

# Intrusion Tolerance as a Two-Level Game

GameSec 2024, New York, USA  
Conference on Decision and Game Theory for Security

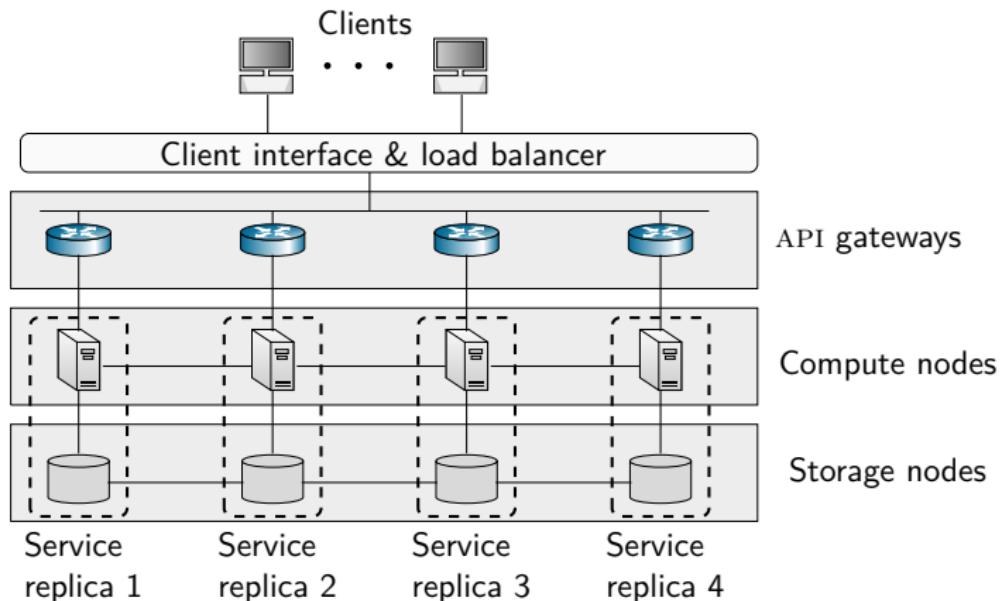
Kim Hammar & Rolf Stadler

*kimham@kth.se*  
KTH Royal Institute of Technology

Oct 16, 2024

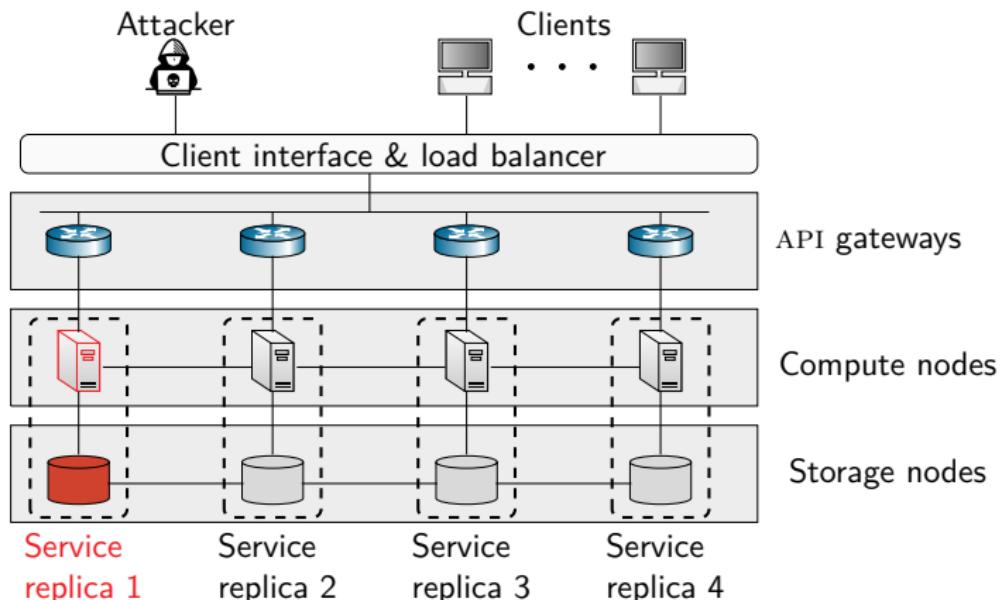


# Use Case: Intrusion Tolerance



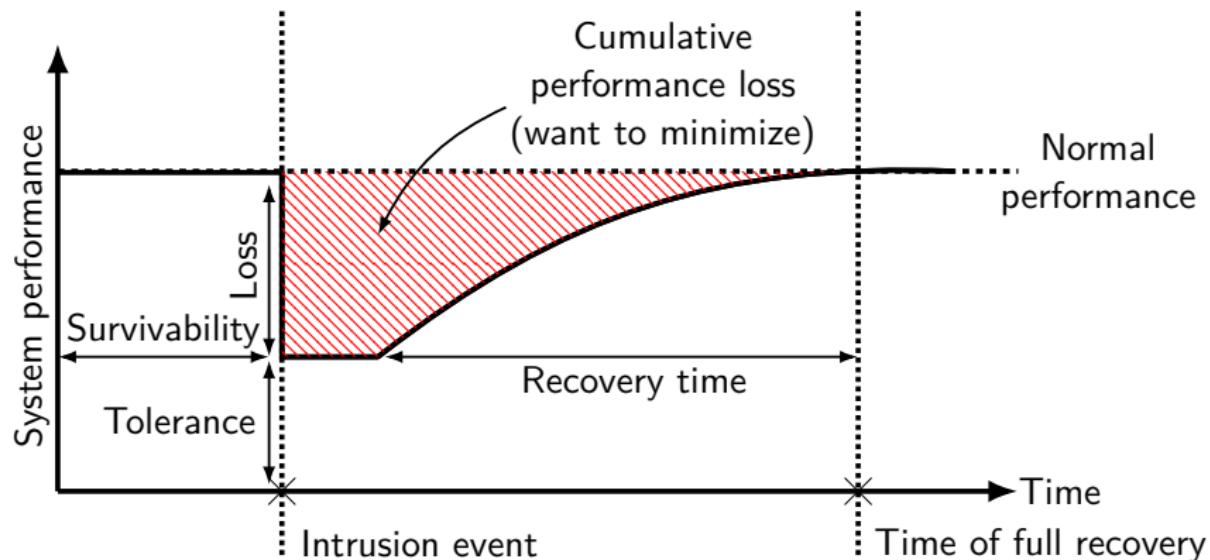
- ▶ A **replicated system** offers a service to a client population.
- ▶ The system should provide **service without disruption**.

# Use Case: Intrusion Tolerance



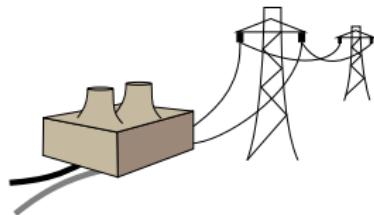
- ▶ An **attacker** seeks to intrude on the system and disrupt service.
- ▶ The system should **tolerate intrusions**.

# Intrusion Tolerance (Simplified)



# Increasing Demand for Intrusion-Tolerant Systems

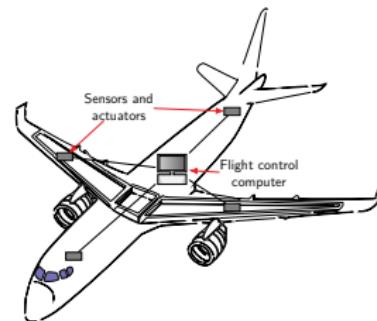
- ▶ As our **reliance on online services grows**, there is an increasing demand for intrusion-tolerant systems.
- ▶ Example applications:



**Power grids**  
e.g., SCADA systems<sup>1</sup>.



**Safety-critical IT systems**  
e.g., banking systems,  
e-commerce applications<sup>2</sup>,  
healthcare systems, etc.



