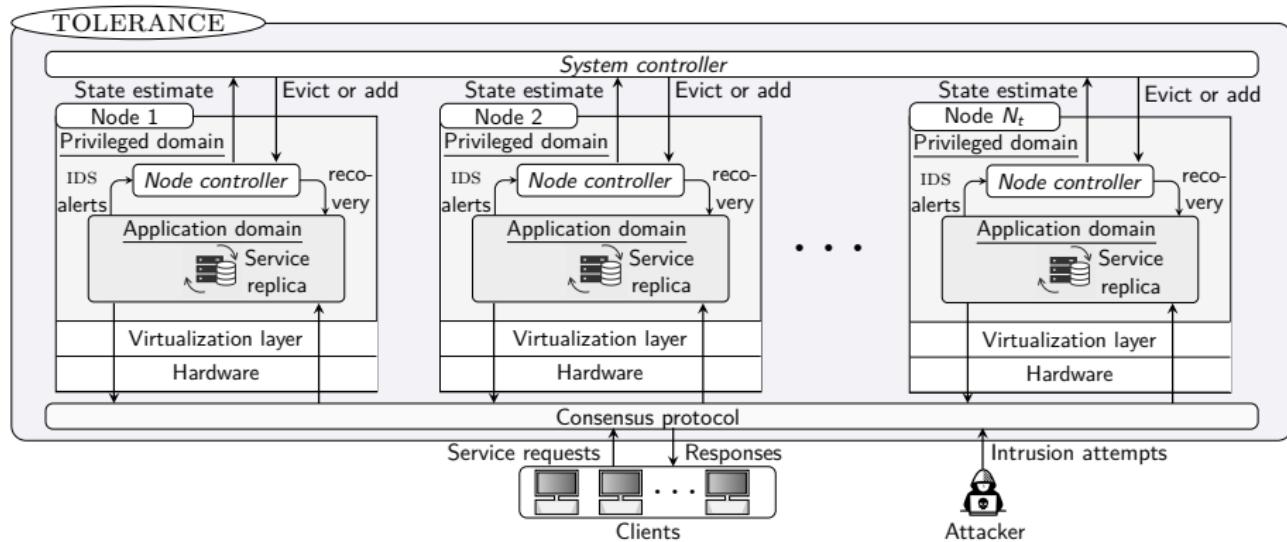
Miguel Correia^{3,4}, Nuno Ferreira Neves³, Lau Cheuk Lung³, Paulo Veríssimo^{3,4}
³ Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Edifício C1, Piso 3, 1749-001 Lisboa, Portugal
⁴ Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rio Brilhante Campus, 1115, 80215-640, Brazil
Received 20 October 2005; revised as revised from 28 March 2006; accepted 30 March 2006

Published 2023

- Fixed number of replicas
- Periodic recoveries

The TOLERANCE Architecture

Two-level recovery and replication control with feedback.



Definition 1 (Correct service)

The system provides **correct service** if the healthy replicas satisfy the following properties:

Each request is eventually executed. (Liveness)

Each executed request was sent by a client. (Validity)

Each replica executes the same request sequence. (Safety)

Proposition 1 (Correctness of TOLERANCE)

*A system that implements the TOLERANCE architecture **provides correct service** if*

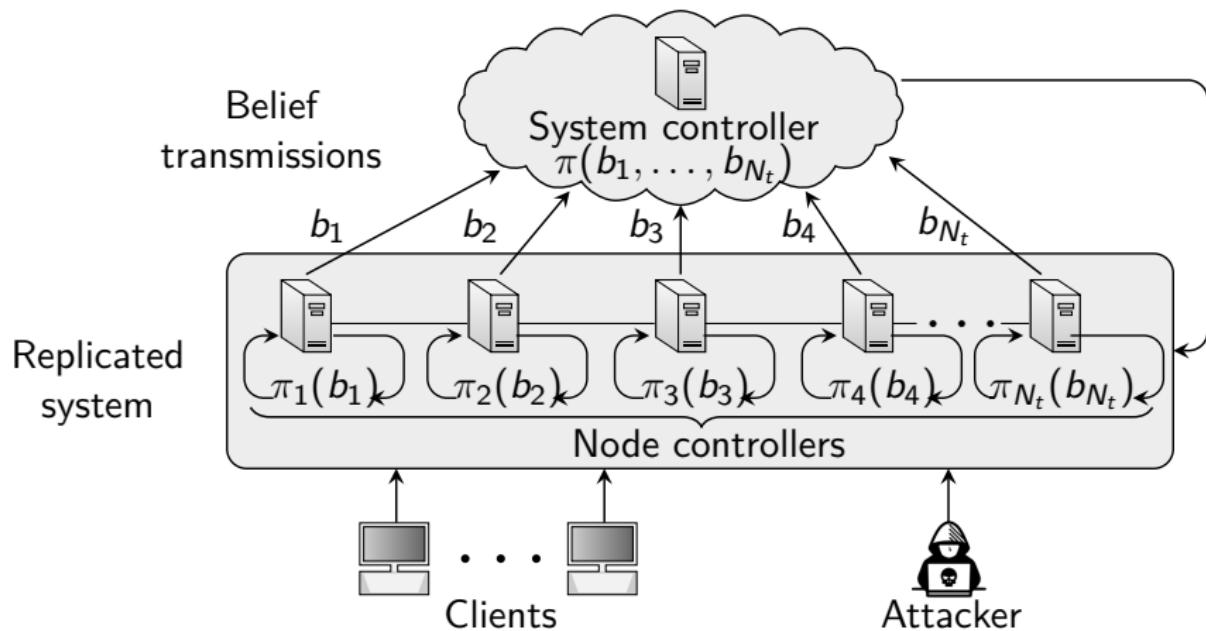
Network links are authenticated.

At most f nodes are compromised or crashed simultaneously.

$$N_t \geq 2f + 1.$$

The system is partially synchronous.

Intrusion Tolerance as a Two-Level Game



- ▶ We formulate intrusion tolerance as a two-level game.
- ▶ The **local game models intrusion recovery**.
- ▶ The **global game models replication control**.

Assumption 1

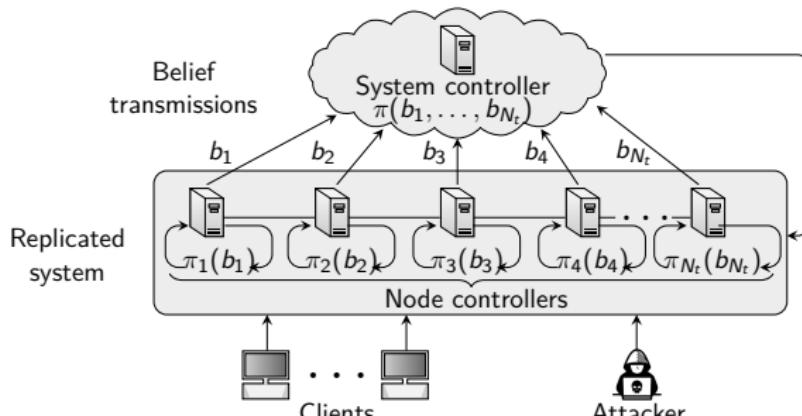
The probability that the system controller fails is negligible.

Assumption 2

Compromise and crash events are statistically independent across nodes.

Assumption 3

The attacker can infer the observations of the controllers.

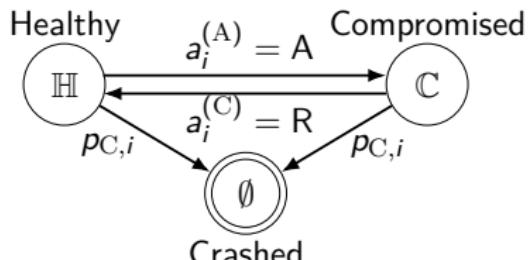


The Local Recovery Game

- ▶ Partially observed stochastic game Γ_i .
- ▶ Players: (C)ontroller and (A)ttacker.

