

Intrusion Tolerance for Networked Systems through Two-Level Feedback Control

IEEE DSN 2024, Brisbane, Australia
International Conference on Dependable Systems and Networks

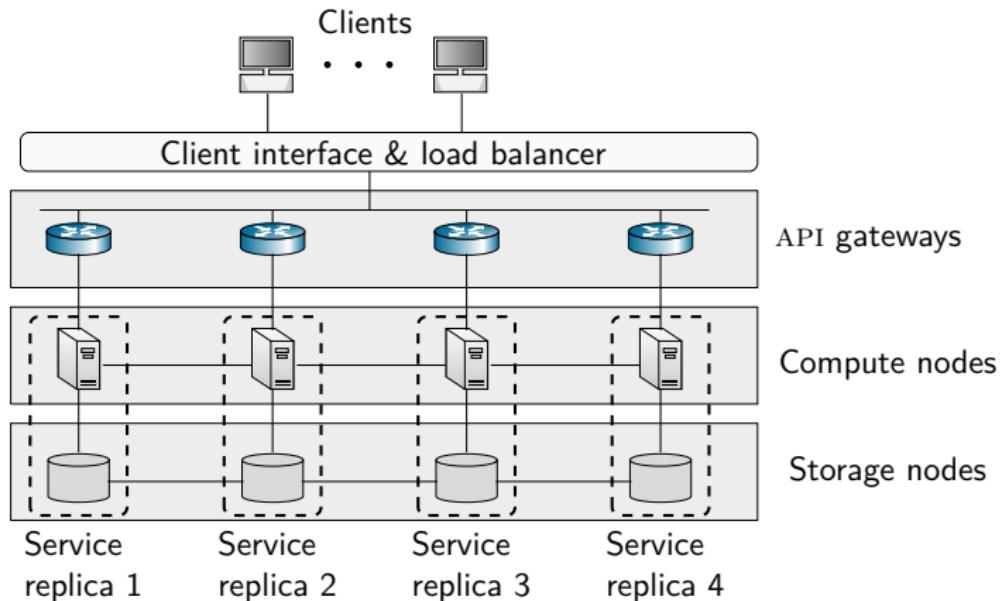
Kim Hammar and Rolf Stadler

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

June 27, 2024

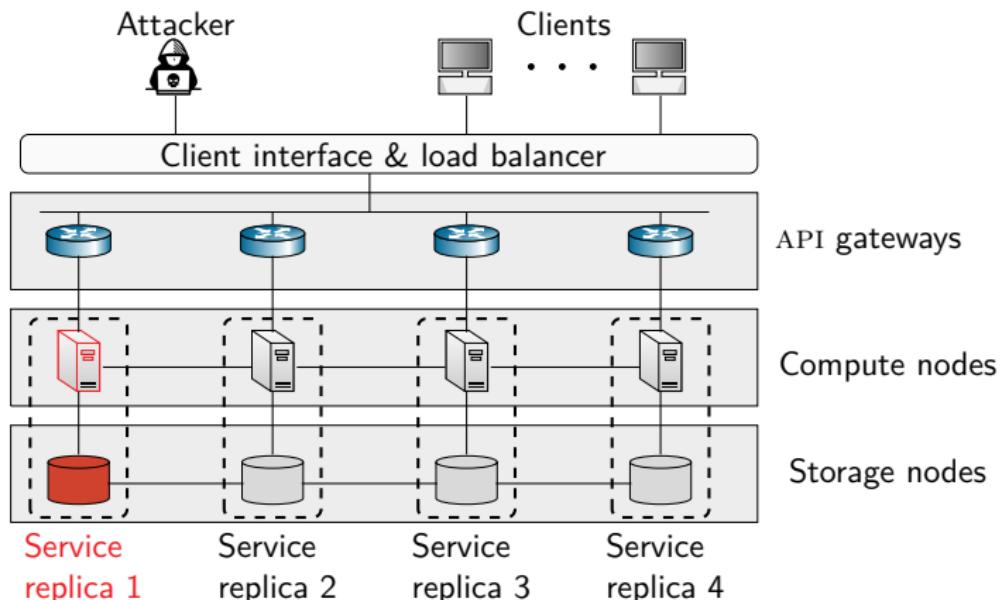


Use Case: Intrusion Tolerance



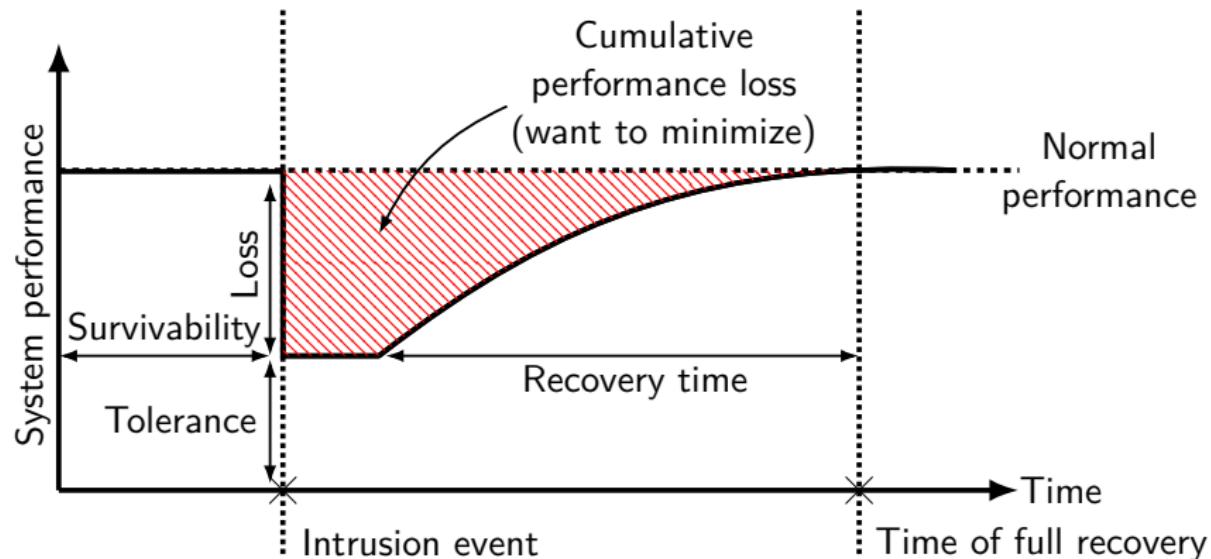
- ▶ A **replicated system** offers a service to a client population.
- ▶ The system should provide **service without disruption**.

Use Case: Intrusion Tolerance



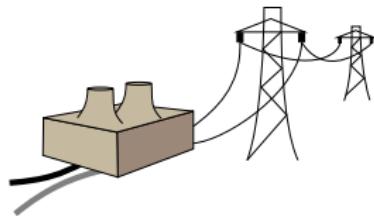
- ▶ An **attacker** seeks to intrude on the system and disrupt service.
- ▶ The system should **tolerate intrusions**.

Intrusion Tolerance (Simplified)



Increasing Demand for Intrusion-Tolerant Systems

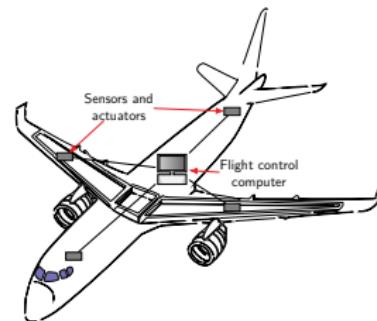
- ▶ As our **reliance on online services grows**, there is an increasing demand for intrusion-tolerant systems.
- ▶ Example applications:



Power grids
e.g., SCADA systems¹.