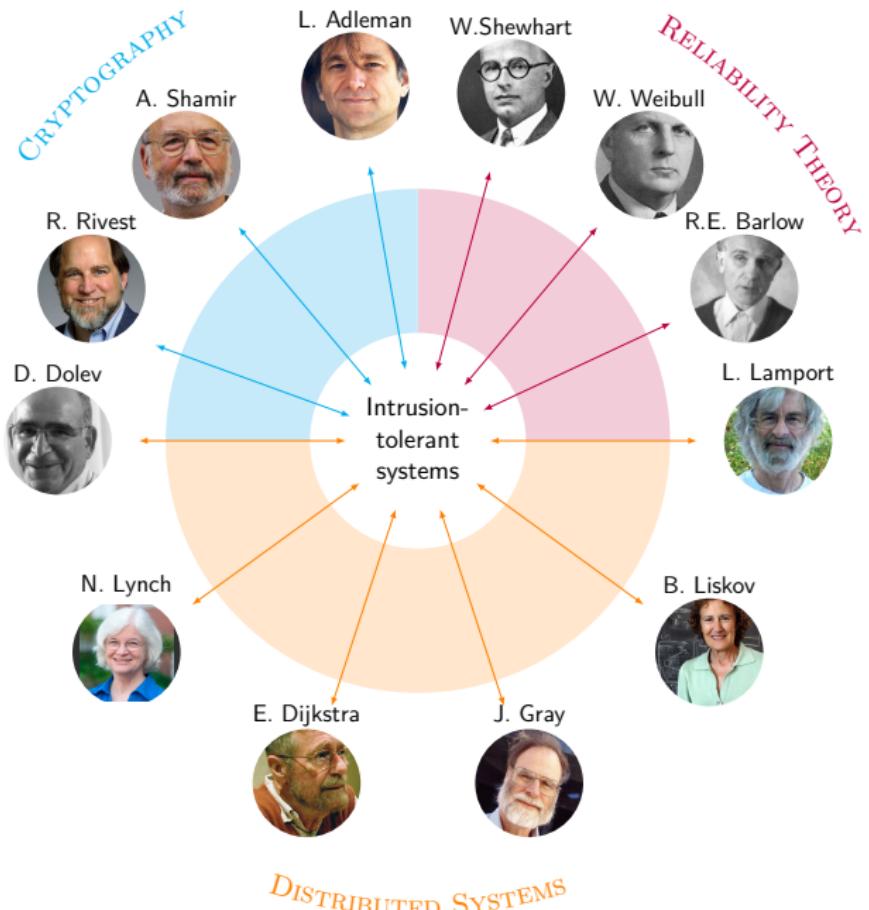
**Real-time control systems**  
e.g., flight control computer<sup>3</sup>.

<sup>1</sup>Amy 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).

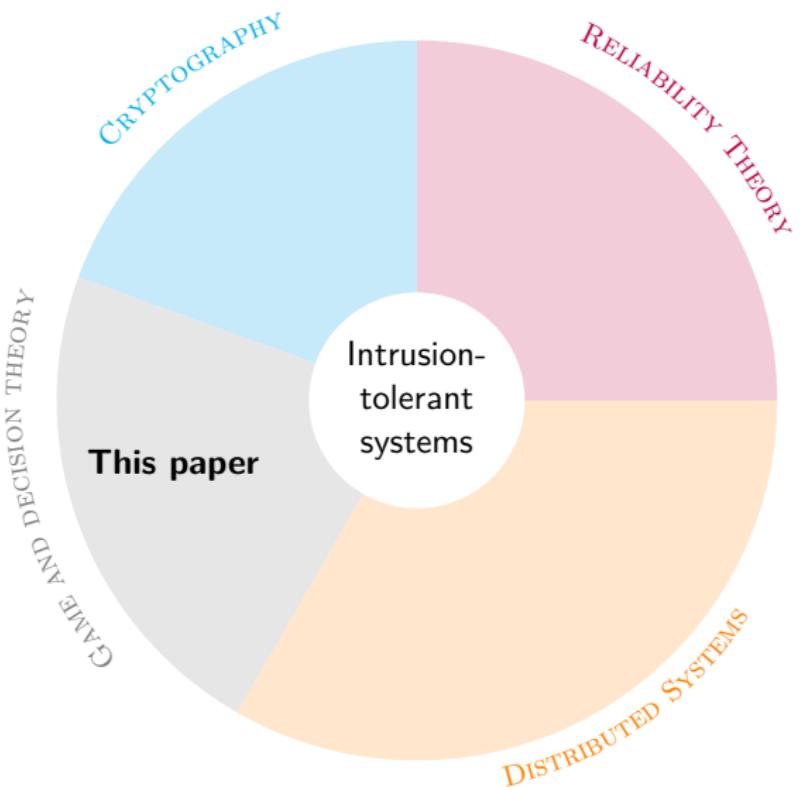
<sup>2</sup>Jukka Soikkeli et al. "Redundancy Planning for Cost Efficient Resilience to Cyber Attacks". In: *IEEE Transactions on Dependable and Secure Computing* 20.2 (2023), pp. 1154–1168. DOI: [10.1109/TDSC.2022.3151462](https://doi.org/10.1109/TDSC.2022.3151462).

<sup>3</sup>J.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).

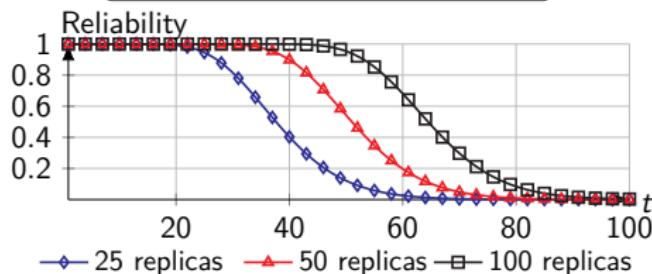
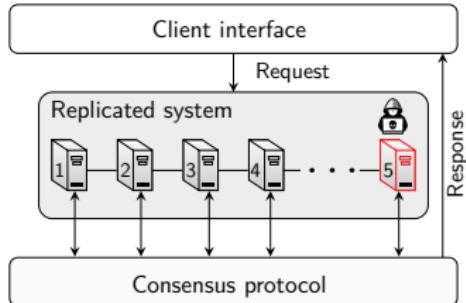
# Theoretical Foundations of Intrusion Tolerance



# Our Contribution



# Building Blocks of An Intrusion-Tolerant System

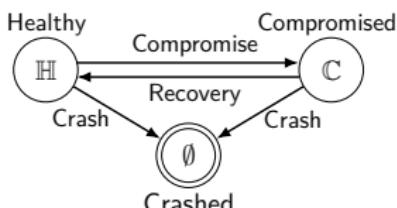


## 1. Intrusion-tolerant consensus protocol

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](mailto: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 several basic protocols that solve several basic problems in distributed systems, including asynchronous group membership, reliable broadcast, consensus (e.g., leader election and 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  
reiter@research.att.com

**Abstract:** Rampart is a toolkit of protocols to facilitate the development of high-integrity services, i.e., distributed services that retain their availability and correctness despite the malicious prorogation of some component servers by an attacker. At the core of Rampart are new protocols that solve several basic problems in distributed computing, including asynchronous group membership, reliable multicast (Byzantine errors), and leader election. Using these primitives, Rampart supports the development of high-integrity services via the technique of state machine replication, and also extends the 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.

## 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 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

systems  
and  
inter-  
process  
con-  
nectiv-  
ity  
and  
reliabil-  
ity  
and  
perfor-  
mance  
and  
cost  
and  
energy  
and  
etc.

# 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](mailto: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](mailto:kimk@alpha.ece.ucsb.edu), [moser@ece.ucsb.edu](mailto:moser@ece.ucsb.edu), [pmms@ece.ucsb.edu](mailto: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 ensure 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](mailto: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](mailto:kimk@csba.ece.acsl.edu), [moser@ece.acsl.edu](mailto:moser@ece.acsl.edu), [pmms@ece.acsl.edu](mailto: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 reliability 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 Welch<sup>1</sup>, 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](mailto:{R.J.Stroud,J.P.Warne,Peter.Ryan}@ncl.ac.uk)  
[Ian.Welch@mcs.vt.edu](mailto: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 Kihlstrom, 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 use 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 Welch<sup>1</sup>, 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<sup>1,\*</sup> and Paul Rubel<sup>1</sup>, Michael Atighetchi<sup>1</sup>, Franklin Webber<sup>1</sup>, William H. Sanders<sup>2</sup>, Mouna Seri<sup>2</sup>, HariGovind Ramasamy<sup>3</sup>, James Lyons<sup>2</sup>, Tod Courtney<sup>3</sup>, Adnan Agbaria<sup>2</sup>, Michel Cukier<sup>3</sup>, Jeanna Gossett<sup>4</sup>, Idit Keidar<sup>5</sup>

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

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

<sup>3</sup> University of Maryland at College Park, Maryland. mckukier@eng.umd.edu <sup>4</sup> The Boeing Company. jeanna.m.gossett@boeing.com <sup>5</sup> 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 consistent 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 Welch<sup>1</sup>, 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 make 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 traffic

## An architecture for adaptive intrusion-tolerant applications

Partha Pal<sup>1,\*</sup> and Paul Ruhel<sup>1</sup>, Michael Atighetchi<sup>1</sup>, Franklin Webber<sup>1</sup>, William H. Sanders<sup>2</sup>, Monia Seri<sup>2</sup>, HarGovind Ramasamy<sup>3</sup>, James Lyons<sup>2</sup>, Tod Courtney<sup>4</sup>, Adnan Agbaria<sup>5</sup>, Michel Cukier<sup>6</sup>, Joanna Gossett<sup>7</sup>, Ilti Keldar<sup>8</sup>

<sup>1</sup> IBM Technologies, Cambridge, Massachusetts. {pal, pruhel, maitigh, fwebber}@ibm.com

<sup>2</sup> University of Illinois at Urbana-Champaign. {wbs, seri, rama, jlyons, tod}