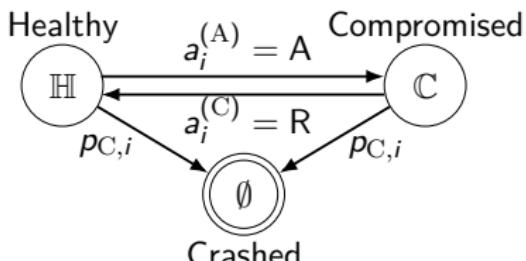
- ▶ Controller actions: (R)ecover and (W)ait.
- ▶ Attacker actions: (A)ttack and (F)alse alarm.

- ▶ States: $\mathcal{S}_N = \{\mathbb{H}, \mathbb{C}, \emptyset\}$.
- ▶ $p_{C,i}$: crash probability, $p_{A,i}$: attack success probability.
- ▶ Observation $o_{i,t} \sim z_i(\cdot | a^{(A)})$: IDS alerts at time t .



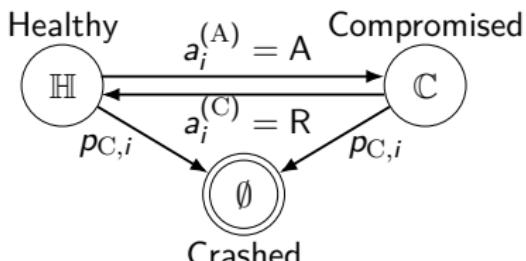
The Local Recovery Game

- ▶ Partially observed stochastic game Γ_i .
- ▶ Players: (C)ontroller and (A)ttacker.
- ▶ Controller actions: (R)ecover and (W)ait.
- ▶ Attacker actions: (A)ttack and (F)alse alarm.
- ▶ States: $\mathcal{S}_N = \{\mathbb{H}, \mathbb{C}, \emptyset\}$.
- ▶ $p_{C,i}$: crash probability, $p_{A,i}$: attack success probability.
- ▶ Observation $o_{i,t} \sim z_i(\cdot | a^{(A)})$: IDS alerts at time t .



The Local Recovery Game

- ▶ Partially observed stochastic game Γ_i .
- ▶ Players: (C)ontroller and (A)ttacker.
- ▶ Controller actions: (R)ecover and (W)ait.
- ▶ Attacker actions: (A)ttack and (F)alse alarm.
- ▶ States: $\mathcal{S}_N = \{\mathbb{H}, \mathbb{C}, \emptyset\}$.
- ▶ $p_{C,i}$: crash probability, $p_{A,i}$: attack success probability.
- ▶ Observation $o_{i,t} \sim z_i(\cdot | a^{(A)})$: IDS alerts at time t .



Node Controller Strategy

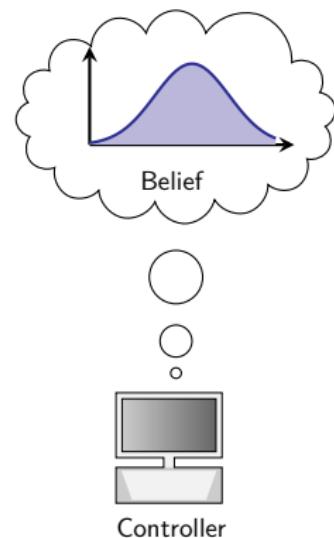
- ▶ The controller computes the **belief**

$$b_{i,t}(s) \triangleq \mathbb{P}[S_{i,t} = \mathbb{C} | \mathbf{h}_t^{(C)}].$$

$$\mathbf{h}_t^{(C)} \triangleq (b_{i,1}, a_{i,1}^{(C)}, o_{i,2}, a_{i,2}^{(C)}, o_{i,3}, \dots, a_{i,t-1}^{(C)}, o_{i,t}).$$

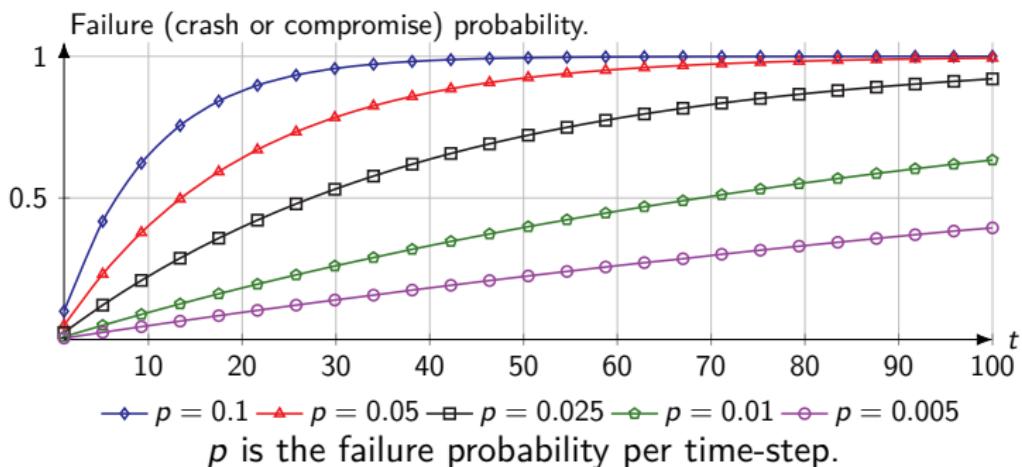
- ▶ Controller strategy:

$$\pi^{(C)} : [0, 1] \rightarrow \Delta(\{W, R\}).$$

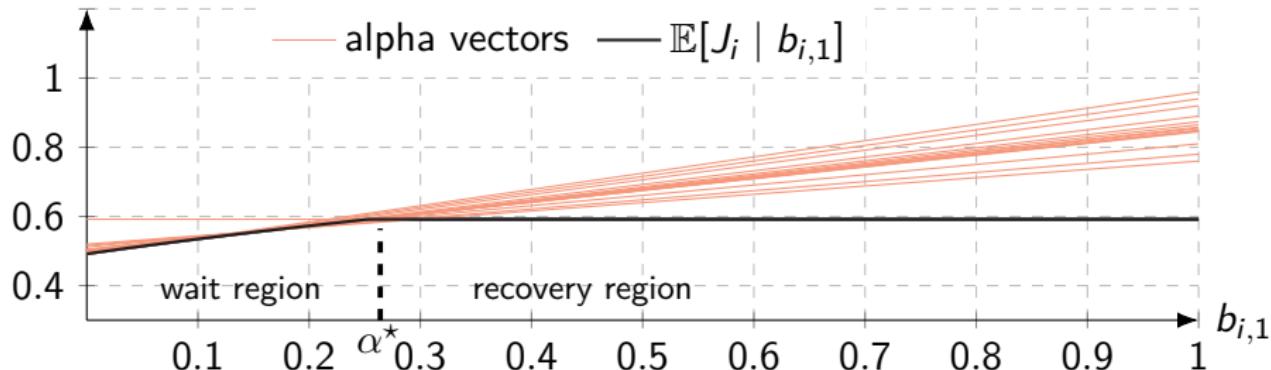


Node Controller Objective

- ▶ **Cost:** $J_i \triangleq \eta T_i^{(R)} + F_i^{(R)}$. (Zero-sum game)
 - ▶ $T_i^{(R)}$ is the average *time-to-recovery*.
 - ▶ $F_i^{(R)}$ is the *recovery frequency*.
 - ▶ $\eta > 1$ is a scaling factor.
- ▶ **Bounded-time-to-recovery constraint:** The time between two recoveries can be at most Δ_R .



