Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS)

CPSWeek 2011

April 11, 2011
Chicago, Illinois
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>1</td>
</tr>
<tr>
<td>WELCOME MESSAGE</td>
<td>3</td>
</tr>
<tr>
<td>WORKSHOP OVERVIEW</td>
<td>4</td>
</tr>
<tr>
<td>WORKSHOP ORGANIZATION</td>
<td>5</td>
</tr>
<tr>
<td>TRUST CENTER OVERVIEW</td>
<td>6</td>
</tr>
<tr>
<td>KEYNOTE TALKS</td>
<td>7</td>
</tr>
<tr>
<td>WORKSHOP PAPERS</td>
<td>9</td>
</tr>
</tbody>
</table>

## WORKSHOP PAPERS

1. **Correlated Failures of Power Systems: The Analysis of the Nordic Grid**
   Martin Andreasson (Royal Institute of Technology, Sweden (KTH)), Saurabh Amin (University of California, Berkeley), Galina Schwartz (University of California, Berkeley), Karl Henrik Johansson (Royal Institute of Technology, Sweden (KTH)), Henrik Sandberg (Royal Institute of Technology, Sweden (KTH)), S. Shankar Sastry (University of California, Berkeley) .................................................................................................................... 9

2. **Resource Allocation Problems in Networked Cyber Physical Systems in Adversarial Scenarios**
   Sourabh Bhattacharya (University of Illinois at Urbana-Champaign), Ali Khanafer (University of Illinois at Urbana-Champaign), Tamer Basar (University of Illinois at Urbana-Champaign) ............................................................................................................................................. 18

3. **Enhancing Cyber-Physical Security through Data Patterns**
   Richard Chow (Palo Alto Research Center), Ersin Uzun (Palo Alto Research Center), Alvaro A. Cardenas (Fujitsu Laboratories of America), Zhexuan Song (Fujitsu Laboratories of America), Sung Lee (Fujitsu Laboratories of America) .................................................................................................................... 25

4. **Novel Reconfigurable Silicon Physical Unclonable Functions**
   Yingjie Lao (University of Minnesota, Twin Cities), Keshab K. Parhi (University of Minnesota, Twin Cities) ...................................................................................................................................... 30

5. **Verification of Information Flow Properties in Cyber-Physical Systems**
   Bruce McMillin (Missouri University of Science and Technology), Ravi Akella (Missouri University of Science and Technology) .................................................................................................................................. 37

6. **Secure Data Transmission against False Data Injection Attacks in Wireless Sensor Networks**
   Yilin Mo (Carnegie Mellon University), Bruno Sinopoli (Carnegie Mellon University) ........................................................................................................................................... 41

   Quanyan Zhu (University of Illinois at Urbana-Champaign), Tamer Basar (University of Illinois at Urbana-Champaign) ..................................................................................................................................... 47
TABLE OF CONTENTS (cont.)

Management of Control System Information Security: Control System Patch Management
Quanyan Zhu (University of Illinois at Urbana-Champaign), Miles McQueen (Idaho National Laboratory), Craig Rieger (Idaho National Laboratory), Tamer Basar (University of Illinois at Urbana-Champaign) ................................................................................................................... 51

Secure Routing in Smart Grids
Quanyan Zhu (University of Illinois at Urbana-Champaign), Dong Wei (Siemens Corporation), Tamer Basar (University of Illinois at Urbana-Champaign) ....................................................................... 55
WELCOME MESSAGE

On behalf of the Workshop Program Committee, it is our pleasure to welcome you to the Workshop on Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS) in conjunction with CPSWeek 2011 in Chicago, Illinois.

This workshop will bring together novel concepts and theories that can help in the development of the science of dependable and secure cyber-physical systems (CPS). These systems govern the operation of critical infrastructures such as power transmission, water distribution, transportation, healthcare, building automation, and process control. The use of internet-connected devices and commodity IT solutions and the malicious intents of hackers and cybercriminals have made these systems vulnerable. Despite attempts to develop guidelines for the design and operation of security policies, much remains to be done to achieve a principled, science-based approach to enhance security, trustworthiness, and dependability of control systems.

The workshop will focus on system theoretic approaches to address fundamental challenges to make CPS secure, dependable, and trustworthy, with a particular emphasis given to control and verification challenges arising as a result of complex interdependencies between these networked systems. In doing so, the workshop will serve as a first step toward the development of a principled approach to high-confidence CPS.

We greatly appreciate your participation and hope you find the workshop informative.