Safety-critical IT systems
e.g., banking systems,
e-commerce applications²,
healthcare systems, etc.



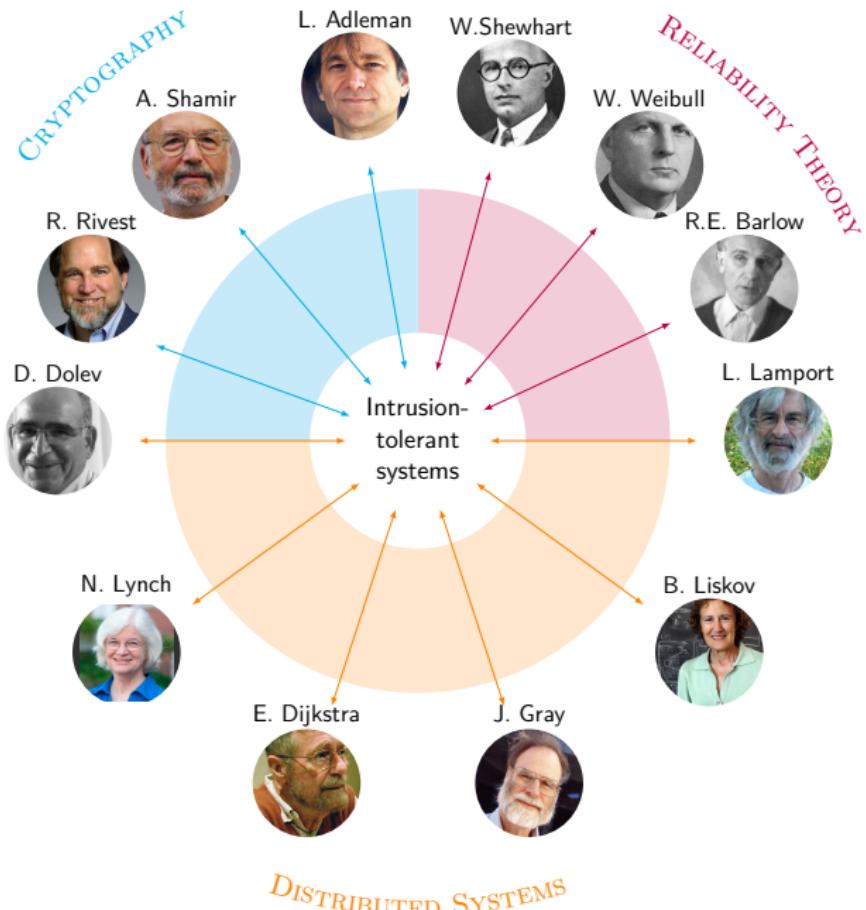
Real-time control systems
e.g., flight control computer³.

¹Amy 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).

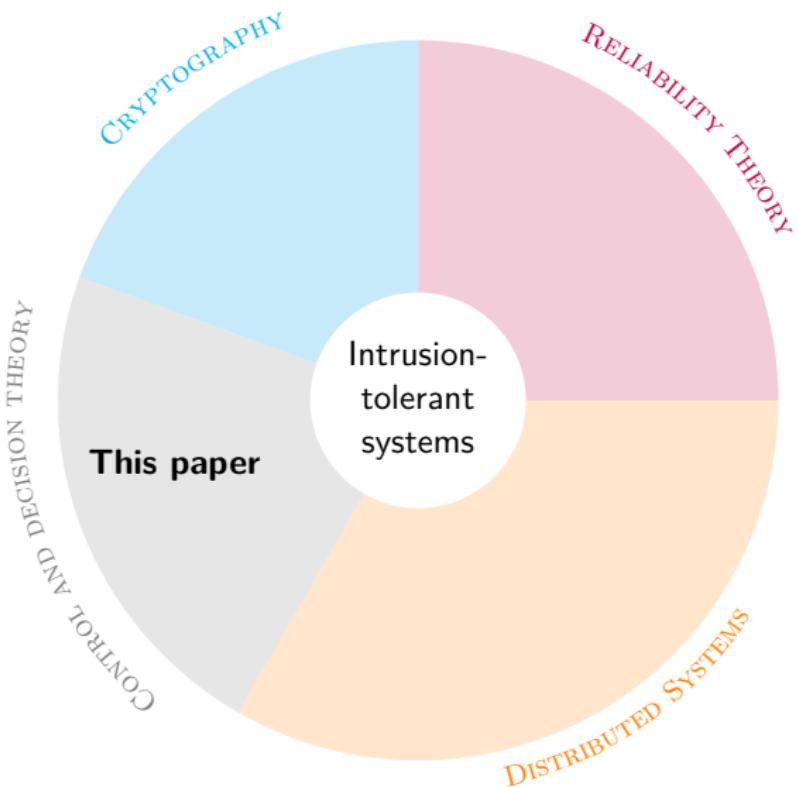
²Jukka Soikkeli et al. "Redundancy Planning for Cost Efficient Resilience to Cyber Attacks". In: *IEEE Transactions on Dependable and Secure Computing* 20.2 (2023), pp. 1154–1168. DOI: [10.1109/TDSC.2022.3151462](https://doi.org/10.1109/TDSC.2022.3151462).

³J.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).

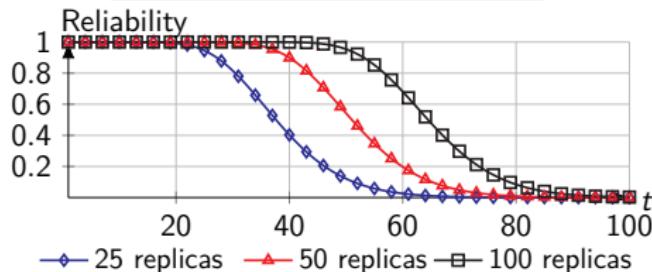
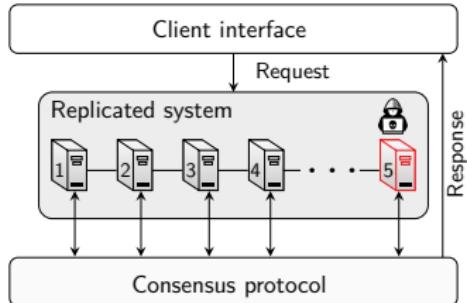
Theoretical Foundations of Intrusion Tolerance



Our Contribution



Building Blocks of An Intrusion-Tolerant System

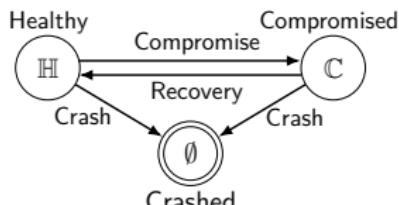


1. Intrusion-tolerant consensus protocol

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. Rampant 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 generation of requests. It is designed to extend the facilities of RamiX, a framework that solves several basic problems in distributed computing, including asynchronous group membership, reliable multicast (Byzantine agreement), and atomic multicasts. Using those protocols, Rampant supports the development of high-integrity services via the technique of state machine replication, and also extends this technique with a new approach called replicated state machines. The main advantage of Rampant over prior, focused approaches is its protocol abstraction. We show that its performance is comparable to its implementation, and we sketch its performance in the SPIN 2010+ implementation. We also sketch its

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 ensure a common total order on messages, and consistent group membership.