Threshold Structure of the Controller's Best Response



The controller's best response value.

Theorem 2

There exists a best response strategy that satisfies

$$\tilde{\pi}_{i,t}^{(C)}(b_{i,t}) = R \iff b_{i,t} \geq \alpha_{i,t}^* \quad \forall t,$$

where $\alpha_{i,t}^ \in [0, 1]$ is a threshold.*

Efficient Computation of Best Responses

Algorithm 1: Threshold Optimization

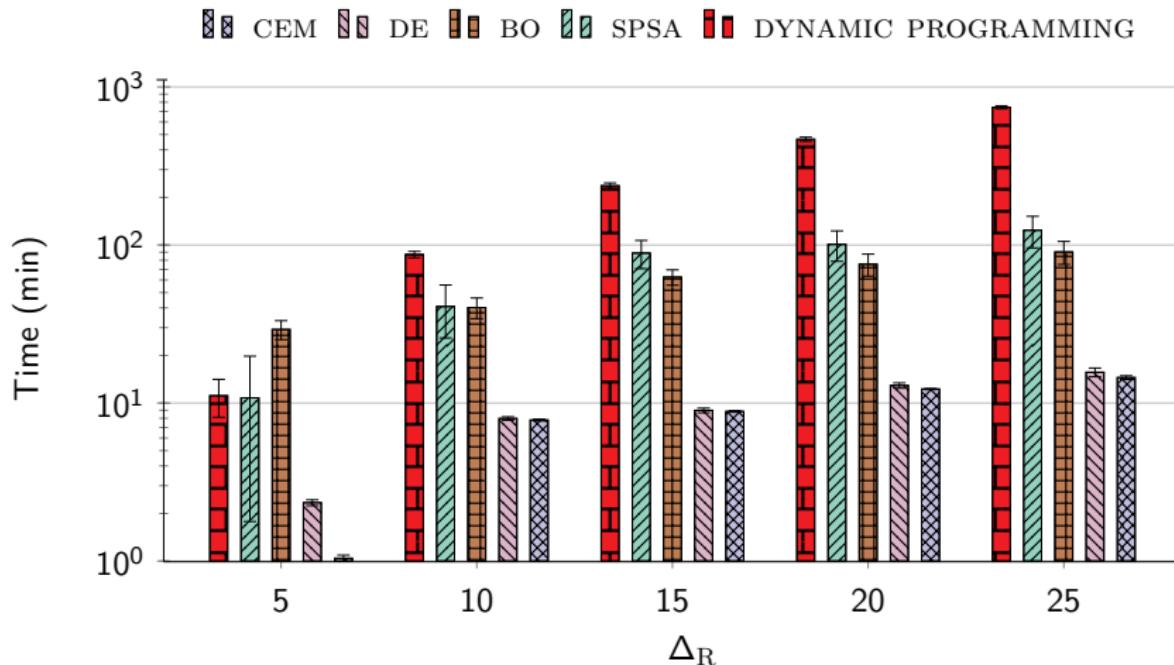
- 1 **Input:** Objective function J_i , parametric optimizer po .
- 2 **Output:** A approximate best response strategy $\hat{\pi}_{i,\theta}^{(C)}$.

3 Algorithm

- 4 $\Theta \leftarrow [0, 1]$.
 - 5 For each $\theta \in \Theta$, define $\pi_{i,\theta}^{(C)}(b_{i,t})$ as
 - 6
$$\pi_{i,\theta}^{(C)}(b_{i,t}) \triangleq \begin{cases} R & \text{if } b_{i,t} \geq \theta \\ W & \text{otherwise.} \end{cases}$$
 - 7 $J_\theta \leftarrow \mathbb{E}_{\pi_{i,\theta}^{(C)}}[J_i]$.
 - 8 $\hat{\pi}_{i,\theta}^{(C)} \leftarrow \text{po}(\Theta, J_\theta)$.
 - 9 **return** $\hat{\pi}_{i,\theta}^{(C)}$.
-

- ▶ Examples of **parameteric optimization algorithmns**: CEM, BO, CMA-ES, DE, SPSA, etc.

Efficient Computation of Best Responses



Mean compute time to obtain a best response for different values of the bounded-time-to-recovery constraint Δ_R .

Definition 3 (Perfect Bayesian equilibrium (PBE))

Let \mathbb{B} denote the belief operator. Then (π^*, \mathbb{B}) is a PBE iff

1. Optimality:

π^* is a Nash equilibrium (NE) in $\Gamma|_{\mathbf{h}_{i,t}^{(C)}}$ $\forall \mathbf{h}_{i,t}^{(C)}$, where $\Gamma|_{\mathbf{h}_{i,t}^{(C)}}$ is the subgame starting from $\mathbb{B}(\mathbf{h}_t^{(C)}, \pi_{i,t}^{*,(A)})$.

2. Belief consistency:

For any $\mathbf{h}_{i,t}^{(C)}$ with $\mathbb{P}[\mathbf{h}_{i,t}^{(C)} | \pi^*, \mathbf{b}_1] > 0$, then

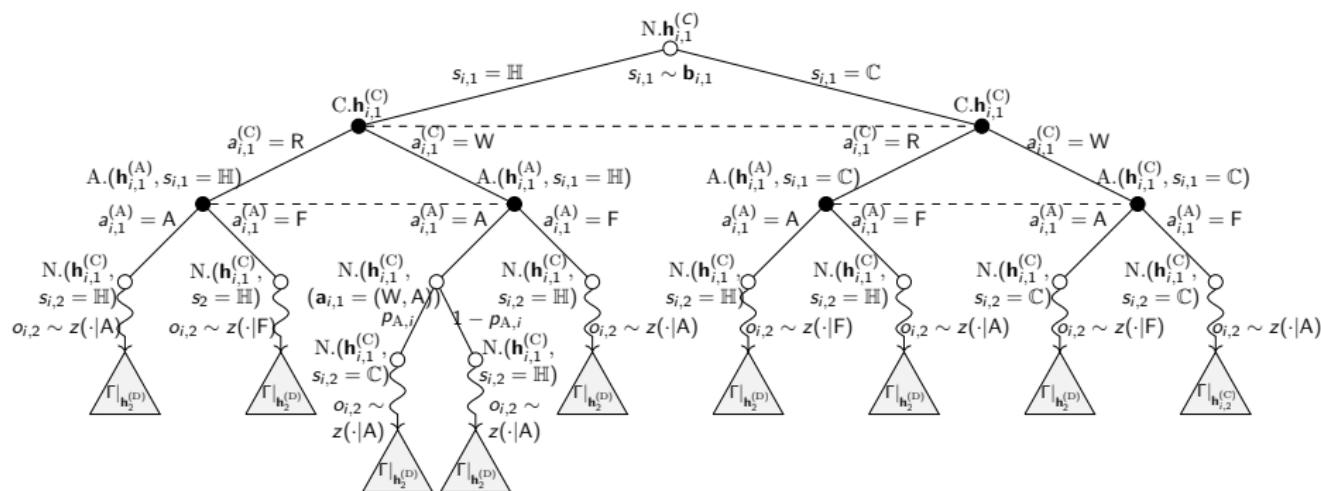
$$\mathbb{B}(\mathbf{h}_{i,t}^{(C)}, \pi_{i,t}^{*,(A)})$$

$$= \mathbb{B}(\mathbb{B}(\mathbf{h}_{i,t-1}^{(C)}, \pi_{i,t}^{*,(A)}), \pi_{i,t}^{*,(C)}(\mathbb{B}(\mathbf{h}_{i,t-1}^{(C)}, \pi_{i,t}^{*,(A)})), o_t, \pi_{i,t}^{*,(A)}).$$