Sincerely,

The Workshop Steering Committee

Helen Gill, Ph.D.  Brad Martin
National Science Foundation National Security Agency

S. Shankar Sastry, Ph.D. Janos Sztipanovits, Ph.D.
University of California, Berkeley Vanderbilt University
WORKSHOP OVERVIEW

The Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS) will focus on system theoretic approaches to address fundamental challenges to make cyber-physical systems (CPS) secure, dependable, and trustworthy. A particular emphasis will be given on the control and verification challenges arising as a result of complex interdependencies between these networked systems. In doing so, the workshop will serve as a first step toward the development of a principled approach to high confidence CPS.

The main aim of this workshop is to bring together novel concepts and theories that can help in the development of the science of dependable and secure cyber-physical systems. This workshop also aims to foster collaborations between researchers from the fields of control and systems theory, embedded systems, game theory, software verification and formal methods, and computer security. The scope of this workshop is to discuss theories and methodologies that encompass ideas from:

- Fault-tolerant and networked control systems
- Game theory for multi-agent dynamics in uncertain environments, and
- Learning and verification theory for secure and trustworthy systems.

Topics of interest will include, but are not restricted to, the following:

- Taxonomy of attacks and attack models for control systems
- Novel security challenges in control systems
- Testbeds for security of critical infrastructure systems
- Decision and game theoretic approaches to security analysis
- Design architectures for prevention and resilience against attacks
- Risk assessment and verification of security properties
- Detectability and diagnosis of attacks
- Economics based studies of security and reliability
- Resilience and robustness against attacks
- Response and reconfiguration methods
- Cyber awareness of human-centric systems
- Complexity and resilience in control systems

Approaches that can be applied to particular critical infrastructure systems in Transportation (surface and aviation), Energy (smart grid and building energy management), and Healthcare (medical systems and associated embedded devices) are particularly welcomed. Also welcomed is foundational work that cuts across multiple application areas or advances the scientific understanding of underlying principles for the development of secure and trustworthy systems, including ways to measure the security properties of a system and methods to conduct robust and repeatable experimentation.
WORKSHOP ORGANIZATION

STEERING COMMITTEE
- Helen Gill (National Science Foundation)
- Brad Martin (National Security Agency)
- Shankar Sastry (University of California, Berkeley)
- Janos Sztipanovits (Vanderbilt University)

PROGRAM COMMITTEE
- Tamer Basar (University of Illinois at Urbana-Champaign)
- Michael Chertkov (Los Alamos National Laboratory)
- Richard Chow (PARC)
- John Chuang (University of California, Berkeley)
- George Cybenko (Dartmouth College)
- Anupam Datta (Carnegie Mellon University)
- Karl Henrik Johansson (Royal Institute of Technology, Sweden)
- Gabor Karsai (Vanderbilt University)
- Rupak Majumdar (University of California, Los Angeles)
- Radha Poovendran (University of Washington)
- Craig Rieger (Idaho National Laboratory)
- Galina Schwartz (University of California, Berkeley)

WORKSHOP ORGANIZERS
- Saurabh Amin (University of California, Berkeley)
- Katie Dey (PRO-telligent)
- Frankie King (PRO-telligent)
- Larry Rohrbough (University of California, Berkeley)
TRUST CENTER OVERVIEW

The Team for Research in Ubiquitous Secure Technology (TRUST) is focused on the development of cyber security science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure. Established as a National Science Foundation Science and Technology Center (STC), TRUST is addressing technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.

TRUST activities are advancing a leading-edge research agenda to improve the state-of-the-art in cyber security; developing a robust education plan to teach the next generation of computer scientists, engineers, and social scientists; and pursuing knowledge transfer opportunities to transition TRUST results to end users within industry and the government.

TRUST is addressing technical, operational, privacy, and policy challenges via interdisciplinary projects that combine fundamental science and applied research to deliver breakthrough advances in trustworthy systems in three “grand challenge” areas:

- **Financial Infrastructures** – Creation of a trustworthy environment that links and supports commercial transactions among financial institutions, online retailers, and customers.

- **Health Infrastructures** – Technology that advances “Healthcare Informatics” to enable engaged patients, personalized medicine, providers as coach-consultants, and agile evidence-based care.

- **Physical Infrastructures** – Advances that support Next Generation Supervisory Control and Data Acquisition (SCADA) and control systems, including power, water, and telecommunications.