<sup>3</sup> University of Maryland at College Park, Maryland. ramsay@cs.umd.edu

<sup>4</sup> The Boeing Company. jocca.m.gossett@MW.Boeing.com

<sup>5</sup> Department of Electrical Engineering, Technion - Israel Institute of Technology. adnan@ee.technion.ac.il

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

Miguel Correia <sup>a,\*</sup>, Nuno Ferreira Neves <sup>a</sup>, Lau Cheuk Lung <sup>b</sup>, Paulo Veríssimo <sup>a</sup>

<sup>a</sup> Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C6, Piso 3, 1749-016 Lisboa, Portugal  
<sup>b</sup> Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica de São Paulo, São Paulo, São Paulo, Brazil, 01322-000

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 Welch<sup>1</sup>, 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 <sup>a,\*</sup>, Nuno Ferreira Neves <sup>a</sup>, Lau Cheuk Lung <sup>b</sup>, Paulo Veríssimo <sup>a</sup>

<sup>a</sup> Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Edifício C8, Piso 3, 1749-002 Lisboa, Portugal  
<sup>b</sup> 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<sup>1,2</sup> and Paul Rubel<sup>1</sup>, Michael Atighechi<sup>1</sup>, Franklin Webber<sup>1</sup>, William H. Sanders<sup>2</sup>, Monna Serf<sup>2</sup>, HarGovind Ramaswamy<sup>3</sup>, James Lyons<sup>2</sup>, Tod Courtney<sup>4</sup>, Adina Aguirre<sup>5</sup>, Michel Culier<sup>6</sup>, Jerome Gosset<sup>4</sup>, Idit Keidar<sup>3</sup>

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

<sup>2</sup> University of Illinois at Urbana-Champaign, {whs, serf, ramsawy, jlyons, tod, gosset}@illinois.edu

<sup>3</sup> University of Maryland at College Park, Maryland, mculier@engr.umd.edu<sup>4</sup> The Boeing Company, jessica.o.gosset@FW Boeing.com<sup>5</sup> 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 Welsh<sup>1</sup>, 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@nucs.vuw.ac.nz

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

Miguel Correia <sup>a,\*</sup>, Nuno Ferreira Neves <sup>b</sup>, Lau Cheuk Lung <sup>b</sup>, Paulo Veríssimo <sup>a</sup>

<sup>a</sup> Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Piso 3, 1749-002 Lisboa, Portugal  
<sup>b</sup> 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<sup>1,\*</sup> and Paul Rubel<sup>1</sup>, Michael Atighetechi<sup>1</sup>, Franklin Webber<sup>1</sup>, William H. Sanders<sup>2</sup>, Monna Serf<sup>2</sup>, HarGovind Ramaswamy<sup>3</sup>, James Lyons<sup>2</sup>, Tod Courtney<sup>4</sup>, Adina Agustini<sup>5</sup>, Michel Calher<sup>5</sup>, Jerome Gossett<sup>4</sup>, Idit Keidar<sup>5</sup>

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

<sup>2</sup> University of Illinois at Urbana-Champaign, {whs, serf, ramasy, jlyons, tod}

gabson}@illinois.edu

<sup>3</sup> University of Maryland College Park, Maryland, rams@engr.umd.edu<sup>4</sup> The Boeing

Company, jlyons.o.gov@boeing.com<sup>5</sup> Department of Electrical Engineering,

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

## Resilient Intrusion Tolerance through Proactive and Reactive Recovery<sup>\*</sup>

Paulo Sousa Alysson Neves Bessani Miguel Correia  
Nuno Ferreira Neves Paulo Veríssimo  
LASIGE, Faculdade de Ciências da Universidade de Lisboa – Portugal  
[pjousa, 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. Johnson et al. [1997] discuss the problem of a group member failing to affect 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 mail (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 Welch<sup>1</sup>, 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 <sup>a,\*</sup>, Nuno Ferreira Neves <sup>a</sup>, Lau Cheuk Lung <sup>b</sup>, Paulo Verissimo <sup>a</sup>

<sup>a</sup> Faculdade de Ciéncias da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Piso 3, 1749-016 Lisboa, Portugal  
<sup>b</sup> Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rue Imaculada 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<sup>1,\*</sup> and Paul Rubeil<sup>1</sup>, Michael Atighetchi<sup>1</sup>,  
William H. Sanders<sup>2</sup>, Mouna Seri<sup>2</sup>, HarGovardhan Ram<sup>2</sup>,  
Tod Courtney<sup>3</sup>, Adnan Agbaria<sup>3</sup>, Michel Cukier<sup>3</sup>, Jos<sup>3</sup>  
Tobias Distler<sup>4</sup>, Rüdiger Kapitz<sup>4</sup>  
<sup>1</sup> BBN Technologies, Cambridge, Massachusetts, {ppal, grubel, mihai, wshs, tsdistler, rkapitz}@bbn.com  
<sup>2</sup> University of Illinois at Urbana-Champaign, {ws, seri, mouna}@uiuc.edu  
<sup>3</sup> University of Maryland at College Park, Maryland, mca@cs.umd.edu  
<sup>4</sup> Computer Science, mca@cs.umd.edu, Boeing com, Department of Electrical Engineering,  
Institute of Technology, rkapitz@boeing.com

## 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<sup>a</sup> Alysson Neves Bessani<sup>a</sup> Miguel Correia<sup>a</sup>  
Nuno Ferreira Neves<sup>a</sup> Paulo Verissimo<sup>a</sup>  
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

Amir Babay<sup>a</sup>, Thomas Tantillo<sup>a</sup>, 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 Kuhlstrom<sup>1</sup>, L. E. Moser<sup>2</sup>, P. M. Melliar-Smith<sup>3</sup>  
<sup>1</sup> Department of Electrical and Computer Engineering  
<sup>2</sup> 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 of normal (fault-free) operation a

## 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 Welch<sup>1</sup>, 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 <sup>a,\*</sup>, Nuno Ferreira Neves <sup>a</sup>, Lau Cheuk Lung <sup>b</sup>, Paulo Veríssimo <sup>a</sup>

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

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

## An architecture for adaptive intrusion-tolerant applications

Partha Pal<sup>1,\*</sup> and Paul Rubel<sup>2</sup>, Michael Atighechi<sup>3</sup>,  
William H. Sanders<sup>2</sup>, Monna Seri<sup>2</sup>, Hartmut Raun  
Tom Courtney<sup>4</sup>, Adnan Agbaria<sup>5</sup>, Michel Olsker<sup>5</sup>, Joe

<sup>1</sup> BBN Technologies, Cambridge, Massachusetts [ppal, prbel],  
University of Illinois at Urbana-Champaign [mhs, seri, vers],  
<sup>2</sup> University of Maryland at College Park, Maryland, *westover*,  
Computer Systems, jessas@cs.umd.edu, <sup>3</sup> Boring.com [michael],  
Technion Israel Institute of Technology, molsker@tx.technion.ac.il

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

Tobias Distler <sup>1</sup> Rüdiger Kapitzka <sup>1</sup>

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

Hans P. Reiser

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

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

Aug Baker<sup>1</sup>, Thomas Baetke<sup>2</sup>, Trevor Attie, Martin Platzer, and Yair Arad  
<sup>1</sup> John Hopkins University — {dbak, tsbaetke, tattie, yarad}@cs.jhu.edu  
<sup>2</sup> AT&T Labs — {platzer}@research.att.com

Special Concepts LLC — {yacov} @specialconcepts.com

## Resilient Intrusion Tolerance through Proactive a

Pando Souza <sup>1</sup> Alysson Neves Bassani <sup>1</sup> Mig  
Nuno Ferreira Neves <sup>1</sup> Paulo Veríssimo <sup>1</sup>  
LASIGE, Faculdade de Ciéncias da Universidade de Lisboa — eunimept  
{{pjoussa, bassani, npr, 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 Paliogianni<sup>1</sup> and Paul Bubel<sup>2</sup>, Michael Albrecht<sup>2</sup>,  
William H. Sanders<sup>2</sup>, Monica Sey<sup>3</sup>, Hartmut Klaue<sup>3</sup>,  
Tom Courtney<sup>3</sup>, Adams Agius<sup>3</sup>, Miguel Cukier<sup>3</sup>, Jon

<sup>1</sup> IBM Technologies, Cambridge, Massachusetts, 01990, USA  
<sup>2</sup> University of Illinois at Urbana-Champaign, Dept. of Computer Science, Urbana, IL 61801, USA  
<sup>3</sup> University of Maryland at College Park, Department of Electrical and Computer Engineering, 3401 Computer and Space Sciences Bldg., College Park, MD 20742, USA

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

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

## Resilient Intrusion Tolerance through Proactive a

Paulo Sousa<sup>1</sup> Alysson Neves Bessani<sup>2</sup> Mig  
Nuno Ferreira Neves<sup>3</sup> Paulo Veríssimo<sup>4</sup>  
LASIGE, Faculdade de Ciências da Universidade de Lisboa - e-mail:  
psousa, bessani, npe, nuno, pver@di.fc.ul.pt

