Lecture Notes in Computer Science 13146

More information about this subseries at https://link.springer.com/bookseries/7410

Somanath Tripathy · Rudrapatna K. Shyamasundar ·
Rajiv Ranjan (Eds.)

Information Systems Security

17th International Conference, ICISS 2021
Patna, India, December 16–20, 2021
Proceedings

Springer

Editors
Somanath Tripathy
Indian Institute of Technology Patna
Patna, India

Rudrapatna K. Shyamasundar
Indian Institute of Technology Bombay
Mumbai, India

Rajiv Ranjan
Newcastle University
Newcastle upon Tyne, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-92570-3 ISBN 978-3-030-92571-0 (eBook)
https://doi.org/10.1007/978-3-030-92571-0

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This book comprises the proceedings of the 17th International Conference on Information Systems Security (ICISS 2021), held at the Indian Institute of Technology (IIT) Patna from December 16 to 20, 2021, in a hybrid mode.

A total of 65 papers were submitted in response to the call for papers for this edition of ICISS. We received submissions from authors in several countries. All the submissions were subjected to a blind evaluation procedure by the Technical Program Committee, which was composed of 47 experts from academia and industry. Each paper was reviewed by at least three experts. The papers were evaluated and discussed online by members of the Technical Program Committee over a week. After careful consideration of the merits of the papers the conference accepted nine full papers, two short papers, and four work-in-progress papers. The net acceptance rate of the conference was approximately 22%. A wide range of topics in systems security and privacy are covered, both in theory and in practice, such as attack detection, malware identification, distributed system security, cryptology, and asset management through blockchains including applications of artificial intelligence and machine learning for security. In addition to the accepted papers, the conference program featured three keynote talks by three distinguished speakers working in the field of security. The keynote speakers, in alphabetical order by first name, were as follows:

- George Cybenko, Dorothy and Walter Gramm Professor of Engineering at Dartmouth College, USA.
- Milind Tambe, Gordon McKay Professor of Computer Science and Director of the Center for Research in Computation and Society (CRCS) at Harvard University, USA, and Director of AI for Social Good at Google Research India.
- Omer Rana, Professor of Performance Engineering at Cardiff University, UK.

Thanks to these experts who took their precious time to address the audience live during somewhat odd hours.

The success of ICISS 2021 would not have been possible without the contributions of the numerous volunteers who gave their time and energy to ensure the success of the conference and its associated events. We would like to express our gratitude to the Program Committee for their hard work and prompt submission of their evaluations of papers, and we thank the publicity chairs for attracting good submissions in this pandemic period. Our thanks go to the local organizing committee as well as the faculty, staff, and students at the Department of Computer Science and Engineering, Indian Institute of Technology Patna for all the efforts and support for the smooth running of the conference in the hybrid mode. Thanks also go to the Steering Committee for their invaluable support in these trying times of the COVID-19 pandemic. The Conference Management Toolkit from Microsoft was crucial in carrying out the arduous chores of examining submissions, reviewing papers, and alerting authors about the status of their papers. It is our pleasure to express our gratitude to Springer Nature for assisting us in disseminating the proceedings of the conference in the LNCS series as in the past. Special thanks go to Ronan Nugent and Anna Kramer for making the proceedings available online at the time of conference with very little leeway in terms of time.

Last but certainly not least, we would like to thank all the authors who submitted papers and the conference participants. We hope you find the proceedings of ICISS 2021 interesting, stimulating, and inspiring for future research.

December 2021

Somanath Tripathy
Rudrapatna K. Shyamasundar
Rajiv Ranjan

Organization

General Chair

R. K. Shyamasundar	IIT Bombay, India

Technical Program Co-chairs

Rajiv Ranjan	Newcastle University, UK
Somanath Tripathy	IIT Patna, India

Publicity Chairs

Vishwas Patil	IIT Bombay, India
N. V. Narendra Kumar	IDRBT, India
Devki Nandan Jha	University of Oxford, UK

Local Organizing Committee

Jimson Mathew	IIT Patna, India
Preetam Kumar	IIT Patna, India
Samrat Mondal	IIT Patna, India
Mayank Agarwal	IIT Patna, India
Somanath Tripathy	IIT Patna, India