TRUST is led by the University of California, Berkeley with partner institutions Carnegie Mellon University, Cornell University, San Jose State University, Stanford University, and Vanderbilt University. TRUST projects have a holistic view that addresses computer security, software technology, analysis of complex interacting systems, and economic, legal, and public policy issues. As such, TRUST draws on researchers in such diverse fields as Computer Engineering, Computer Science, Economics, Electrical Engineering, Law, Public Policy, and the Social Sciences.

More information on TRUST is available at [http://www.truststc.org](http://www.truststc.org).
KEYNOTE TALKS

Cyber-Security Analysis and Resilient Control Design for Infrastructure Systems
S. Shankar Sastry (University of California, Berkeley)

ABSTRACT: The extensive use of information and communication technologies raises concerns about the vulnerabilities of critical infrastructure systems to both random failures and security attacks. Cyber-security of Supervisory Control and Data Acquisition (SCADA) systems is especially important, because they are employed for sensing and control of large physical infrastructures. This work focuses on the design of novel control methods and security mechanisms for infrastructure systems, and applies them to water distribution, process control, and energy management systems. The talk will discuss the progress made in following research areas: (1) security threat assessment, (2) model-based attack diagnosis, and (3) resilient control design. First, cyber-security assessment for SCADA systems will be performed based on well-defined attacker and defender objectives. The mathematical model of SCADA systems considered in this work has two control levels; i.e., regulatory control using distributed proportional-integral controllers, and supervisory fault diagnosis based on approximate dynamical system models. Second, design of attack diagnosis schemes that incorporate the knowledge of physical dynamics of the system will be presented. The performance of these schemes on a class of deception attacks will be described. Third, some fundamental limits on the closed-loop performance of networked control systems, and their implications to security of SCADA systems will be discussed. Finally, the necessity of security mechanisms which account for these limits and the presence of interdependent risks will be justified using a game-theoretic model.

BIOGRAPHY: S. Shankar Sastry is the Dean of Engineering and Roy W. Carlson Professor of Engineering at the University of California, Berkeley. He helped establish and is Director of TRUST (Team for Research in Ubiquitous Secure Technology), an NSF Science & Technology Center and is Faculty Director of the Blum Center for Developing Economies. He was Director of CITRIS, Chair, Department of Electrical Engineering and Computer Sciences, UC Berkeley, Director, DARPA Information Technology Office, and Director, UC Berkeley Electronics Research Laboratory. Dr. Sastry received his Ph.D. degree in 1981 from the University of California, Berkeley. He was on the faculty of MIT as Assistant Professor from 1980-82 and Harvard University as a chaired Gordon McKay professor in 1994. His areas of research are embedded control especially for wireless systems, cybersecurity for embedded systems, critical infrastructure protection, autonomous software for unmanned systems (especially aerial vehicles), computer vision, nonlinear and adaptive control, control of hybrid and embedded systems, and network embedded systems and software. He has coauthored over 450 technical papers and 9 books and served as Associate Editor for numerous publications, including: IEEE Transactions on Automatic Control; IEEE Control Magazine; IEEE Transactions on Circuits and Systems; the Journal of Mathematical Systems, Estimation and Control; IMA Journal of Control and Information; the International Journal of Adaptive Control and Signal Processing; Journal of Biomimetic Systems and Materials. He is currently an Associate Editor of the IEEE Proceedings. Dr. Sastry was elected into the National Academy of Engineering in 2001 and the American Academy of Arts and Sciences (AAAS) in 2004 and made a Fellow of the IEEE in 1994. He received the President of India Gold Medal in 1977, the IBM Faculty Development award for 1983–1985, the NSF Presidential Young Investigator Award in 1985, the American Automatic Control Council Eckman Award in 1990, the Distinguished Alumnus Award of the Indian Institute of Technology in 1999, the David Marr prize for the best paper at the International Conference in Computer Vision in 1999, the Ragazzini Award for Distinguished Accomplishments in teaching in 2005, and the C.L. Tien Award for Academic Leadership in 2010. He was awarded an M. A. (honoris causa) from Harvard in 1994 and an honorary doctorate from the Royal Institute of Technology, Sweden in 2007. Dr. Sastry has been a member of the Air Force Scientific Advisory Board from 2002-2005 and the Defense Science Board in 2008, he is on the corporate boards of Crossbow, Inc. and C3-Carbon, LLC, and has supervised over 60 doctoral students and over 50 M.S. students to completion.