The approach adopted by SecuringRing 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

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 to replicas proactively. The recovery mech-

- 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 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 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

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 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. {pal, pruhel, maitigh, fwebber}@ibm.com

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

³ University of Maryland at College Park, Maryland. ramsay@cs.umd.edu

⁴ The Boeing Company. jpcxx.m.gossett@MW.Boeing.com

⁵ 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 ^{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 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 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 Desembargador Conrado, 1155, 80215-900, Brazil

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

An architecture for adaptive intrusion-tolerant applications

Partha Pal^{1,*} and Paul Rubel¹, Michael Atighehchi¹, Franklin Webber¹, William H. Sanders², Monna Seri², HarGovind Ramaswamy³, James Lyons², Tod Courtney⁴, Adina Aguirre⁵, Michel Culier⁶, Jerome Gosset⁴, Idit Keidar³

¹ IBM Technologies, Cambridge, Massachusetts, {ppal, prubel, matighechi, frankweb}@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.edu⁷ The Boeing

Company, jessica.o.gosset@FW Boeing.com⁸ 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@cs.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@nucs.vuw.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 Ciéncias da Computação, Pontifícia Universidade Católica do Paraná, Rua Dona Francisca, 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, ramsway, jlyons, tod}

gossett}@uiuc.edu

³ University of Maryland at College Park, Maryland, rams@engr.umd.edu⁴ The Boeing

Company, jlyons.cs.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 Ciéncias 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
zeiter@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
kpm@eei.ee.ucsb.edu, moser@eei.ee.ucsb.edu, pmm@eei.ee.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

Practical Byzantine Fault Tolerance and Proactive Recovery

MIGUEL CASTRO
Microsoft Research
and
BARBARA LISKOV

A Qualitative Analysis of the Intrusion-Tolerance Capabilities of the MAETIA 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 Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Bloco C8, Faz. 3, 1749-016 Lisboa, Portugal
^b Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rua Imaculada Conceição, 1155, 80215-900, Brazil

An architecture for adaptive intrusion-tolerant applications

Partha Paul¹, and Paul Rinzel¹, Michael Aiglethoff¹, William H. Sanders², Monica Senz³, Harald-Gerd Raus³, Tod Courtney⁴, Adnan Agbavio², Michel Cukier¹, Jen Tobias Dostler¹, Rüdiger Kapitza¹
 Friedrich-Alexander University Erlangen-Nürnberg, Germany
¹BRN Tübingen, Tübingen, Massachusetts, USA; ²Brandeis University, Waltham, MA, USA; ³University of Illinois at Urbana-Champaign, Urbana, IL, USA; ⁴University of Maryland at College Park, Maryland, USA;

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

Hans P. Reiser
LASIGE
idade de Lisboa, P.
joseph@fdi.mct.pt

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
 {miguel, bessani, msc, nuno, pnv}@di.fc.ul.pt

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

Amy Babay*, Thomas Tantillo*, Trevor Aron, Marco Platania, and Yair Amir
Johns Hopkins University — {babay, tantillo, taron1, yairamir}@cs.jhu.edu
AT&T Labs — {platania}@research.att.com
Second Concepts LLC — yairamir@secondconcepts.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 protect Byzantine faults is to optimize the 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 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 Referência 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 Paul^{1,*} and Paul Rubel², Michael Atighechi³,
William H. Sanders², Monna Seri², HarGowind Ramu
Tol Courtney⁴, Adina Agarwal⁵, Michel Olsker⁵, Joe

¹ BBN Technologies, Cambridge, Massachusetts [ppal, prbel],
University of Illinois at Urbana-Champaign [mba, seri, ramsu]
² 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, shol@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@di.fc.ul.pt

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

Aug Baker¹, Thomas Baetke², Trevor Attie, Martin Platzer, and Yair Arad
¹ John Hopkins University — {dbak, tsbaetke, tattie, mplatzer}@cs.jhu.edu
² AT&T Labs — {pharran}@research.att.com

Special Concepts LLC — {yaronr}@specialconcepts.com

Resilient Intrusion Tolerance through Proactive a

Pando Souza ¹ Alysson Neves Bassani ¹ Mig
Nuno Ferreira Neves ² Paulo Veríssimo ²
LASIGE, Faculdade de Ciéncias da Universidade de Lisboa — e-mail:
{pjsousa, bassani, mpc, 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

processes within an asynchronous intrusion sys-
tem, a consensus total order on messages, and i-
nteresting group memberships.
The approach adopted by SecuringRing is proven

An architecture for adaptive intrusion-tolerant applications

Pantelis Palios¹, Paul Bubel², Michael Albrecht¹,
William H. Sanders³, Monica Sey³, Hartmut Koenig³,
Tom Courtney³, Adams Agius², Michel Cukier², Jon

J. Bello², Technion-Israel Institute of Technology, Haifa, Israel,
j.bello@tx.tau.ac.il
University of Texas at Dallas, Dallas, TX, USA,
msey@utdallas.edu
University of Maryland at College Park, Maryland, USA,
wbs@cs.umd.edu
Technion - Israel Institute of Technology, Haifa, Israel,
m.albrecht@tx.tau.ac.il

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

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

State Transfer for

Hypervisor-Based Proactive Recovery
of Heterogeneous Replicated Services

Tobias Dietrich, Rüdiger Kapitza
Friedrich-Alexander University
Erlangen-Nürnberg, Germany
tobias.dietrich@fau.de

- - -

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

Amy Baker¹, Thomas Taft^{1,2}, Trevor Arai, Mario Pinto, and Yair Arad
¹Johns Hopkins University — {dtb, mario, amry, yair}@cs.jhu.edu
²Special Concepts LLC — {trevor}@specialconcepts.com

Can we do better by leveraging decision theory and optimal control?

A Quantitative Analysis of the Intrusion-Tolerance Capabilities of the MFTA 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

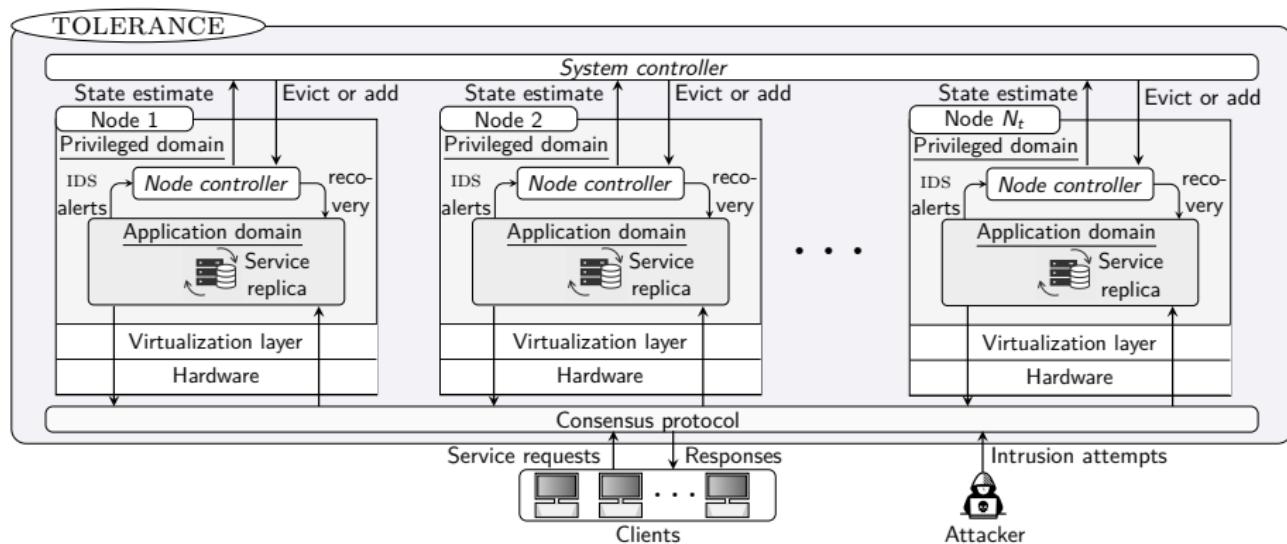
Miguel Correia^{3,4}, Nuno Ferreira Neves³, Lau Cheuk Lung³, Paulo Veríssimo³
³Faculdade de Ciências da Universidade de Lisboa, Departamento de Informática, Campo Grande, Edifício C1, Piso 3, 1749-001 Lisboa, Portugal
⁴Programa de Pós-Graduação em Informática Aplicada, Pontifícia Universidade Católica do Paraná, Rio Brilhante Campus, 1115, 80215-640, Brazil
Received 20 October 2005; revised 16 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*