Steering Committee

Aditya Bagchi	ISI Kolkota, India
Venu Govindaraju	SUNY, USA
Sushil Jajodia	George Mason University, USA
Somesh Jha	University of Wisconsin, USA
Arun Kumar Majumdar	IIT Kharagpur, India
Chandan Mazumdar	Jadavpur University, India
Atul Prakash	University of Michigan, USA
D. Janakiram	IDRBT, India
Pierangela Samarati	University of Milan, Italy
R. K. Shyamasundar	IIT Bombay, India

Program Committee

Adwait Nadkarni	College of William and Mary, USA
Anirban Basu	Hitachi Ltd, Japan, and University of Sussex, UK
Anoop Singhal	NIST, USA

Atul Prakash	University of Michigan, USA
Bimal Roy	ISI Kolkata, India
Bodhisatw Mazumdar	IIT Indore, India
Bruhadeshwar Bezawada	IIT Jammu, India
Changyu Dong	Newcastle University, UK
Claudio Ardagna	University of Milan, Italy
Devki Nandan Jha	University of Oxford, UK
Donghoon Chang	IIIT Delhi, India
Eric Filiol	ENSIBS and CNAM, France
Haibing Lu	Santa Clara University, USA
Hayawardh Vijayakumar	Samsung Research, USA
Indrakshi Ray	Colorado State University, USA
Laszlo Szekeres	Google, USA
Lorenzo De Carli	Worcester Polytechnic Institute, USA
Luigi Logrippo	Université du Québec en Outaouais, Italy
Mahavir Prasad Jhanwar	Ashoka University, India
Mahesh Tripunitara	University of Waterloo, Canada
Manik Lal Das	DA-IICT, India
Mauro Conti	University of Padua, Italy
Michele Carminati	Polytechnic University of Milan, Italy
N. V. Narendra Kumar	IDRBT, India
Peng Liu	Pennsylvania State University, USA
Pierangela Samarati	University of Milan, Italy
Prem Prakash Jayaraman	Swinburne University of Technology, Australia
R. Sekar	Stony Brook University, USA
Rajat Subhra	IIT Kharagpur, India
Rajesh Pillai	DRDO, India
Ram Krishnan	University of Texas at San Antonio, USA
Rinku Dewri	University of Denver, USA
Sabrina De Capitani di Vimercati	University of Milan, Italy
Sanjay Rawat	Vrije University, The Netherlands
Saurabh Garg	University of Tasmania, Australia
Scott Stoller	Stony Brook University, USA
Silvio Ranise	Fondazione Bruno Kessler, Italy
Somitra Sanadhya	IIT Ropar, India
Stijn Volckaert	KU Leuven, Belgium
Souradyuti Paul	IIT Bhilai, India
Sourav Sengupta	NTU, Singapore
Subhamoy Maitra	ISI Kolkata, India
Sushil Jajodia	George Mason University, USA
Venkatakrishnan Venkat	University of Illinois at Chicago, USA
Vijay Atluri	Rutgers University, USA
Vinod Yegneswaran	SRI International, USA
Vishwas Patil	IIT Bombay, India

Abstract of Keynote Talks

Multiagent Reasoning for Social Impact: Results from Deployments for Public Health and Conservation

Milind Tambe

Gordon McKay Professor of Computer Science and Director of the Center for Research in Computation and Society (CRCS), Harvard University, Director, AI for Social Good at Google Research India

Abstract. With the maturing of AI and multiagent systems research, we have a tremendous opportunity to direct these advances towards addressing complex societal problems. I focus on the problems of public health and conservation, and address one key cross-cutting challenge: how to effectively deploy our limited intervention resources in these problem domains. I will present results from work around the globe in using AI for public health, e.g., HIV prevention, Maternal and Child care interventions, and COVID modeling, and AI for conservation, e.g., wildlife conservation. Achieving social impact in these domains often requires methodological advances. To that end, I will highlight key research advances in multiagent reasoning and learning, in particular in, computational game theory, restless bandits and influence maximization in social networks.In pushing this research agenda, our ultimate goal is to facilitate local communities and non-profits to directly benefit from advances in AI tools and techniques.

Data Privacy Re-visited During Covid19

Omer Rana

College Dean of International Professor of Performance Engineering,
Cardiff University, UK

Abstract. The COVID19 Pandemic has highlighted our dependence on online services (from government, e-commerce/retail, and entertainment), often hosted over external cloud computing infrastructure. The users of these services interact with a web interface rather than the larger distributed service provisioning chain that can involve an interlinked group of cloud providers. The data and identity of users are often provided to service provider who may share it (or have automatic sharing agreement) with backend services (such as advertising and analytics). We propose the development of compliance-aware cloud application engineering, which is able to improve transparency of personal data use – particularly with reference to the European GDPR regulation. Key compliance operations and the perceived implementation challenges for the realization of these operations in current cloud infrastructure are outlined. This talk will also explore how the convenience-vs-privacy challenges can be realised as users and service providers go on-line, and the economics behind delivering privacy services as part of cloud-based provision.