Theorem 4 (Existence of equilibrium and best response)

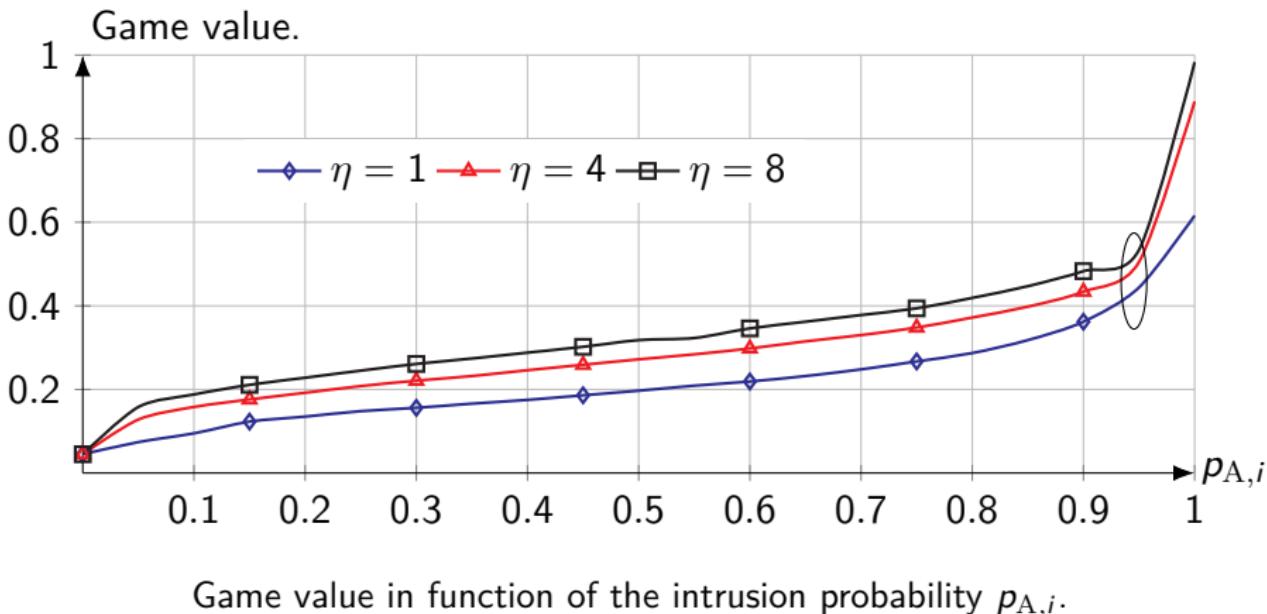
1. For each strategy pair π_i in Γ_i , there exists a pair of best responses.
2. Γ_i has a perfect Bayesian equilibrium (PBE).
3. If $s_{i,t} = 0 \iff b_{i,t} = 0$, then Γ_i has a unique pure PBE.
4. The value of Γ_i is not larger than 1.

Idea Behind the Proof of Equilibrium Existence



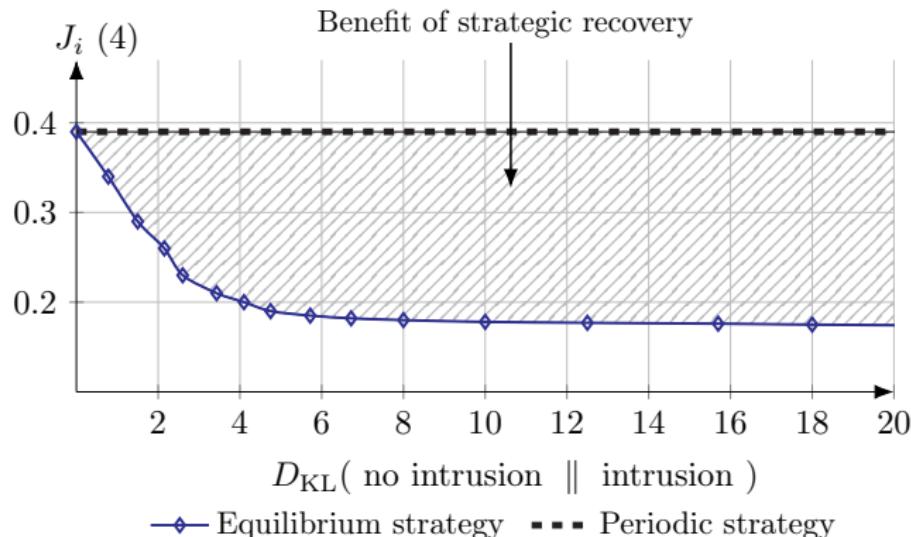
- ▶ Fix the time horizon T . Then we can **convert the game to extensive form**, and hence it has a value.
- ▶ As $T \rightarrow \infty$, the **discount factor** $\gamma \in [0, 1)$ implies that $\lim_{t \rightarrow \infty} \sum_t \gamma^t C_t = 0$, which means that a value exists.

Value of the Local Recovery Game



- We can compute the game value using **Heuristic Search Value Iteration** (HSV).

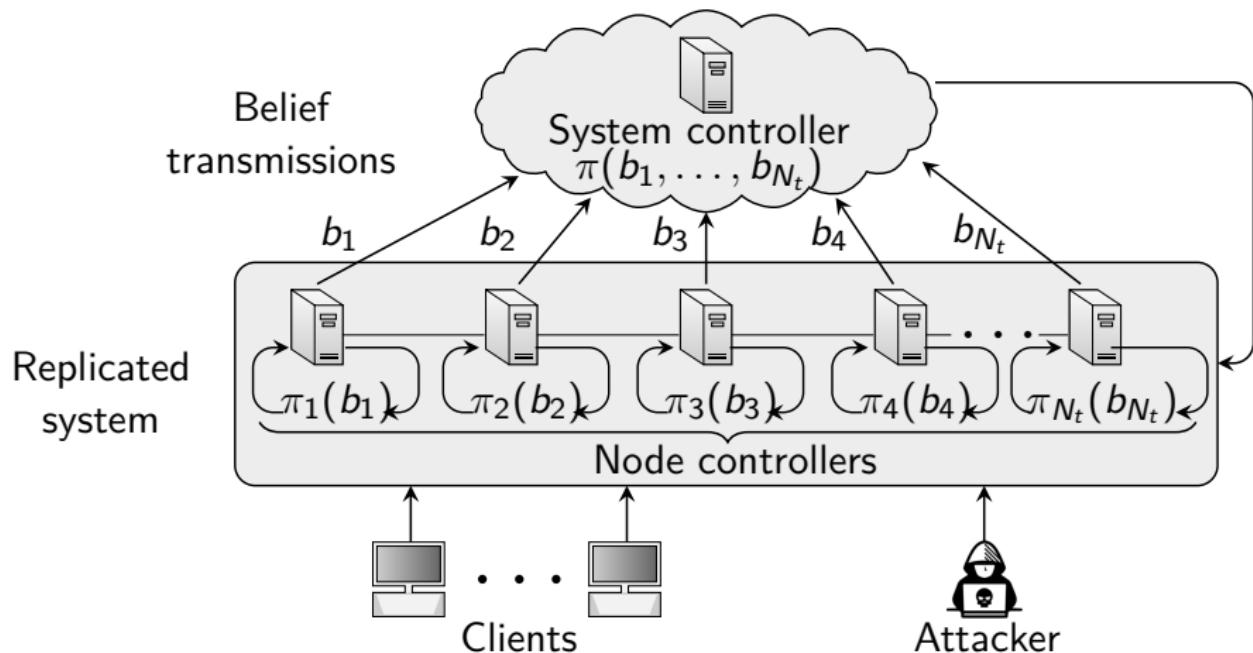
The Benefit of Strategic Recovery



Key insight

Strategic recovery **can significantly reduce operational cost** given that an **intrusion detection model is available**.