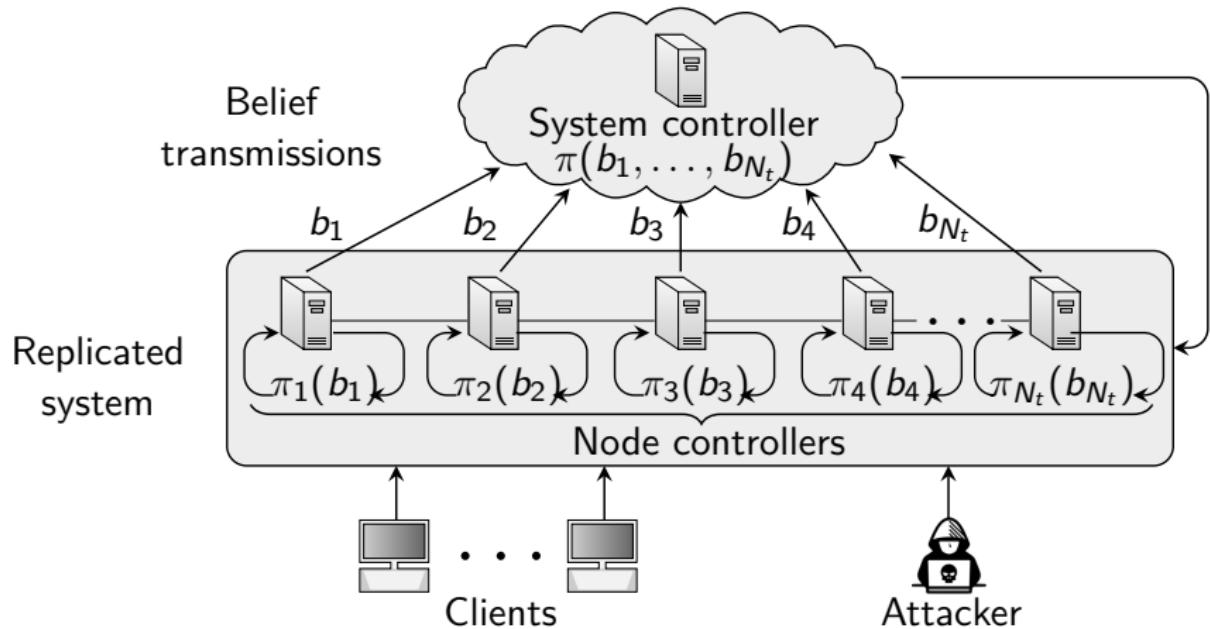
Network links are authenticated.

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 Control Problem



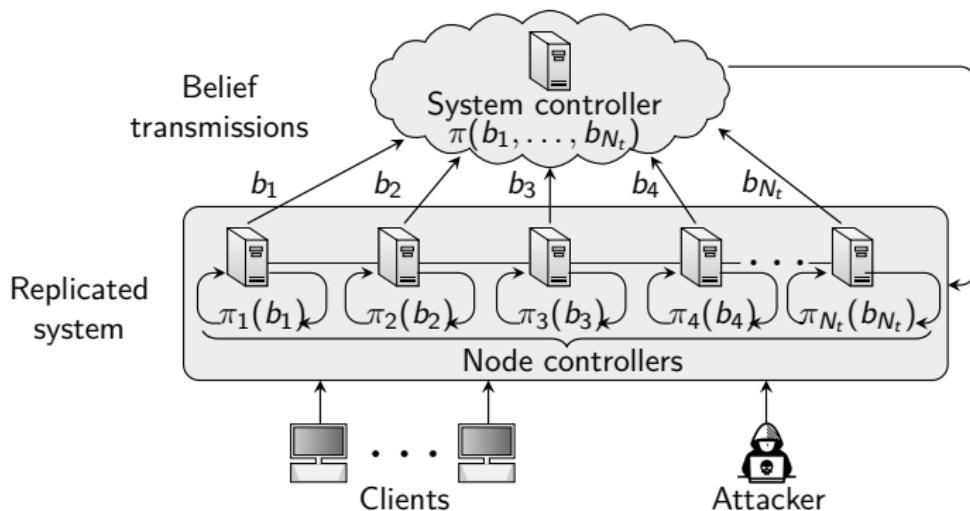
- ▶ The local level models intrusion recovery.
- ▶ The global level models replication control.

Assumption 1

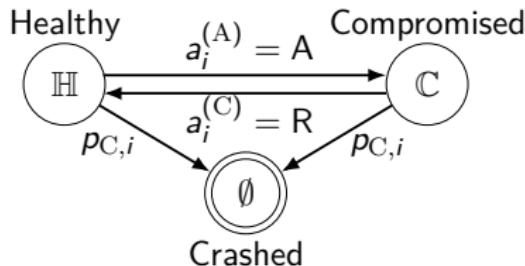
The probability that the system controller fails is negligible.

Assumption 2

Compromise and crash events are statistically independent across nodes.



The Local Control Problem



- ▶ Partially observed Markov decision process Γ_i .
- ▶ Controller actions: (R)ecover and (W)ait. $a_{i,t} \in \{R, W\}$.
- ▶ Node states: $\mathcal{S}_N = \{(\mathbb{H})ealthy, (\mathbb{C})ompromised, \emptyset\}$. $s_{i,t} \in \mathcal{S}_N$.
- ▶ State transition function: $f(s_{i,t} | s_{i,t}, a_{i,t})$.
- ▶ $p_{C,i}$: crash probability, $p_{A,i}$: intrusion probability.
- ▶ Observation $o_{i,t} \sim z_i(\cdot | s_{i,t})$: e.g., IDS alerts at time t .

Node Controller Strategy

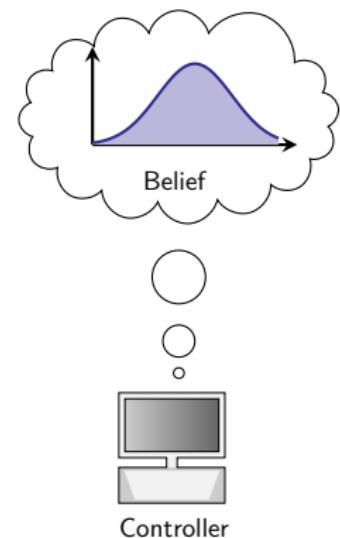
- ▶ The controller computes the **belief**