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

Amy Balmer<sup>1</sup>, Thomas Taft<sup>1</sup>, Trevor Arai, Mario Palusz, and Yair Arad  
Johns Hopkins University — {dtm, mtpal, tara, yair}@cs.jhu.edu  
Special Committee LLC — {trevor}@mathematicalgroup.com

## Can we do better by leveraging game-theoretic strategies?

### A Quantitative Analysis of the Intrusion-Tolerance Capabilities of the MFTAIA Architecture

Robert Stroud, Ian Welch<sup>1</sup>, 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

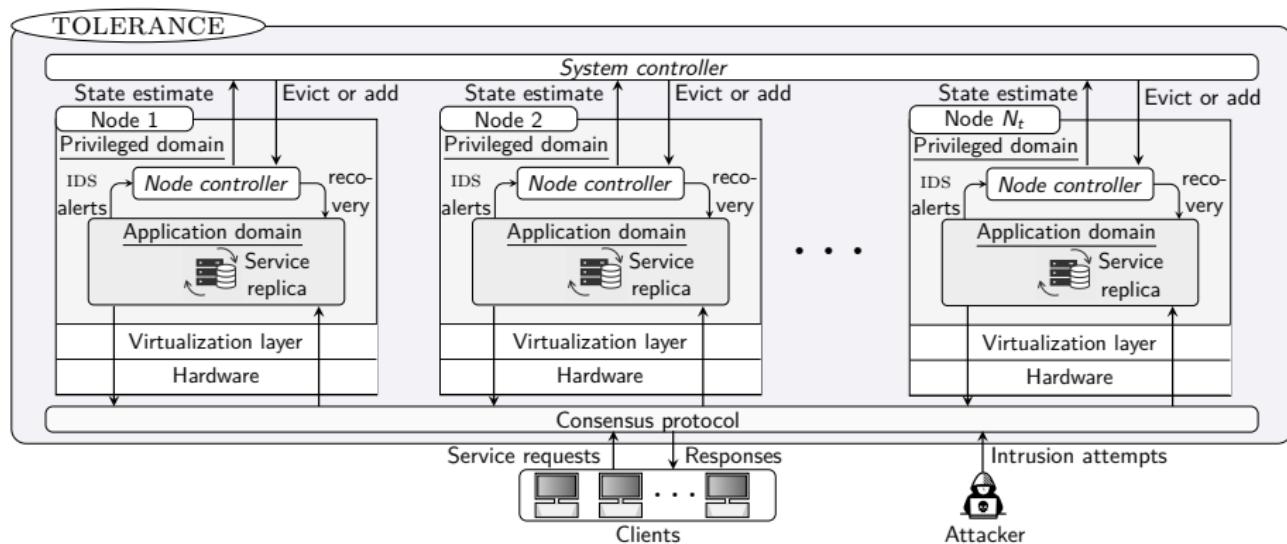
Miguel Correia<sup>3,4</sup>, Nuno Ferreira Neves<sup>3</sup>, Lau Cheuk Lung<sup>3</sup>, Paulo Veríssimo<sup>3,4</sup>  
<sup>3</sup> Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Edifício C1, Piso 3, 1749-001 Lisboa, Portugal  
<sup>4</sup> Programa de 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*

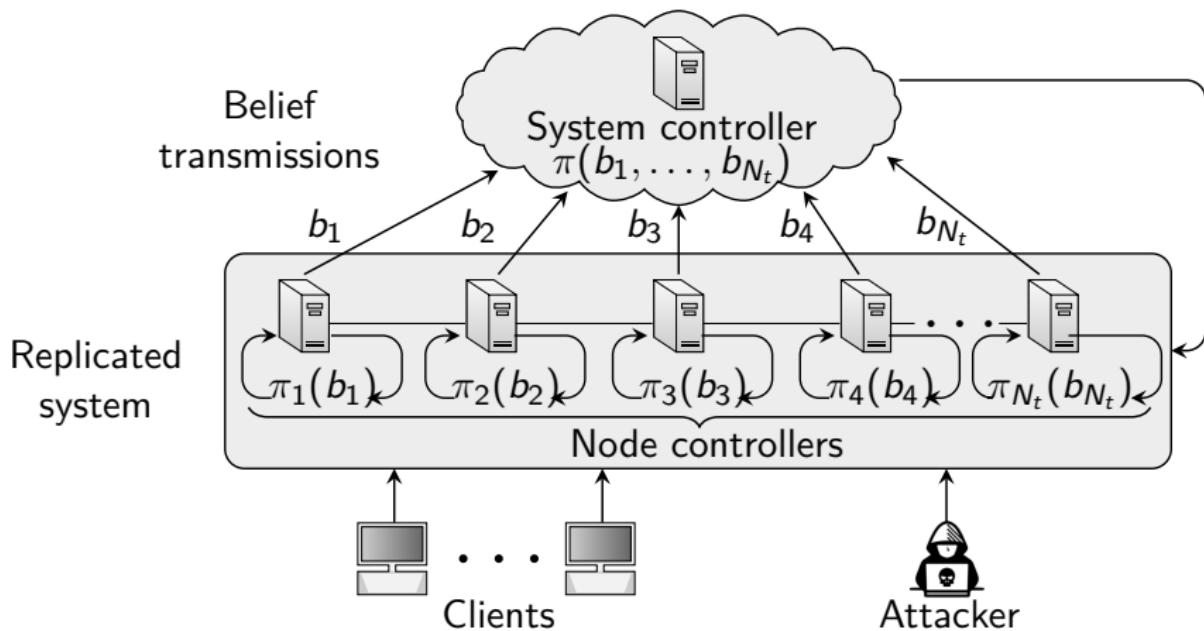
*Network links are authenticated.*

*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



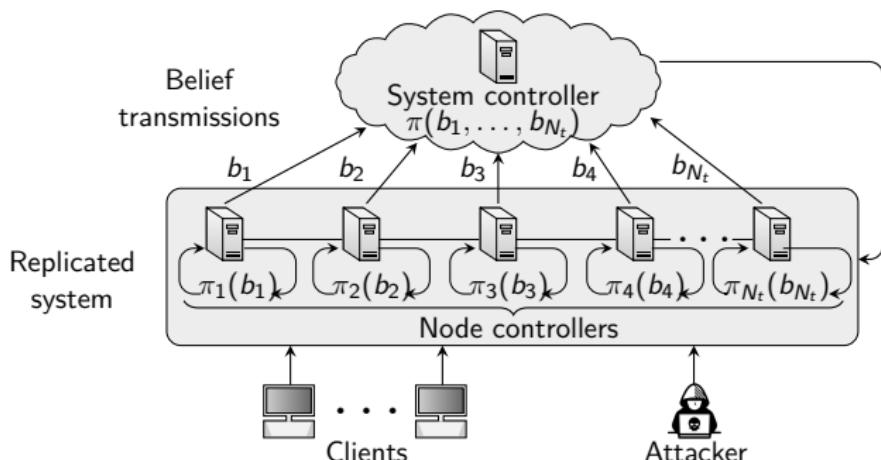
- ▶ We formulate intrusion tolerance as a two-level game.
- ▶ The **local game models intrusion recovery**.
- ▶ The **global game models replication control**.

## Assumption 1

*The probability that the system controller fails is negligible.*

## Assumption 2

*Compromise and crash events are statistically independent across nodes.*

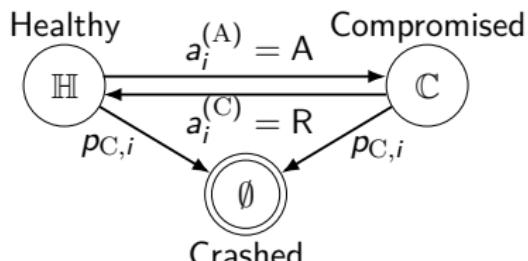


# The Local Recovery Game

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

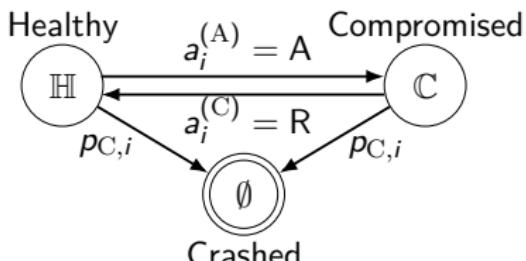
- ▶ Controller actions: (R)ecover and (W)ait.
- ▶ Attacker actions: (A)ttack and (F)alse alarm.

- ▶ 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  $t$ .