Intrusion Tolerance as a Two-Level Game



The Global Replication Game

- ▶ **Constrained stochastic game Γ .**
- ▶ Players: (C)ontroller and (A)ttacker.
- ▶ States: $\mathcal{S}_S = \{0, 1, \dots, s_{\max}\}$, the number of healthy nodes.

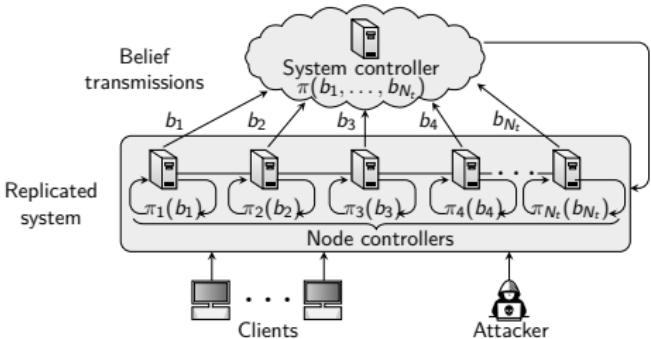
▶ Controller actions: Add $a_t^{(C)} \in \{0, 1\}$ nodes.

▶ Attacker actions: $a_t^{(A)} \in \{F, A\}^{N_t}$.

▶ Markov strategies:

$$\pi^{(C)} : \mathcal{S}_S \rightarrow \Delta(\{0, 1\})$$

$$\pi^{(A)} : \mathcal{S}_S \rightarrow \Delta(\{F, A\}^{N_t}).$$



The Global Replication Game

- ▶ **Constrained stochastic game Γ .**
- ▶ Players: (C)ontroller and (A)ttacker.
- ▶ States: $\mathcal{S}_S = \{0, 1, \dots, s_{\max}\}$, the number of healthy nodes.

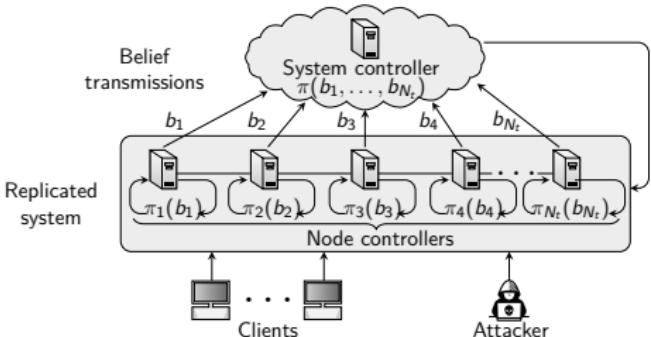
▶ **Controller actions:** Add $a_t^{(C)} \in \{0, 1\}$ nodes.

▶ **Attacker actions:** $\mathbf{a}_t^{(A)} \in \{\mathsf{F}, \mathsf{A}\}^{N_t}$.

▶ Markov strategies:

$$\pi^{(C)} : \mathcal{S}_S \rightarrow \Delta(\{0, 1\})$$

$$\pi^{(A)} : \mathcal{S}_S \rightarrow \Delta(\{\mathsf{F}, \mathsf{A}\}^{N_t}).$$



The Global Replication Game

- ▶ **Constrained stochastic game Γ .**
- ▶ Players: (C)ontroller and (A)ttacker.
- ▶ States: $\mathcal{S}_S = \{0, 1, \dots, s_{\max}\}$, the number of healthy nodes.

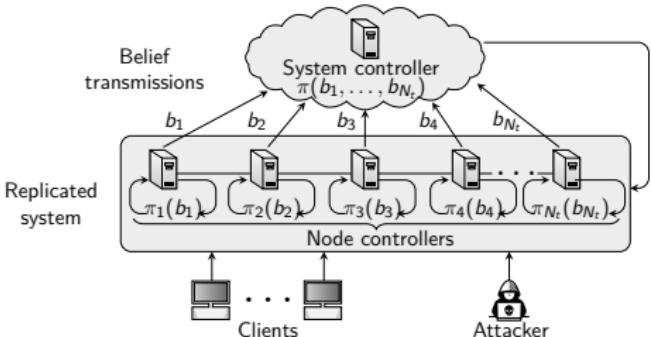
▶ **Controller actions:** Add $a_t^{(C)} \in \{0, 1\}$ nodes.

▶ **Attacker actions:** $\mathbf{a}_t^{(A)} \in \{\mathsf{F}, \mathsf{A}\}^{N_t}$.

▶ **Markov strategies:**

$$\pi^{(C)} : \mathcal{S}_S \rightarrow \Delta(\{0, 1\})$$

$$\pi^{(A)} : \mathcal{S}_S \rightarrow \Delta(\{\mathsf{F}, \mathsf{A}\}^{N_t}).$$



System Controller Objective

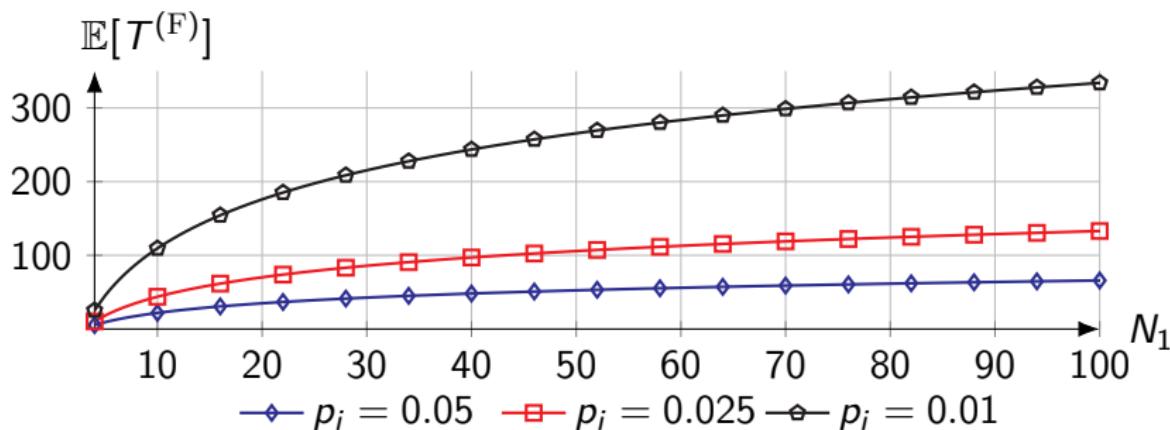
- ▶ **Zero-sum** game.
- ▶ **Cost:** $J \triangleq \lim_{T \rightarrow \infty} \sum_{t=1}^T \frac{a_t^{(C)}}{T}$.
- ▶ **Constraint:** $T^{(A)} \geq \epsilon_A$, where $T^{(A)}$ is the availability.

ϵ_A	<i>Allowed service downtime per year</i>
0.9	36 days
0.95	18 days
0.99	3 days
0.999	8 hours
0.9999	52 minutes
0.99999	5 minutes
1	0 minutes

System Reliability Analysis

- The **Mean-time-to-failure** (MTTF) is the **mean hitting time** of a state where $s_t \leq f$:

$$\mathbb{E}[T^{(F)} | S_1 = s_1] = \mathbb{E}_{(S_t)_{t \geq 1}} \left[\inf \{t \geq 1 | S_t \leq f\} | S_1 = s_1 \right].$$



The MTTF in function of the number of initial nodes N_1 and failure probability per node p_i .