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

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

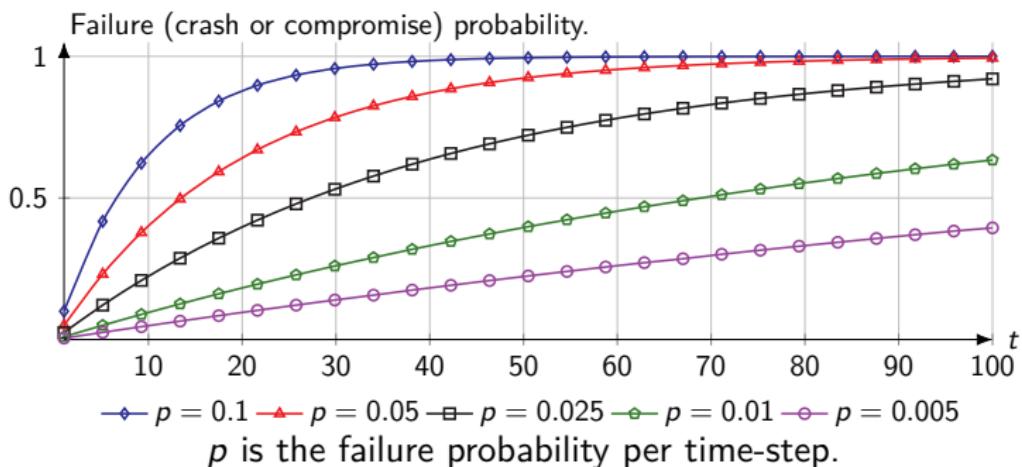
- ▶ Controller strategy:

$$\pi : [0, 1] \rightarrow \{\text{W}, \text{R}\}.$$

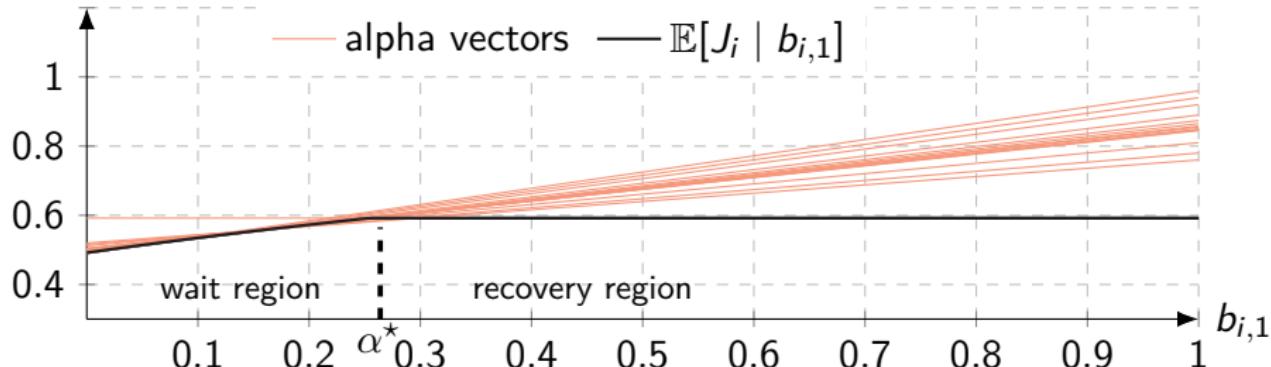


Node Controller Objective

- ▶ **Cost:** $J_i \triangleq \eta T_i^{(R)} + F_i^{(R)}$.
 - ▶ $T_i^{(R)}$ 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 Optimal Control Strategy



The controller's optimal cost function.

Theorem 2

There exists an optimal control strategy that satisfies

$$\pi_{i,t}^*(b_{i,t}) = R \iff b_{i,t} \geq \alpha_{i,t}^*, \quad \forall t,$$

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

Efficient Computation of Optimal Recovery Strategies

Algorithm 1: Threshold Optimization

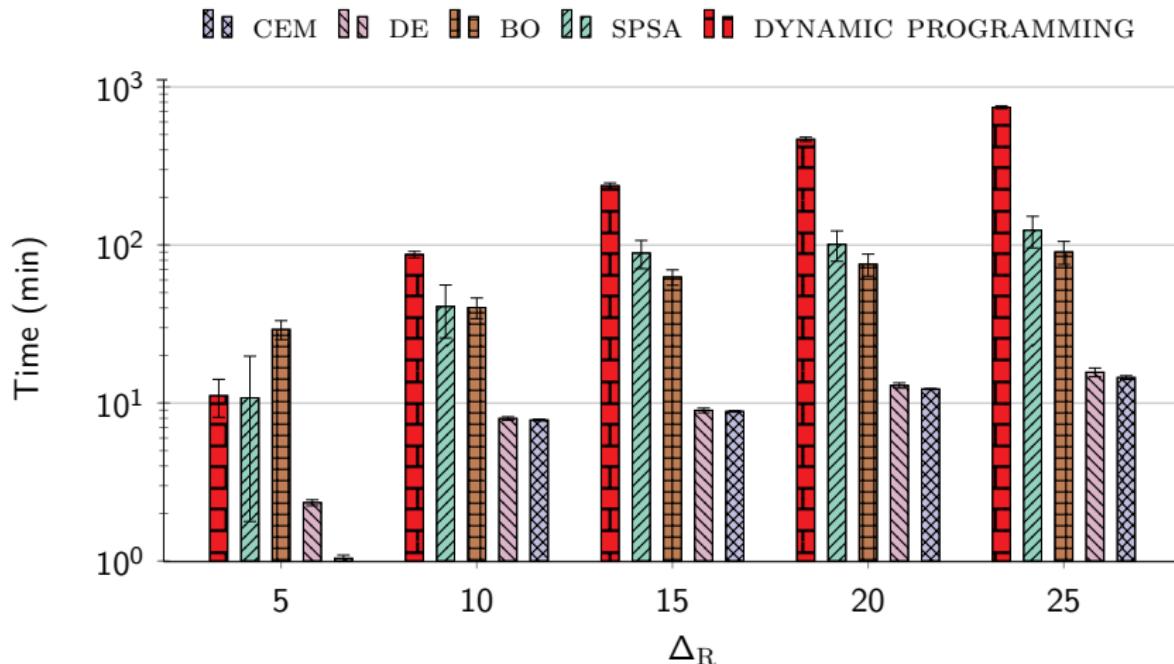
- 1 **Input:** Objective function J_i , parametric optimizer po.
- 2 **Output:** An approximate optimal control strategy $\hat{\pi}_{i,\theta}$.

3 Algorithm

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

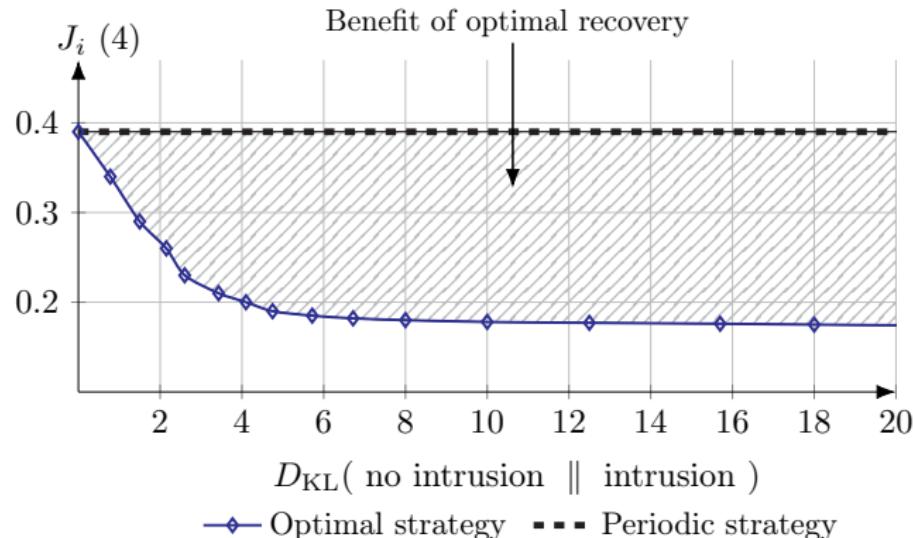
- ▶ Examples of **parameteric optimization algorithmns**: CEM, BO, CMA-ES, DE, SPSA, etc.