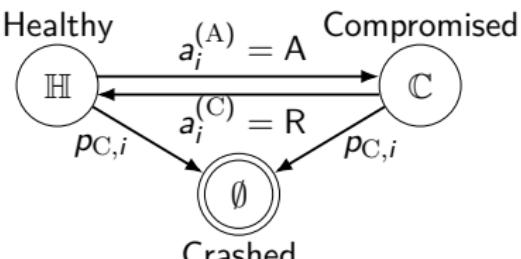


# The Local Recovery Game

- ▶ Partially observed stochastic game  $\Gamma_i$ .
- ▶ 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**  $\Gamma_i$ .
- ▶ 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

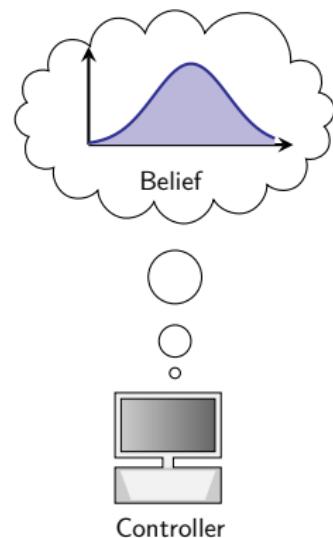
- ▶ The controller computes the **belief**

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

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

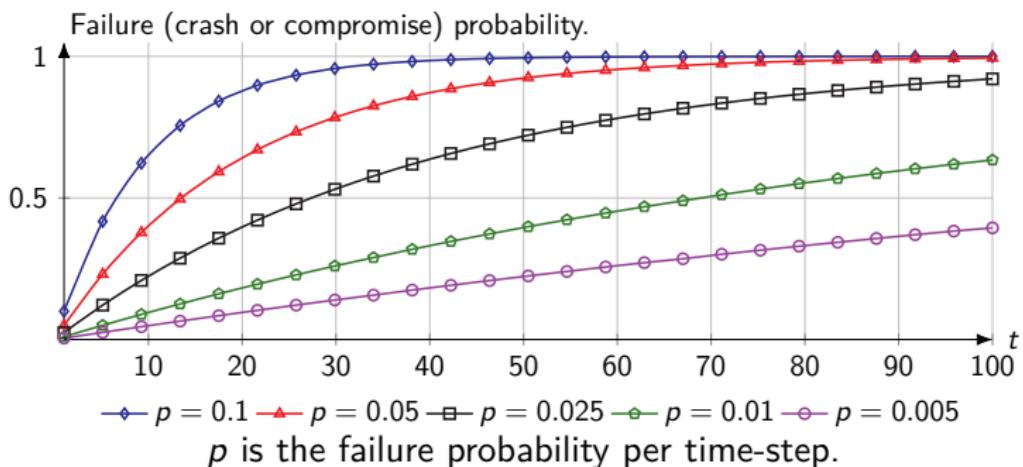
- ▶ Controller strategy:

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

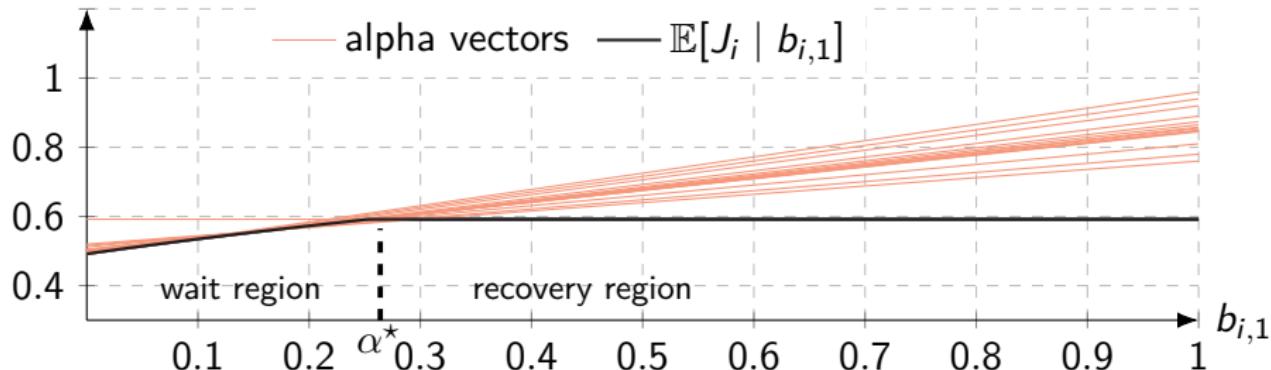


# Node Controller Objective

- ▶ **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  $\Delta_R$ .



# 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

---

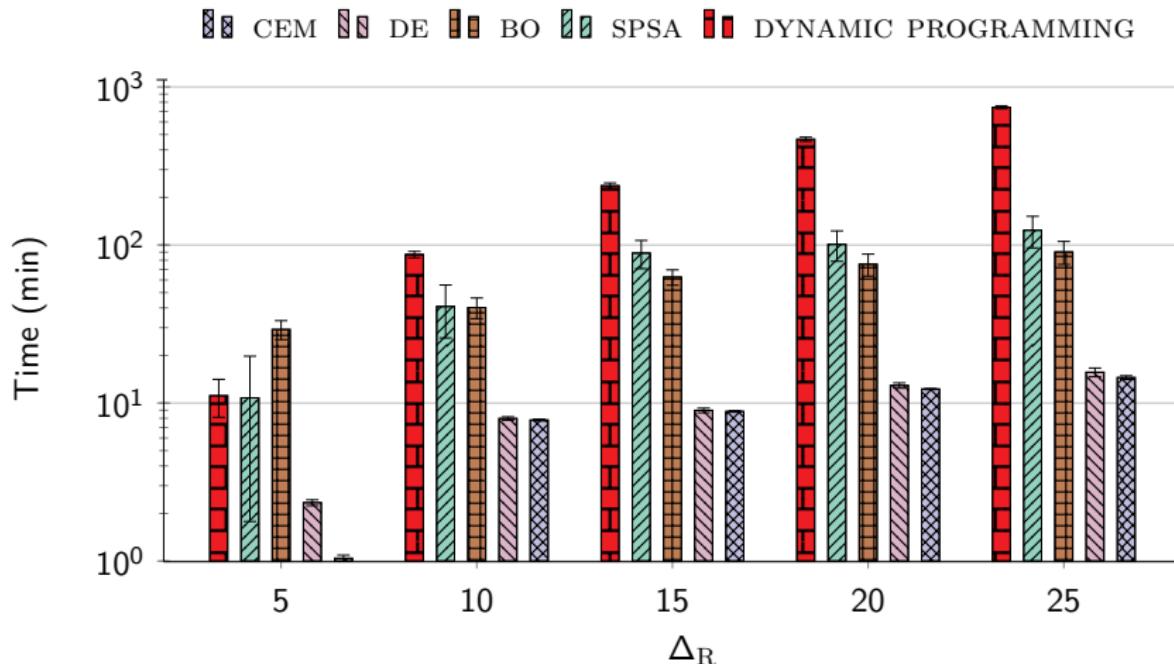
- 1 **Input:** Objective function  $J_i$ , parametric optimizer  $\text{po}$ .
- 2 **Output:** A approximate best response strategy  $\hat{\pi}_{i,\theta}^{(C)}$ .

### 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  $\Delta_R$ .

## Definition 3 (Perfect Bayesian equilibrium (PBE))

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

### 1. Optimality:

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

### 2. Belief consistency:

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

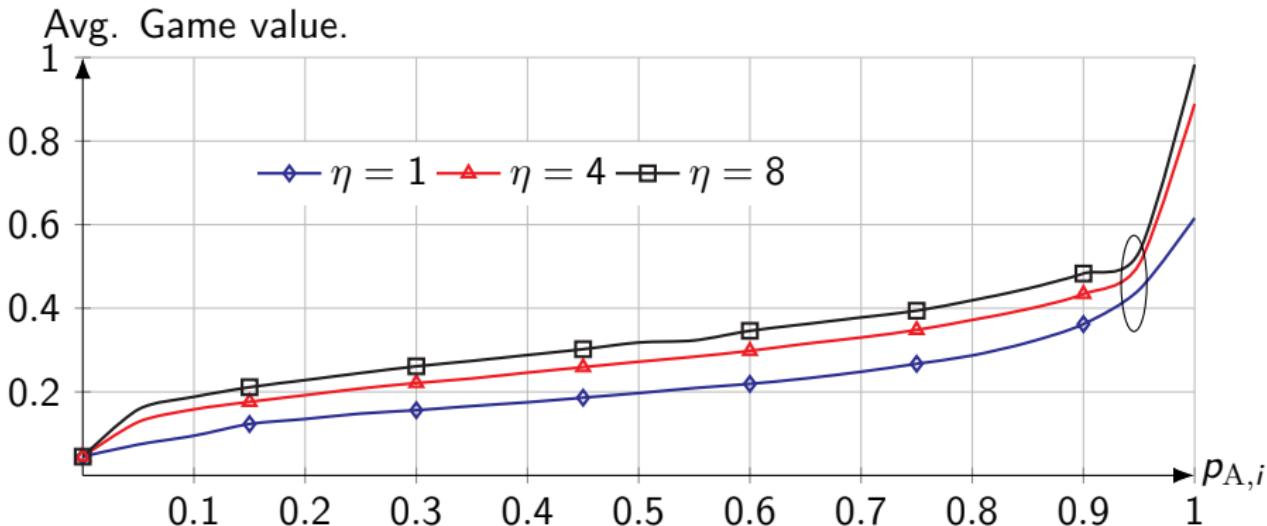
$$\mathbb{B}(\mathbf{h}_{i,t}, \pi_{i,t}^{*,(A)})$$