Theorem 5 (Best Response Existence and Computation)

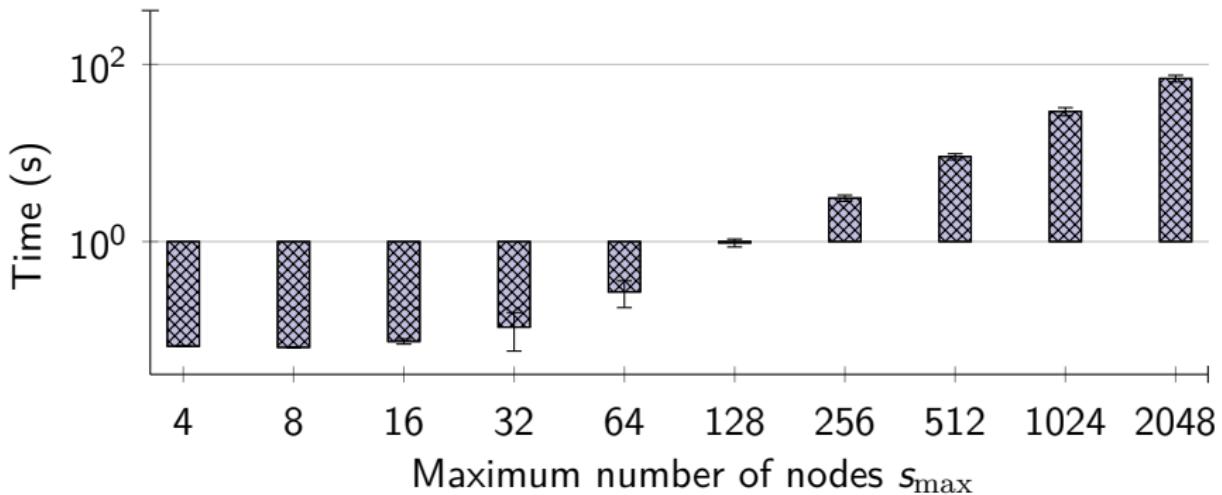
Assuming

- (A) *The Markov chain induced by each strategy pair π is unichain.*
- (B) *The availability constraint is feasible.*

Then the following holds.

1. *For each strategy pair π , there exists a pair of stationary best responses.*
2. *Best responses can be computed by using linear programming.*

Efficient Computation of Best Responses



Mean compute time to obtain a best response in the replication game.

Definition 6 (Markov perfect equilibrium (MPE))

A strategy pair $\pi^* = (\pi^{(C),*}, \pi^{(A),*})$ is a **Markov perfect equilibrium** if each player follows a Markov behavior strategy and π^* is a Nash equilibrium regardless of the initial state.

Theorem 7 (Existence of equilibrium in the global game)

Assuming

- (A) *The Markov chain induced by each strategy pair π is unichain.*
- (B) *The availability constraint is feasible.*

Then the following holds.

1. A constrained, stationary *Markov perfect equilibrium* (MPE) exists.
2. Computing the equilibrium is *PPAD-complete*.

Challenge

Equilibrium computation is intractable in general.

Challenge

Equilibrium computation is intractable in general.

Theorem 8

*Given any attacker strategy, there exists a best response **control strategy that is decreasing in s .***

Efficient Computation of Equilibria

Challenge

Equilibrium computation is intractable in general.

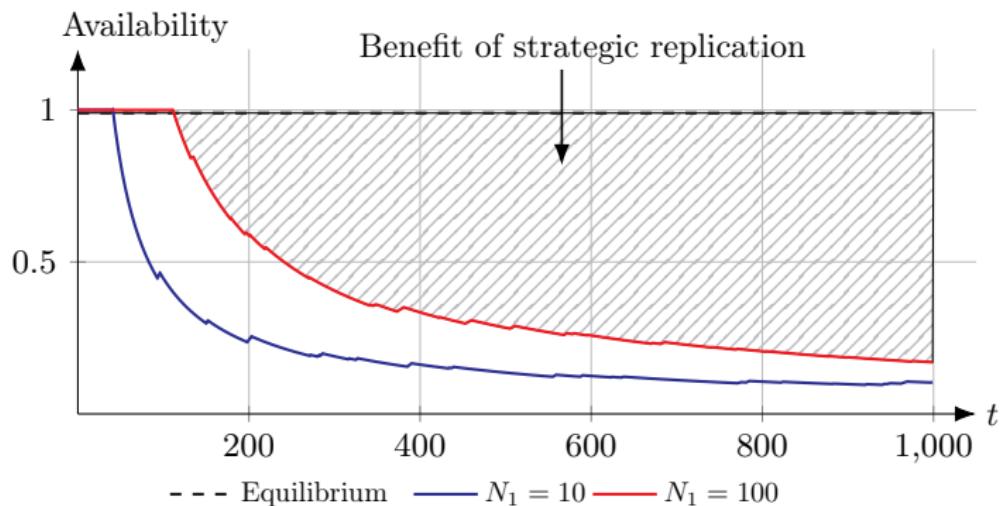
Theorem 9

*Given any attacker strategy, there exists a best response **control strategy that is decreasing in s .***

Corollary 10

Given that the controller strategy is decreasing in s , a weakly dominating strategy for the attacker is to minimize $\mathbb{E}[S]$.

The Benefit of Strategic Replication

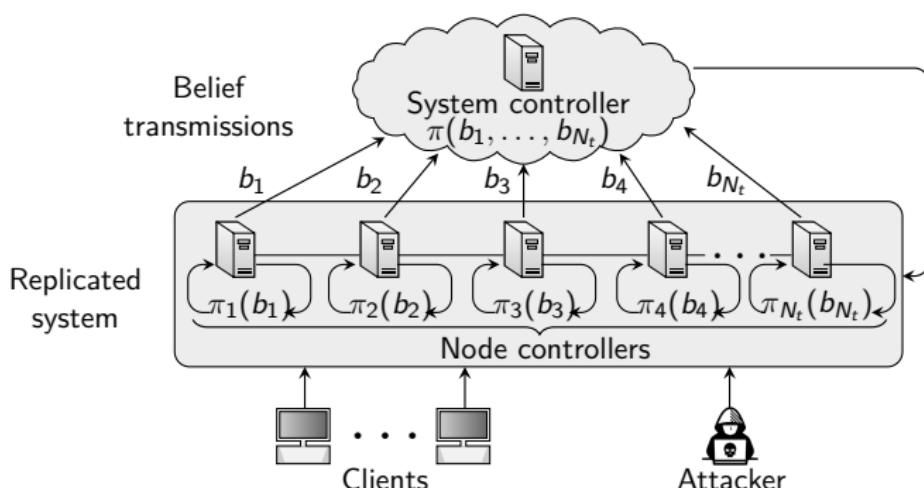


Key insight

Strategic replication can **guarantee a high service availability in expectation**. The **benefit of strategic replication** is mainly prominent for long-running systems.

Summary of the Game-Theoretic Model

- ▶ Partially observed stochastic game models intrusion recovery.
 - ▶ **Threshold structure** of best responses.
 - ▶ Existence of *perfect Bayesian equilibria*.
- ▶ Constrained stochastic game models replication control.
 - ▶ **Threshold structure** of best responses.
 - ▶ Existence of *Markov perfect equilibria*.