Efficient Computation of Optimal Recovery Strategies



Mean compute time to obtain an optimal recovery strategy for different values of the bounded-time-to-recovery constraint Δ_R .

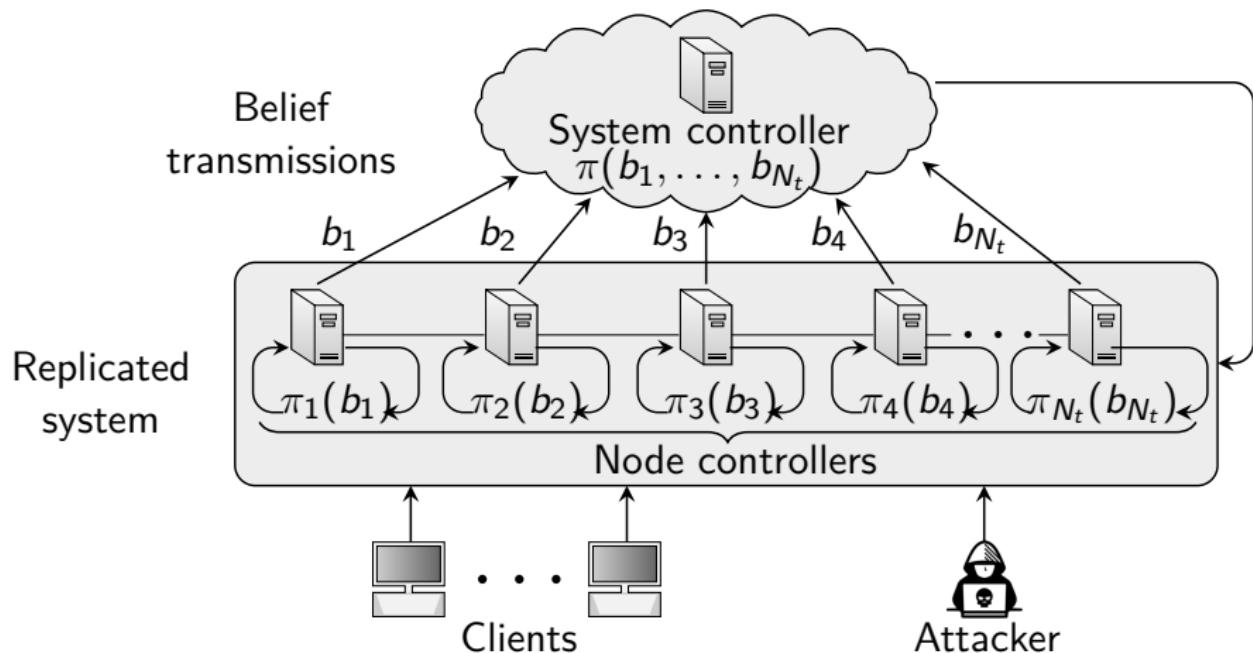
The Benefit of Optimal Recovery Control



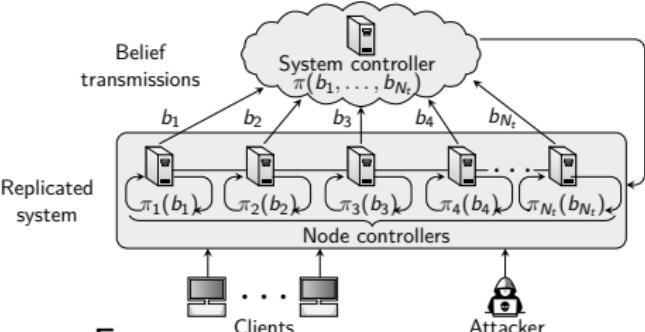
Key insight

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

Intrusion Tolerance as a Two-Level Control Problem



The Global Control Problem



- ▶ **Constrained Markov decision process Γ .**
- ▶ **States:** $\mathcal{S}_S = \{0, 1, \dots, s_{\max}\}$, the number of healthy nodes.
- ▶ **Controller actions:** Add $a_t^{(C)} \in \{0, 1\}$ nodes.
- ▶ **Dynamics f :** depend on the local nodes.
- ▶ **Markov strategy:**

$$\pi : \mathcal{S}_S \rightarrow \{0, 1\}.$$

System Controller Objective

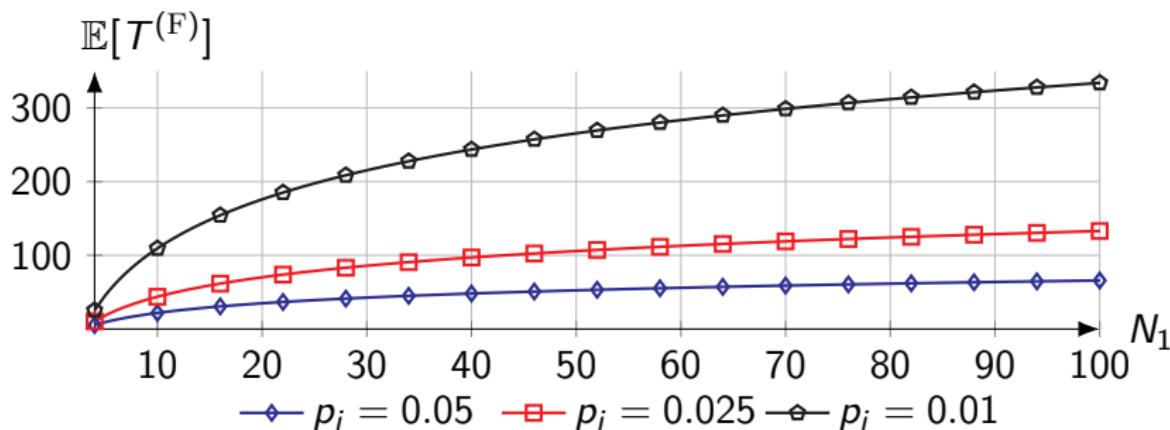
- ▶ **Cost:** $J \triangleq \lim_{T \rightarrow \infty} \sum_{t=1}^T \frac{a_t}{T}$.
- ▶ **Constraint:** $T^{(A)} \geq \epsilon_A$, where $T^{(A)}$ is the availability.

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 3 (Optimal Control Strategy Existence)

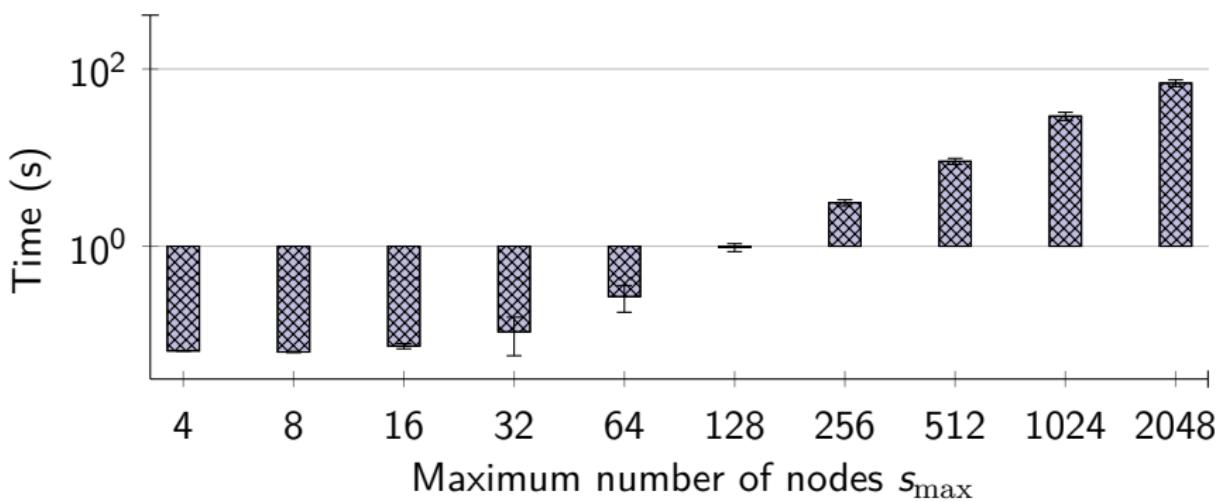
Assuming

- (A) *The Markov chain induced by any control strategy is unichain.*
- (B) *The availability constraint is feasible.*

Then the following holds.