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

## Theorem 4 (Existence of equilibrium and best response)

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

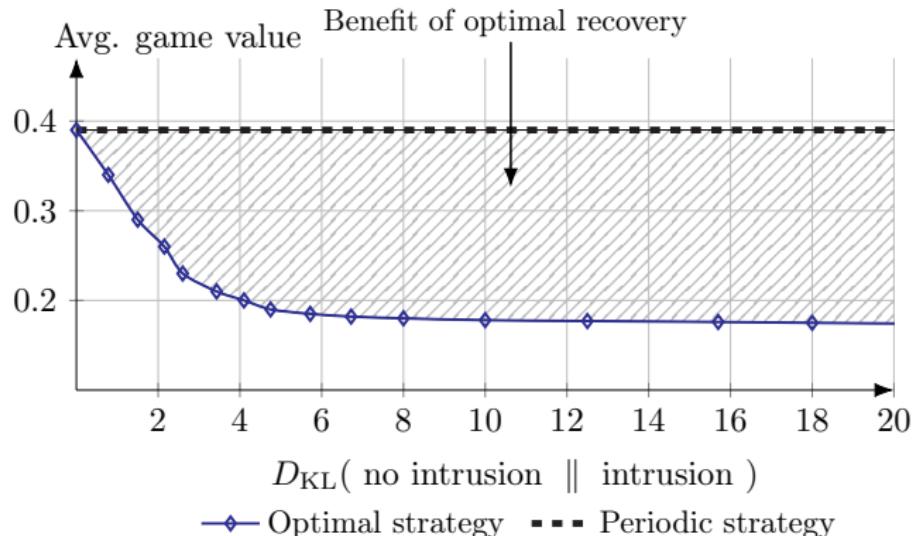
## Value of the Local Recovery Game



Avg. Game value in function of the intrusion probability  $p_{A,i}$ .

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

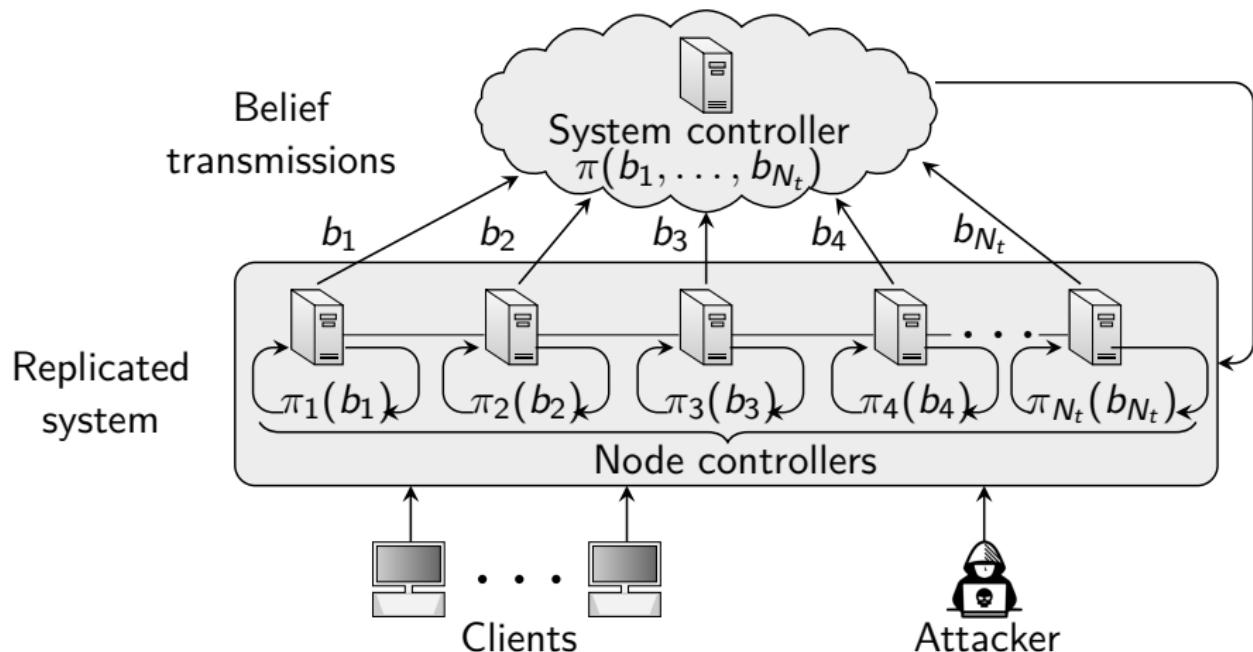
# The Benefit of Strategic Recovery



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

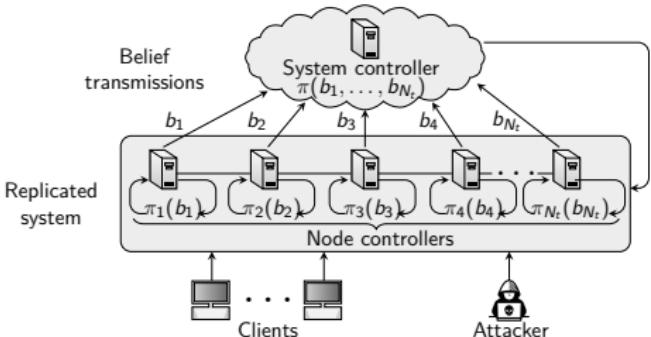
▶ Controller actions: Add  $a_t^{(C)} \in \{0, 1\}$  nodes.

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

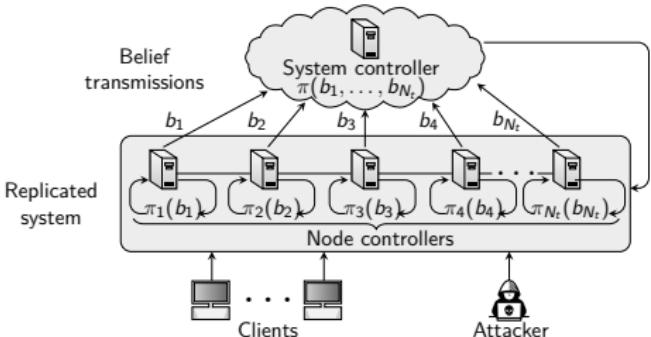
▶ **Controller actions:** Add  $a_t^{(C)} \in \{0, 1\}$  nodes.

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

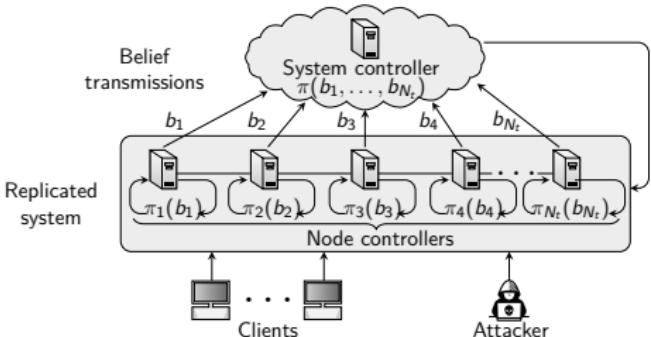
▶ **Controller actions:** Add  $a_t^{(C)} \in \{0, 1\}$  nodes.

▶ **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.

---

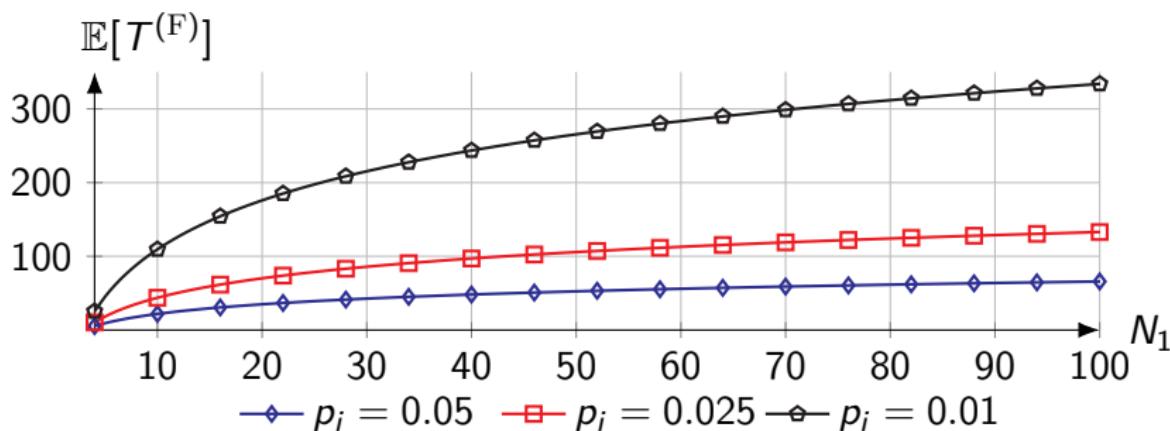
$\epsilon_A$	<i>Allowed service downtime per year</i>
0.9	36 days
0.95	18 days
0.99	3 days
0.999	8 hours
0.9999	52 minutes
0.99999	5 minutes
1	0 minutes