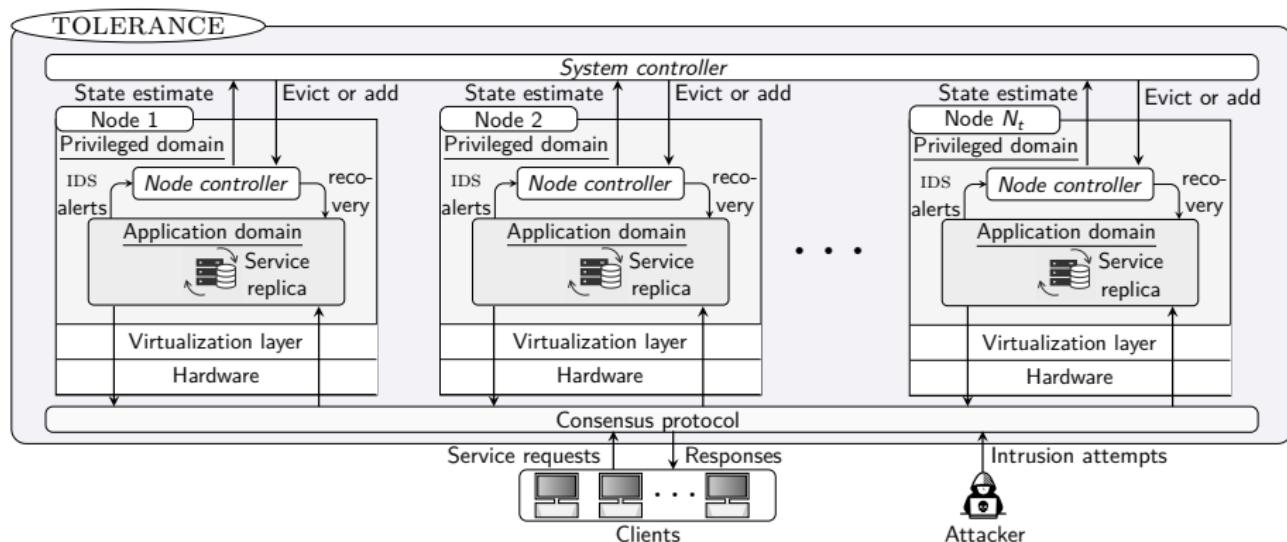


Experiment Setup - Testbed



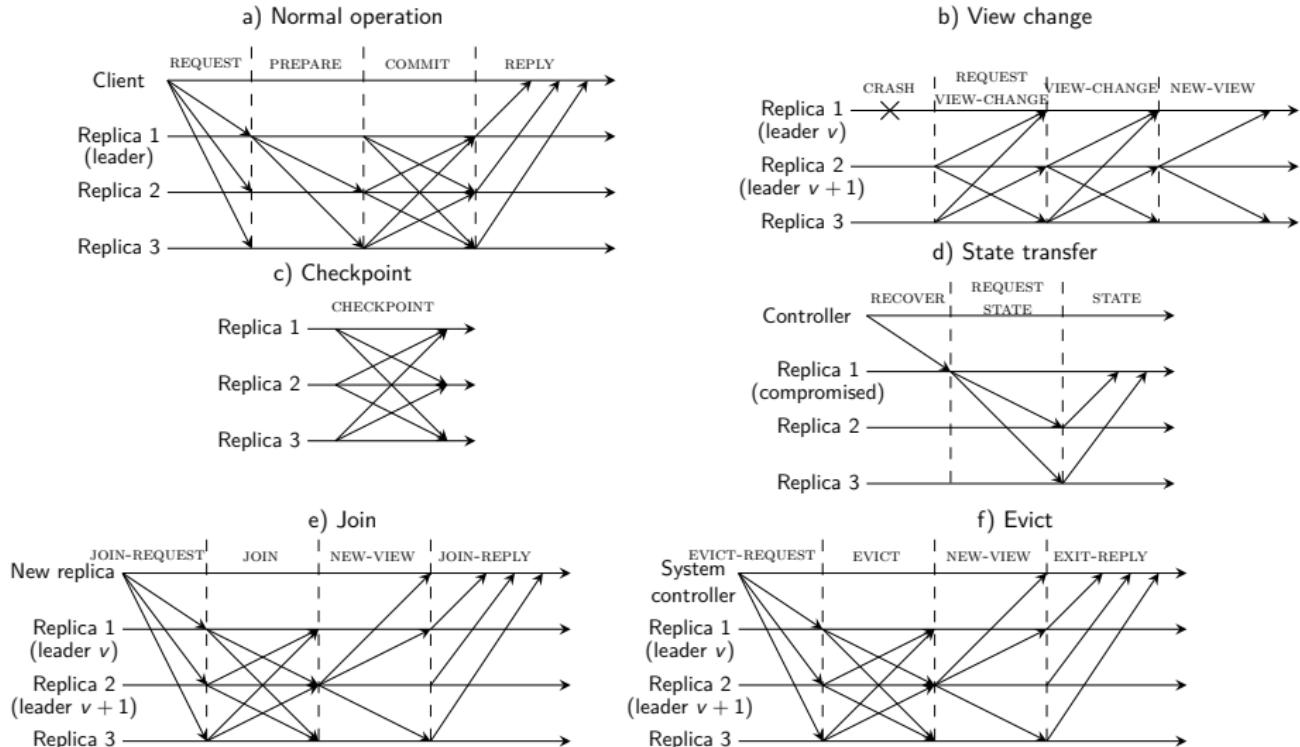
The TOLERANCE Architecture

Two-level recovery and replication control with feedback.

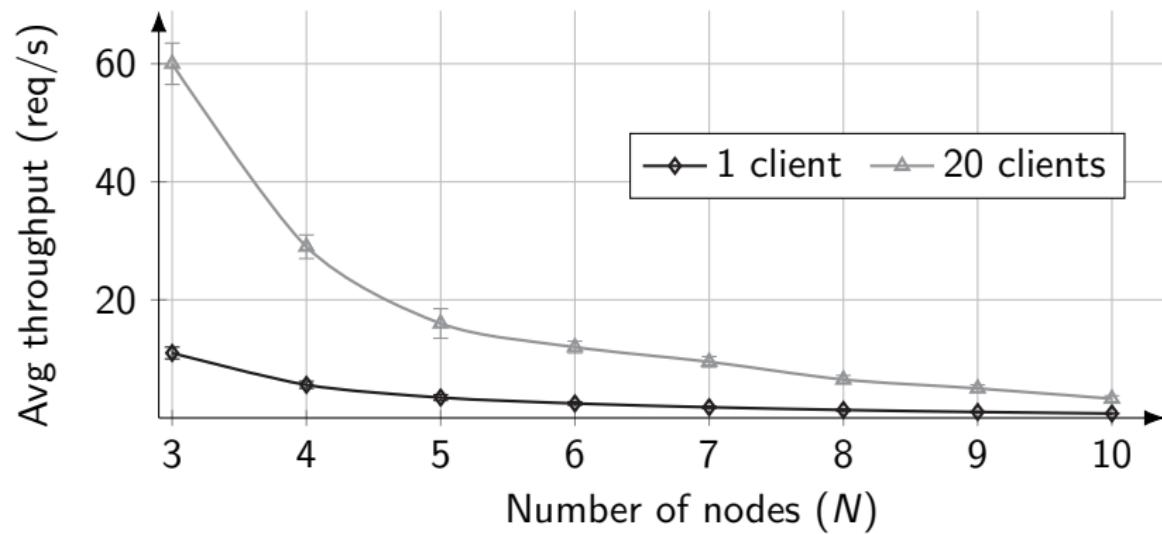


- ▶ A replicated **web service** which offers two operations:
 - ▶ A **read** operation that returns the service state.
 - ▶ A **write** operation that updates the state.

Intrusion-Tolerant Consensus Protocol (MINBFT)



Intrusion-Tolerant Consensus Protocol



Average throughput of our implementation of MINBFT.