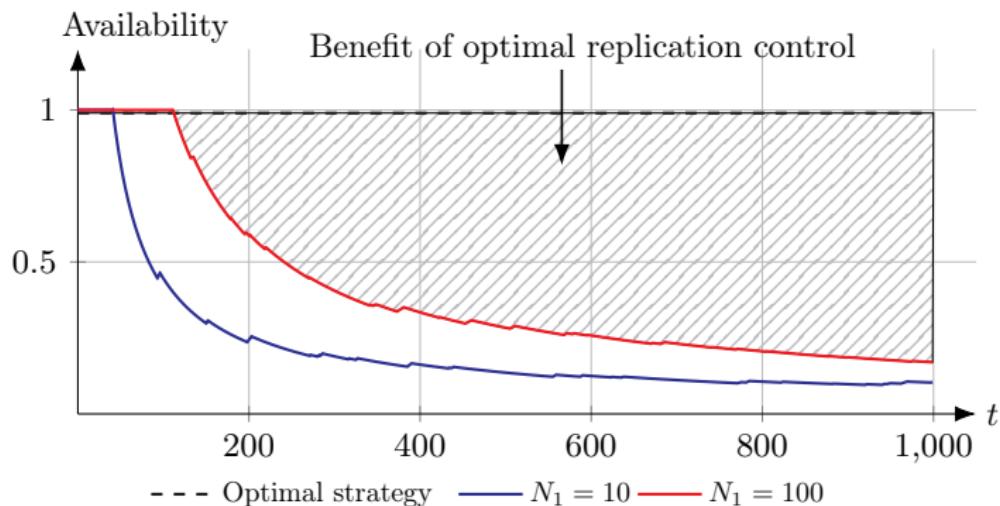
1. *There exists an optimal stationary replication control strategy.*
2. *The optimal strategy has a threshold structure.*
3. *An optimal replication control strategy can be computed by using linear programming.*

Efficient Computation of Optimal Replication Control Strategies



Mean compute time to obtain an optimal replication control strategy.

The Benefit of Optimal Replication Control

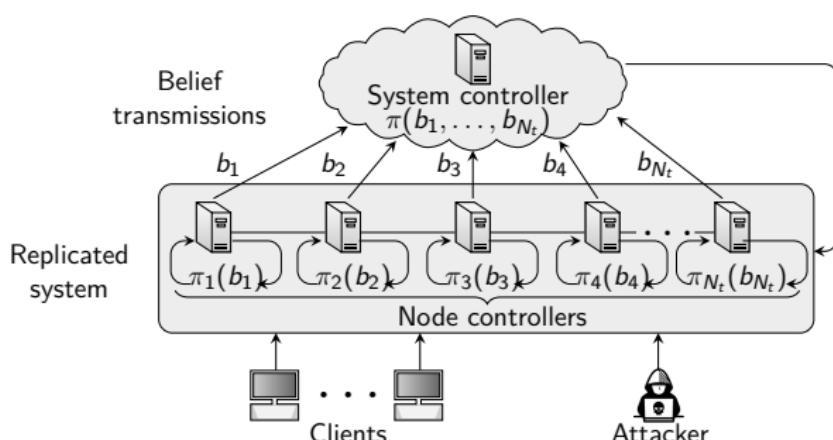


Key insight

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

Summary of the Control-Theoretic Model

- ▶ **Intrusion recovery control.**
 - ▶ Partially observed Markov decision process.
 - ▶ Threshold structure of optimal control strategies.
 - ▶ Efficient computation through *stochastic approximation*.
- ▶ **Replication control.**
 - ▶ Constrained Markov decision process.
 - ▶ Threshold structure of optimal control strategies.
 - ▶ Efficient computation through *linear programming*.

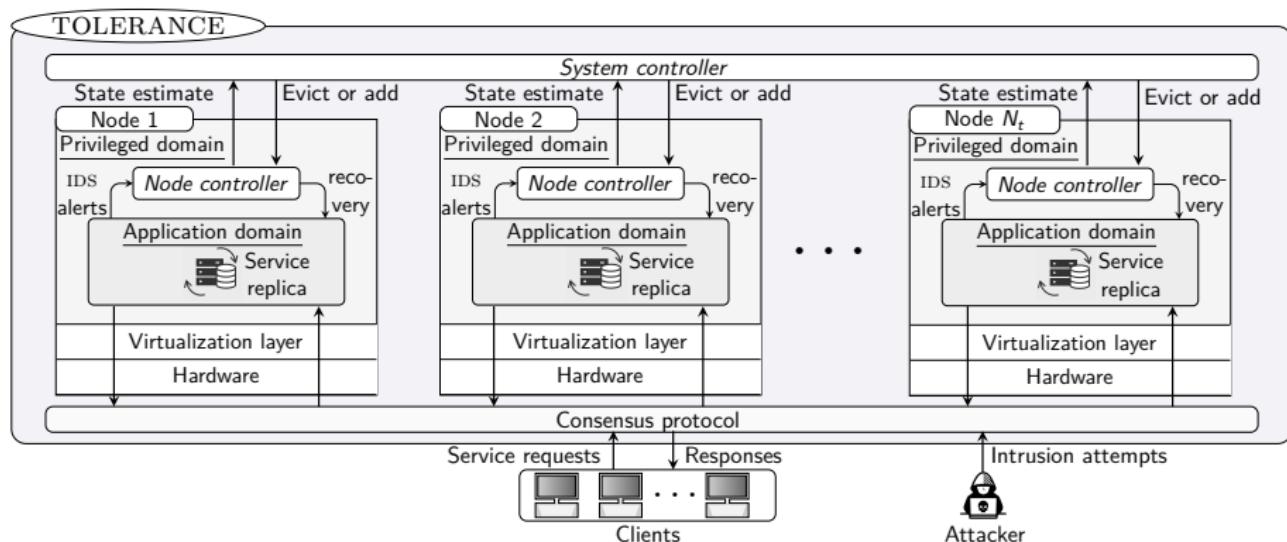


Experiment Setup - Testbed



The TOLERANCE Architecture

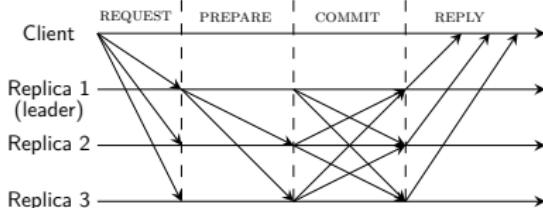
Two-level recovery and replication control with feedback.



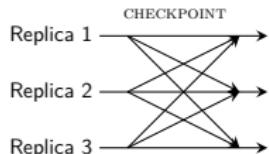
- ▶ A replicated **web service** which offers two operations:
 - ▶ A **read** operation that returns the service state.
 - ▶ A **write** operation that updates the state.