---

# 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 and Equilibrium Existence)

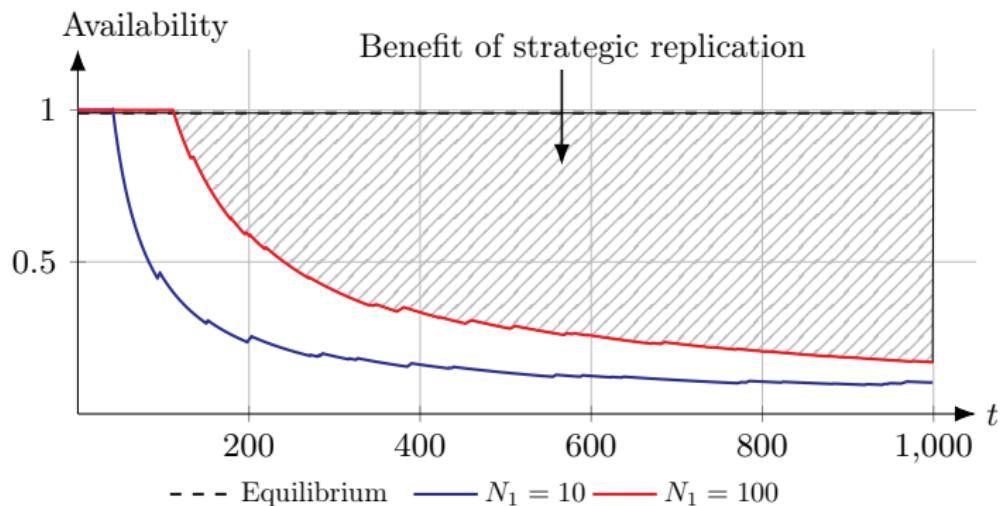
Assuming

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

Then the following holds.

1. *For each strategy pair  $\pi$ , there exists a pair of stationary best responses.*
2. *Best responses can be computed by using linear programming.*
3. *A constrained, stationary Markov perfect equilibrium (MPE) exists.*

# The Benefit of Strategic Replication

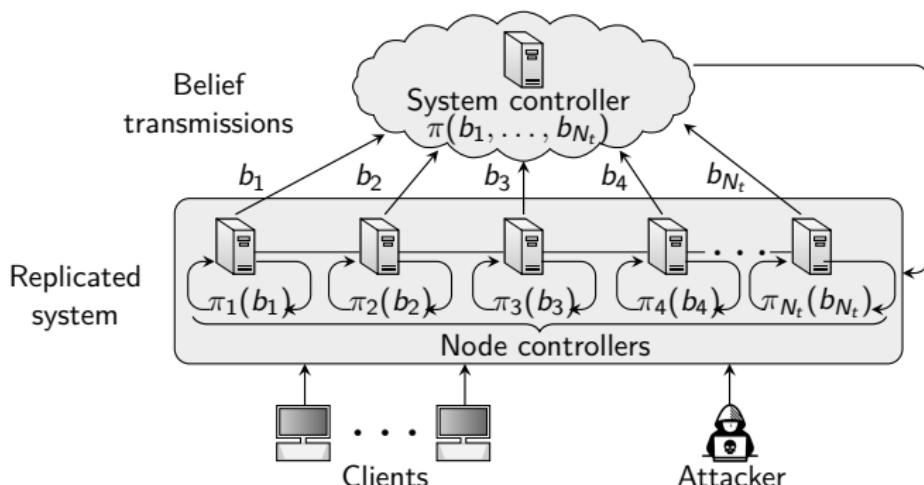


## Key insight

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*.

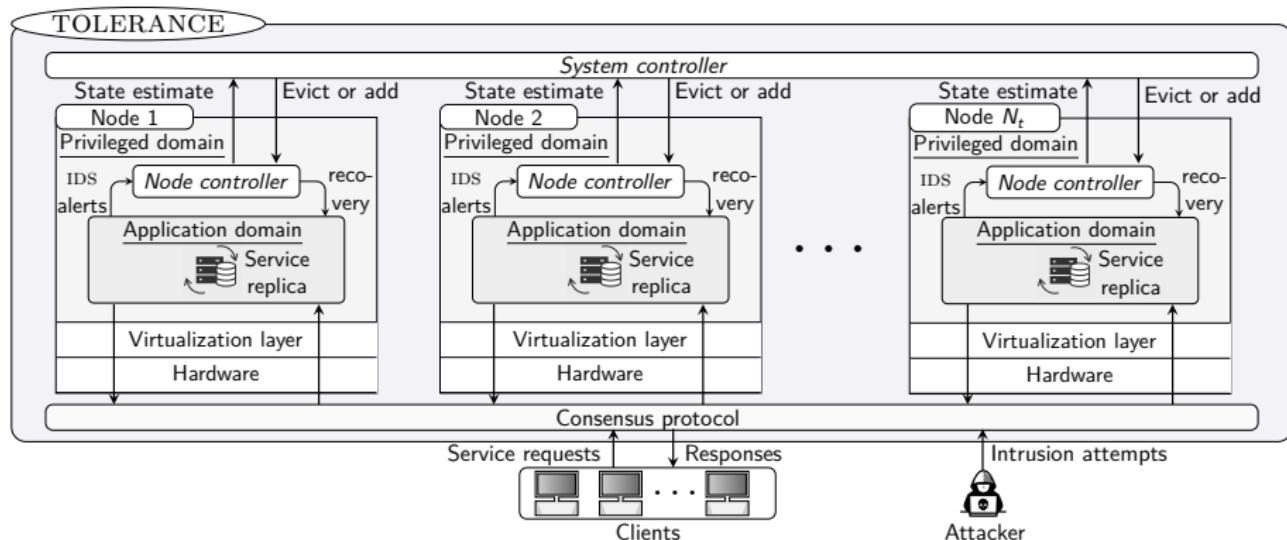


# Experiment Setup - Testbed



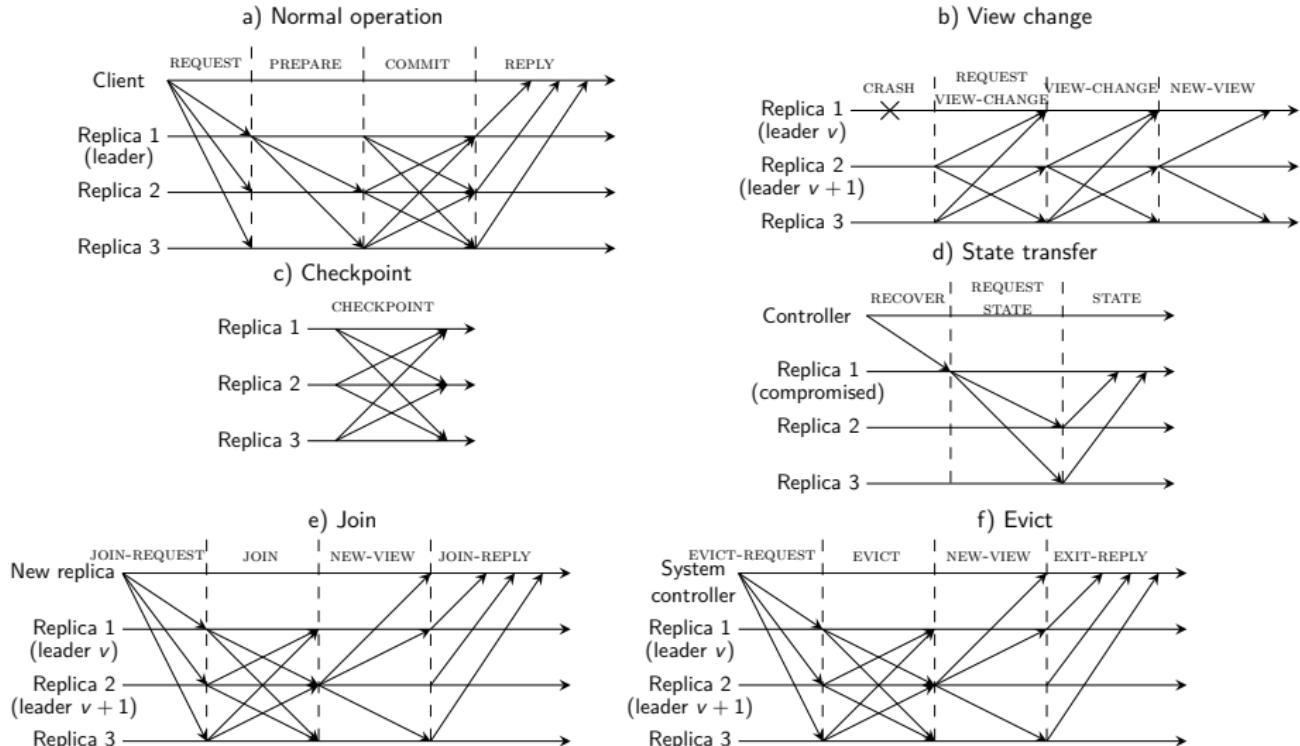
# The TOLERANCE Architecture

Two-level recovery and replication control with feedback.