Modeling and Leveraging Attrition in Cyber Operations

George Cybenko and Roger Hallman

Thayer School of Engineering, Dartmouth College, Hanover NH 03755, USA
gvc@dartmouth.edu
roger.hallman@navy.mil

Abstract. Advanced adaptive cyber operations require some form of online learning in real time using feedback and reinforcement from ongoing interactions. It is well known that operating well in such an environment entails balancing exploitation of currently best-known strategies with exploration of actions that might improve performance. This is the case for example, when a variety of responses are possible to mitigate an ongoing attack. However, unlike offline simulations of reinforcement learning, online reinforcement learning can lead to attrition of assets when exploration results in bad actions. We will present modeling and analysis approaches for learning with attrition in such circumstances.

There is sustained interest in developing cyber and physical systems consisting of multiple coordinated components, each component being simple, inexpensive, and easy to replace. Consider for example the following kind of military vision:

"A military made up of small numbers of large, expensive, heavily manned, and hard- to-replace systems will not survive on future battlefields, where swarms of intelligent machines will deliver violence at a greater volume and higher velocity than ever before." ([Brose 2019])

Examples include cyber-bot networks, Internet of Things (IoT), swarms of unmanned autonomous vehicles (airborne, maritime and land based) as well as cloud computing infrastructures ([Campbell 2018], [Panfili et al. 2018], [Nguyen et al. 2017]). While many of the arguments for such systems are based on cost effectiveness and mission performance, we argue in this work that there are also compelling analytic arguments based on various advantages that machine learning, game theory and secure distributed computing offer for such systems. The goal is to explain those advantages in analytic terms.

The main question we address is "What provable, analytic advantages do swarm-type adaptive/learning systems have over monolithic systems?" Our particular interest is so-called Adaptive Cyber-Defense (ACD) in which cyber-defensive technologies adapt to changes in the attackers' techniques and/or behaviors, as well as to organic changes in the ambient operating environment ([Cybenko et al. 2014], [Jajodia et al. 2019], [Zhu et al. 2014]). Organic changes can be due to dynamic re-configurations of the information infrastructure, such as the addition or removal of compute nodes, sensors, applications and communications links.

The ACD's changes can be made by continuously monitoring the environment, learning its new characteristics, and implementing appropriate new control actions. The basis for making such adaptations in a stationary or slowly changing environment can be based on classical reinforcement learning and adaptive control ideas. However, if the operating environment changes because of adversary adaptations, existing mathematical and algorithmic principles for defensive adaptation do not directly apply with respect to convergence to optimal or near optimal solutions.

We study the problem of online learning using distributed Upper Confidence Bounds (UCB) algorithms [Auer 2002] in which cumulative regret (CR) is the performance criterion. CR is an appropriate performance metric because it captures the overall rate at which the systems' performance is improving, not just the asymptotic conditions under which optimality can be reached. The faster a system can approach some notion of optimality, the more it will outperform an adversary that is also changing but at a slower rate.

A key observation and technical contribution are the use of distributed systems to implement UCB-based learning. This entails the deliberate use of "suboptimal" actions to fully explore the values of the available actions. In other words, the system must sacrifice some of its capabilities to learn faster and perform better. However, because some agents within the distributed system are operating sub-optimally, they will be compromised and so some subset of information in the distributed learning system will lack integrity.

We have considered the problem of online learning, with cumulative regret minimization, for swarms of agents cooperating to achieve high assurance on missions' tasks. To achieve this, we have introduced the concept of "spatial" online learning by which action selection is guided by UCB-type criteria. Because we are dealing with multiple agents, multiple actions are possible by sampling the UCB modified Q-values. We have identified some regret minimizing challenges in so-called spatial learning and conjectured their solutions but without formal proof. Furthermore, we have performed principled simulations showing how learning and recovery rates can change the overall performance of a multiagent learning system.