Intrusion-Tolerant Consensus Protocol (MINBFT)

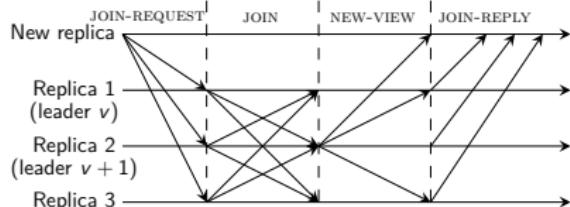
a) Normal operation



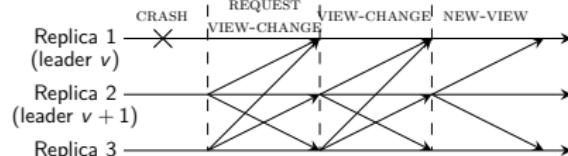
c) Checkpoint



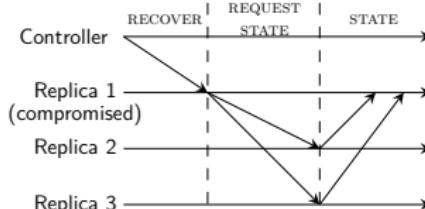
e) Join



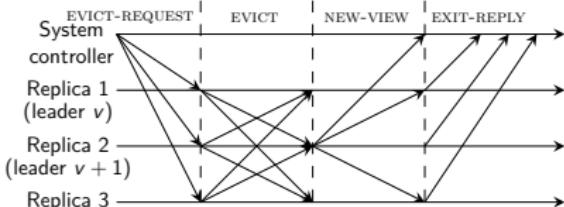
b) View change



d) State transfer



f) Evict



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

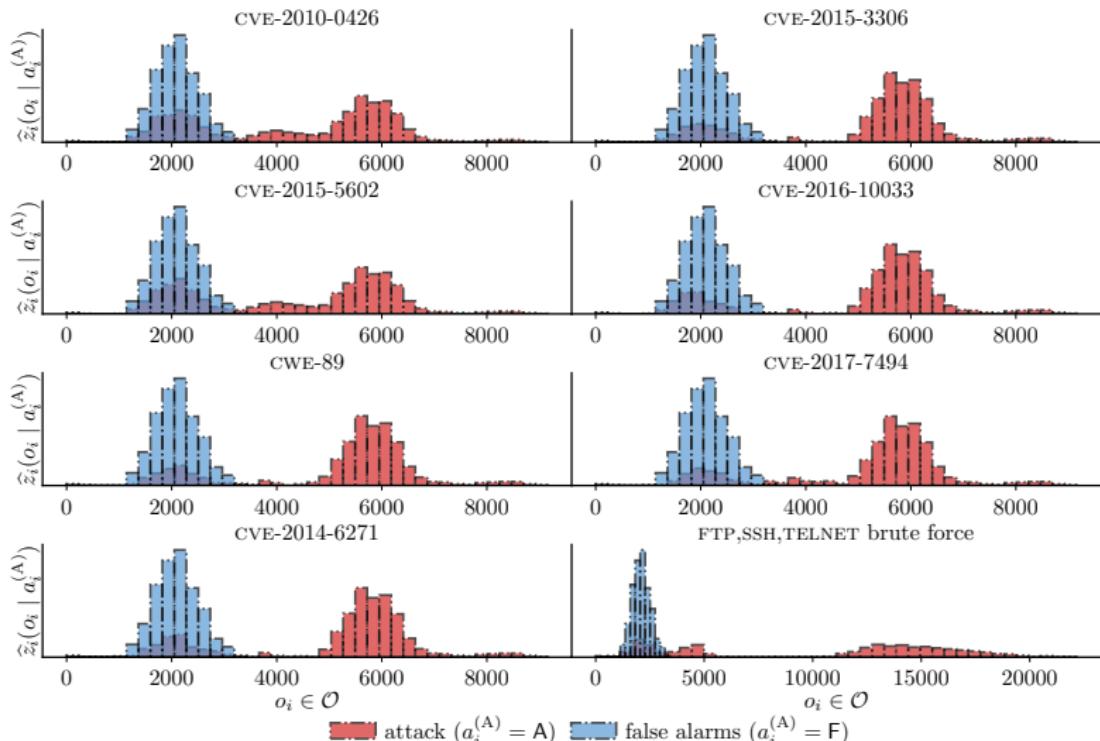
Table 1: Intrusion steps.

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

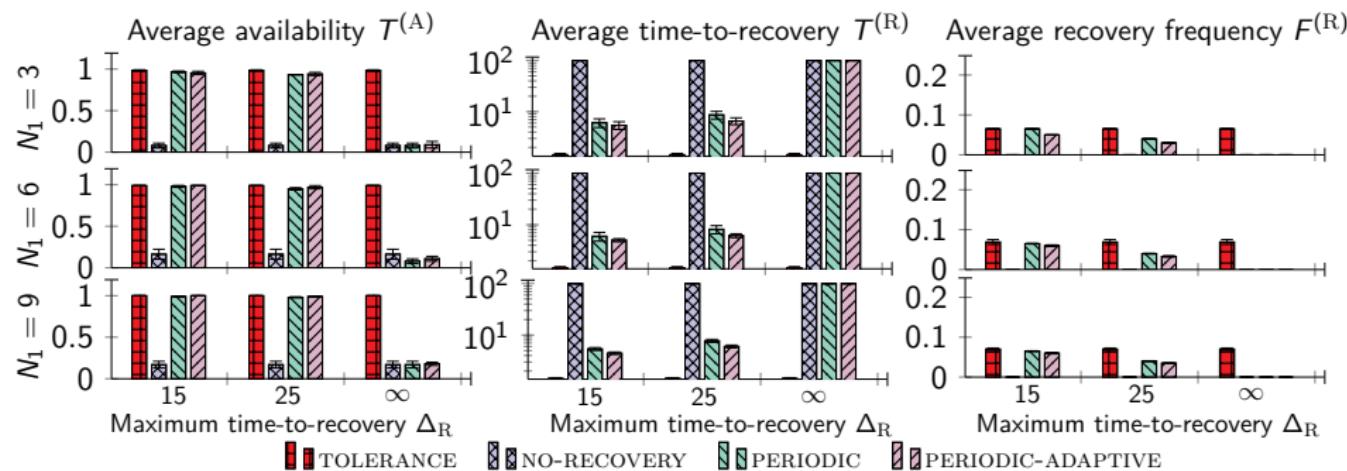
Table 2: Background services.

Estimated Distributions of Intrusion Alerts



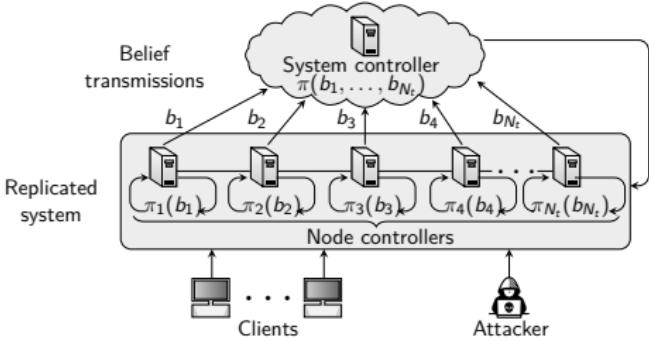
- ▶ We estimate the observation distribution z with the empirical distribution \hat{Z} based on M samples.
- ▶ $\hat{z} \xrightarrow{\text{a.s.}} z$ as $M \rightarrow \infty$ (Glivenko-Cantelli theorem).

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



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