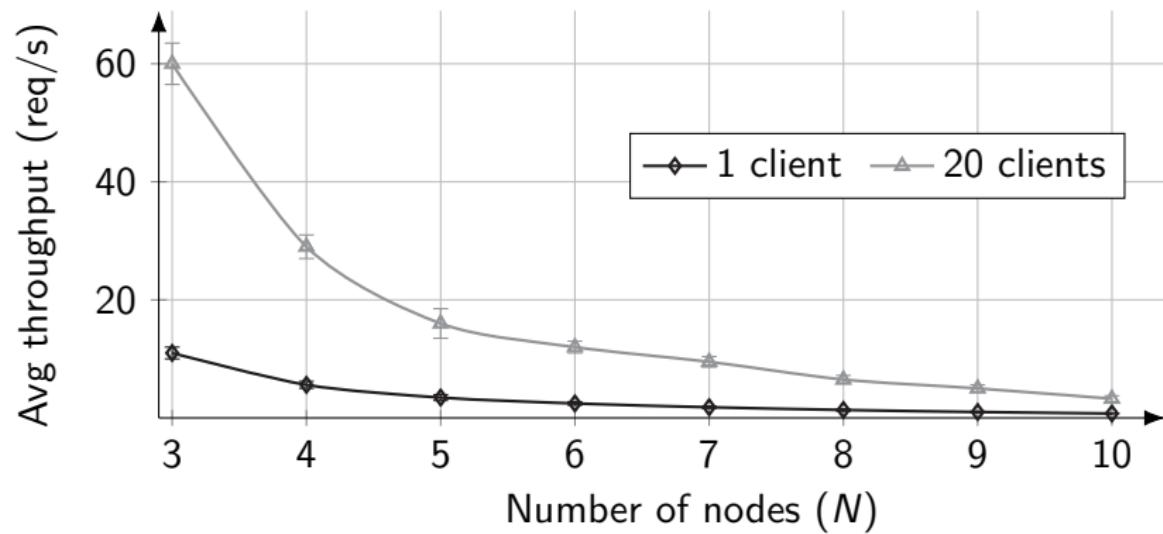


- ▶ A replicated **web service** which offers two operations:
  - ▶ A **read** operation that returns the service state.
  - ▶ A **write** operation that updates the state.

# 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

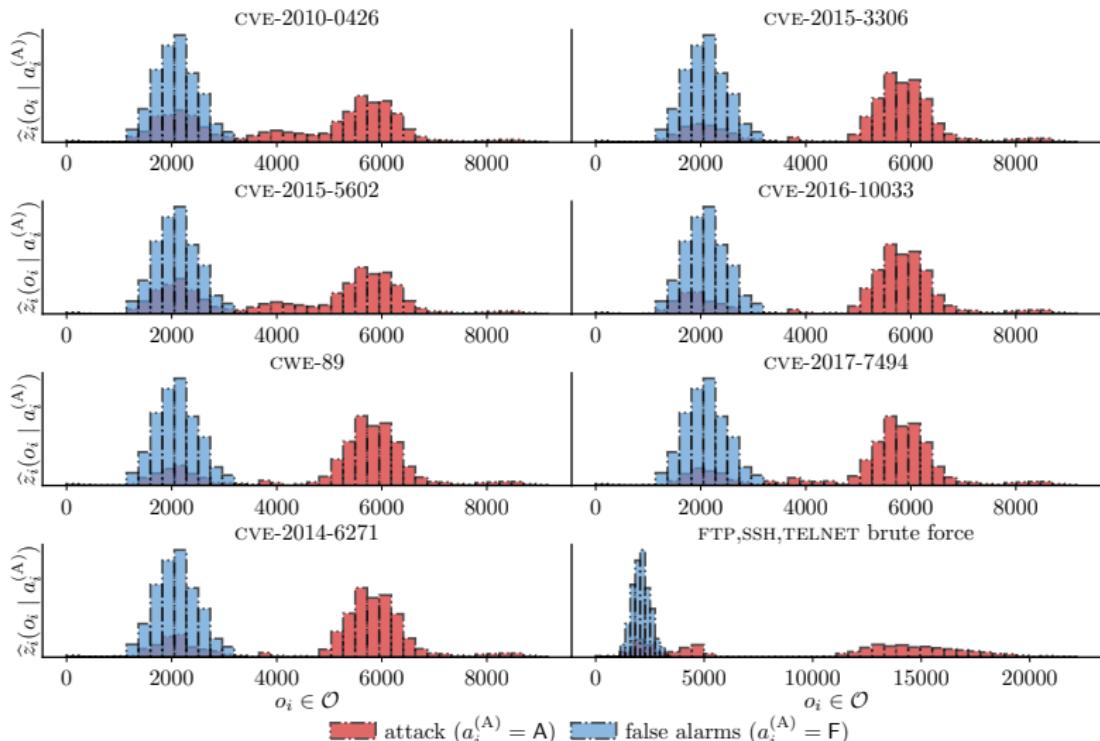
Table 1: Intrusion steps.

## 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

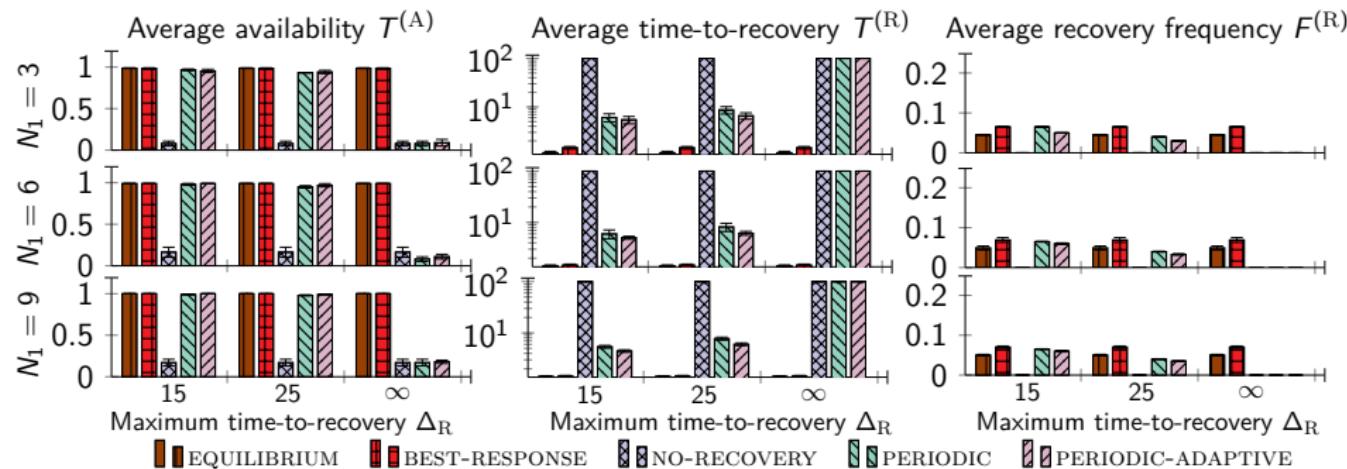
Table 2: Background services.

# Estimated Distributions of Intrusion Alerts



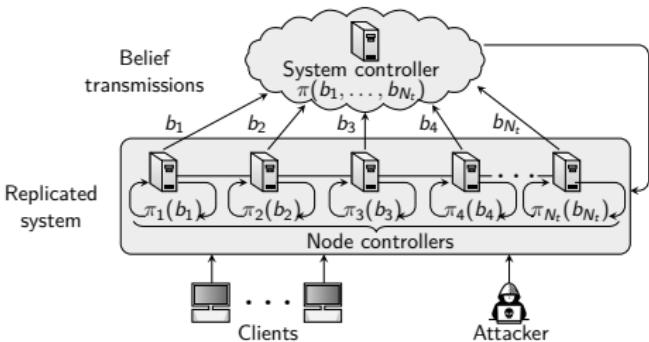
- ▶ We estimate the observation distribution  $z$  with the empirical distribution  $\hat{Z}$  based on  $M$  samples.
- ▶  $\hat{z} \xrightarrow{\text{a.s.}} z$  as  $M \rightarrow \infty$  (Glivenko-Cantelli theorem).

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



Comparison between our game-theoretic control strategies and the baselines; x-axes indicate values of  $\Delta_R$ ; 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.