Although we are keenly interested in convergence rates and algorithms for adversarial engagements in which all players are using online learning to improve play, the results here are solely for stationary environments in which adversaries do not adapt or learn during a single engagement. However, if we can adapt faster than our adversary, we can model them as short-term stationary which might be the best possible approach given no information about the adversary or their adaptation mechanisms.

We have identified some regret minimizing challenges in so-called spatial learning and conjectured their solutions but without formal proof. Furthermore, we have performed principled simulations showing how learning and recovery rates can change the overall performance of a multiagent learning system. While UCB-criteria have been used in offline parallel game play learning (Silver et al. [2016]) those uses are for parallel game playing, that is parallel independent engagement, not a single engagement in which adaptation/learning occurs as we have proposed here. A major opportunity for future work is cumulative regret minimizing, online reinforcement learning algorithms that make as few assumptions about the adversary's learning algorithms.

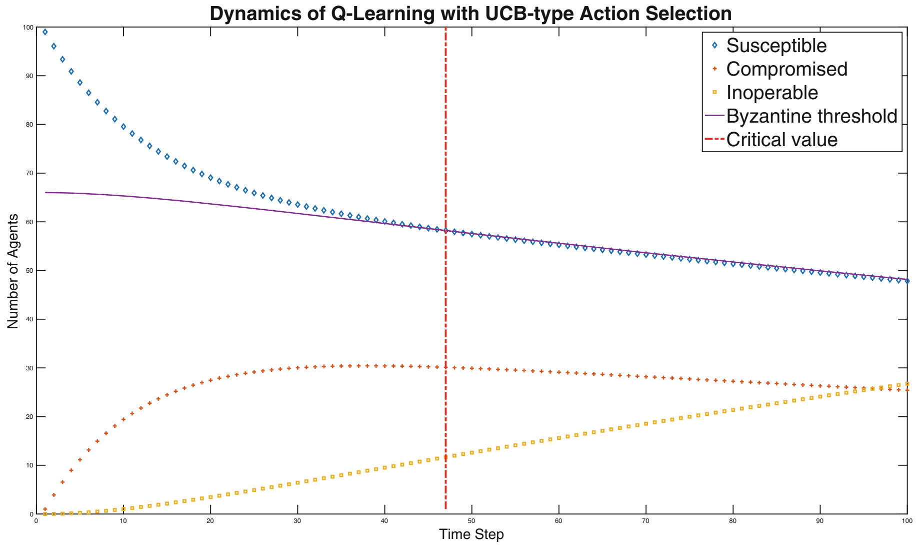

Fig. 1. This figure is typical of the kinds of simulation results from models of the tradeoffs between exploration and performance degradation due to attrition. Additional details and results can be found in [Cybenko 2021].

George Cybenko's research has been partially supported by ARO MURI Grant W911NF-13-1-042 and the US Air Force Research Laboratory. Roger A. Hallman is supported by the United States Department of Defense SMART Scholarship for Service Program funded by USD/R&E (The Under Secretary of Defense-Research and Engineering), National Defense Education Program (NDEP)/BA-1, Basic Research.

References

[Auer 2002] Auer, P.: Using confidence bounds for exploitation-exploration trade-offs. J. Mach. Learn. Res. **3**, 397–422 (2002)

[Brose2019] Brose, C.: The new revolution in military affairs: war's sci-fi future. Foreign Aff. **98**, 122 (2019)

[Campbell 2018] Campbell, A.M.: Enabling tactical autonomy for unmanned surface vehicles in defensive swarm engagements. PhD thesis, Massachusetts Institute of Technology (2018)

[Cybenko 2014] Cybenko, G., Jajodia, S., Wellman, M.P., Liu, P.: Adversarial and uncertain reasoning for adaptive cyber defense: building the scientific foundation. In: International Conference on Information Systems Security, pp. 1–8. Springer (2014)

[Cybenko 2021] George, C., Hallman, R.: Resilient distributed adaptive cyber-defense using blockchain. game theory and machine learning for cyber security, pp. 485–498 (2021)

[Silver 2016] Silver, D.: Mastering the game of Go with deep neural networks and tree search. Nature, **529**(7587), 484 (2016)

[Zhu et al. 2014] Zhu, M., Hu, Z., Liu, P.: Reinforcement learning algorithms for adaptive cyber defense against Heartbleed. In: Proceedings of the First ACM Workshop on Moving Target Defense, pp. 51–58 (2014)

Contents

Attack Detection

Malware Identification

Data Security in Distributed Systems

Applied Cryptography