Experiment Setup - Emulated Intrusions

<i>Replica ID</i>	<i>Intrusion steps</i>
1	TCP SYN scan, FTP brute force
2	TCP SYN scan, SSH brute force
3	TCP SYN scan, TELNET brute force
4	ICMP scan, exploit of CVE-2017-7494
5	ICMP scan, exploit of CVE-2014-6271
6	ICMP scan, exploit of CWE-89 on DVWA
7	ICMP scan, exploit of CVE-2015-3306
8	ICMP scan, exploit of CVE-2016-10033
9	ICMP scan, SSH brute force, exploit of CVE-2010-0426
10	ICMP scan, SSH brute force, exploit of CVE-2015-5602

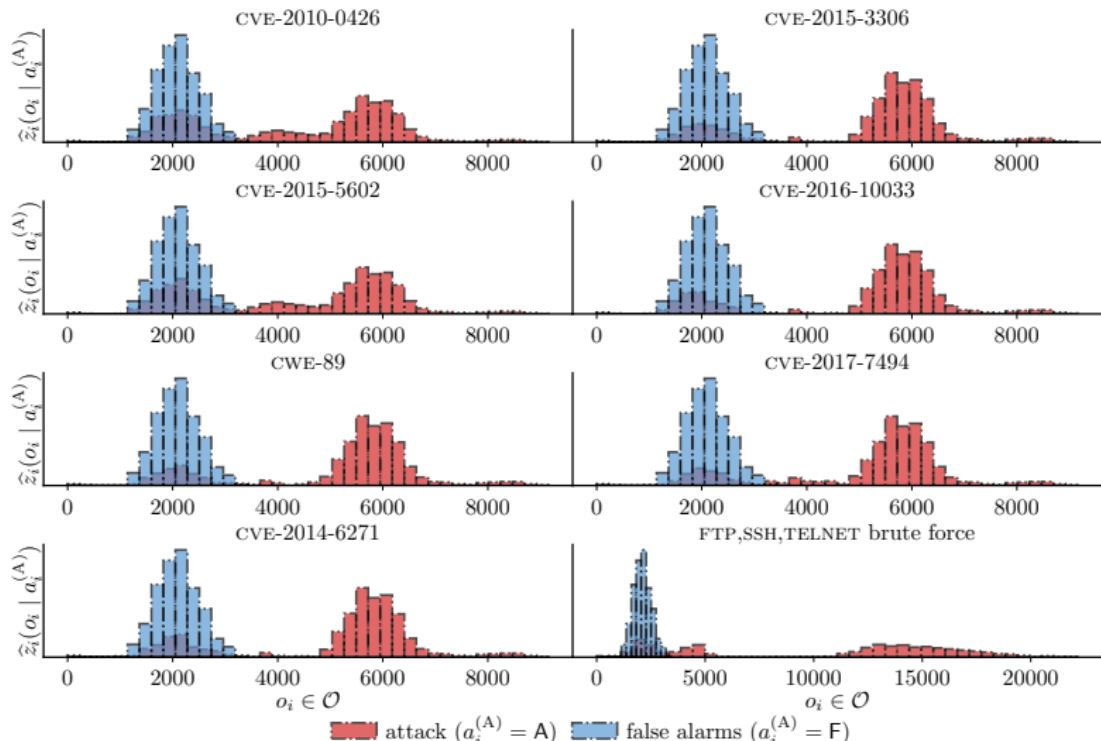
Table 1: Intrusion steps.

Experiment Setup - Background Traffic

<i>Background services</i>	<i>Replica ID(s)</i>
FTP, SSH, MONGODB, HTTP, TEAMSPEAK	1
SSH, DNS, HTTP	2
SSH, TELNET, HTTP	3
SSH, SAMBA, NTP	4
SSH	5, 7, 8, 10
DVWA, IRC, SSH	6
TEAMSPEAK, HTTP, SSH	9

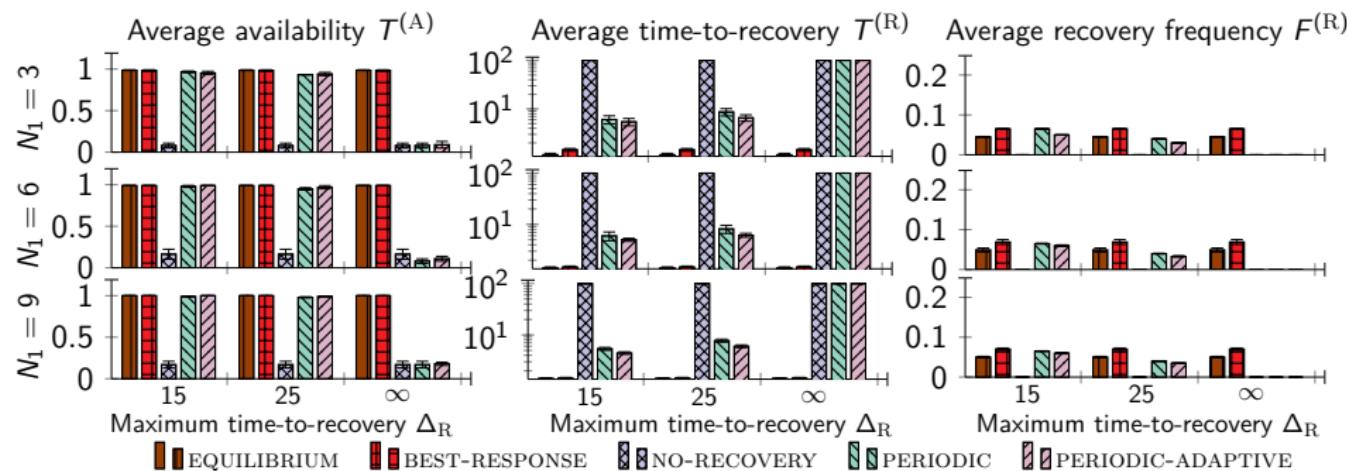
Table 2: Background services.

Estimated Distributions of Intrusion Alerts



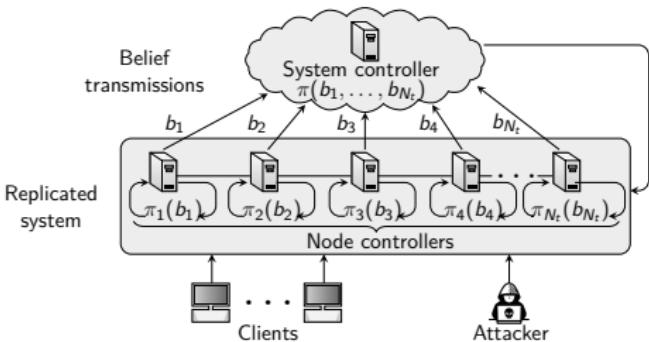
- ▶ We estimate the observation distribution z with the empirical distribution \hat{Z} based on M samples.
- ▶ $\hat{z} \xrightarrow{\text{a.s.}} z$ as $M \rightarrow \infty$ (Glivenko-Cantelli theorem).

Comparison with State-of-the-art Intrusion-Tolerant Systems



Comparison between our game-theoretic control strategies and the baselines; x-axes indicate values of Δ_R ; rows relate to the number of initial nodes N_1 .

Conclusion



- ▶ We present a **game-theoretic model of intrusion tolerance**.
- ▶ We establish **structural results**.
- ▶ We **evaluate the equilibrium strategies on a testbed**.
- ▶ Our game-theoretic strategies have **stronger theoretical guarantees and significantly better practical performance** than the control strategies used in state-of-the-art intrusion-tolerant systems.