Dependable and Secure Automotive Cyber-Physical Systems
William P. Milam (Ford Motor Company)

ABSTRACT: Recently a workshop was help in Michigan to discuss Developing Dependable and Secure Automotive Cyber-Physical Systems from Components. The goal of this workshop was to address emerging...
challenges relative to reliability, availability, safety, and security attributes of software-intensive electronic automotive control systems and road infrastructure systems. An example of such a system would be a self-driving vehicle that must adapt in order to navigate safely and efficiently through traffic in the presence of intersections, pedestrians and other traffic. Another example would be an emergency vehicle with advanced engine and transmission controls integrated with stability control that is able to instantly respond to driver input and road conditions and keep the vehicle in the lane while traversing a curve in icy conditions. We will provide an early report out of the proceedings from that workshop as well as proposed actions and timetables.

BIOGRAPHY: William Milam is a Technical Expert at the Ford Research and Innovation Center, Ford Motor Company. His research addresses modeling and implementation of advanced technology automotive powertrains for improved fuel economy and emissions, through improvements in systems engineering processes for the design of automotive embedded systems. He is a senior member of the IEEE and a member of the SAE. Mr. Milam is a member of the SAE Electronic Design Automation Standards Committee, the SAE Architecture Analysis and Design Language Standards Committee, and chairs the SAE Model Based Embedded System Engineering Task Force. He is also the chair of the USCAR Cyber-Physical Systems Task Force.

Trustworthy Computing and Cyber-Physical Systems
Sam Weber (National Science Foundation)

ABSTRACT: This talk will discuss research challenges in the intersection of Trustworthy Computing and Cyber-Physical Systems. Both research communities have had long, mostly independent, histories despite their obvious common goal of building systems that humans can depend upon. As a result, collaboration between communities results in discovering interesting challenges, possible misunderstandings, and sometimes unexpected benefits.

BIOGRAPHY: Sam Weber is a Program Director for the National Science Foundation’s Trustworthy Computing Program. He received his M.Sc. from the University of Toronto, and his Ph.D. from Cornell University.

Gaps Between Traditional and CPS Security
Janos Sztipanovits (Institute for Software Integrated Systems, Vanderbilt University)

ABSTRACT: Security requirements are traditionally enumerated in terms of confidentiality, integrity, and availability. In CPS, security is integral part of the resilience and dependability requirements that intend to ensure critical functions at all times, despite damage caused by accidental faults, errors, and degradations in the physical plant or malicious intrusions in the computer control system and network. Tradeoff among autonomy, performance, resilience and dependability is complex and need to be approached holistically. If increased complexity brought about by advanced CPS automation leads to brittleness, instability, malfunctions, or vulnerability, the benefits will not be realized and the approach may fail. Achieving resilience to physical faults and cyber attacks in CPS requires an integrated suite of technologies. Current approaches are compartmentalized, not prepared for operating in a complex, highly coupled cyber-physical environment, and cannot take advantage of commonalities in solutions. Fault-tolerant control systems typically assume well-understood models and bounds on the nature of faults in system operation. Intrusion detection systems are rarely used in CPS, and cyber security considerations are largely neglected. Integration of functional, fault management and security architectures are missing even in safety critical industrial automation systems and military systems. In computing systems, fault-tolerance focuses on faults in the hardware or software infrastructure, not on the system-wide impact of these faults. Introducing privacy considerations in system design is a largely unsolved problem. This talk will explore these challenges and discuss research directions that may yield solution.

BIOGRAPHY: Dr. Janos Sztipanovits is the E. Bronson Ingram Distinguished Professor of Engineering at Vanderbilt University. He is founding director of the Institute for Software Integrated Systems (ISIS). His research areas are at the intersection of systems and computer science and engineering. His current research interest includes the foundation and applications of model-based methods for the design of Cyber Physical Systems.
Correlated Failures of Power Systems: Analysis of the Nordic Grid

M. Andreasson*, S. Amin†, G. Schwartz †, K. H. Johansson*, H. Sandberg* and S. S. Sastry†
*ACCESS Linnaeus Center, Royal Institute of Technology, Stockholm, Sweden. {mandreas, kallej, hsan}@kth.se
†TRUST Center, University of California, Berkeley. {saurabh, schwartz, sastry}@eecs.berkeley.edu

Abstract—In this work we have analyzed the effects of correlated failures of power lines on the total system load shed. The total system load shed is determined by solving the optimal load shedding problem, which is the system operator’s best response to a system failure. We have introduced a Monte Carlo based simulation framework for estimating the statistics of the system load shed as a function of stochastic network parameters, and provide explicit guarantees on the sampling accuracy. This framework has been applied to a 470 bus model of the Nordic power system and a correlated Bernoulli failure model. It has been found that increased correlations between Bernoulli failures of power lines can dramatically increase the expected value as well as the variance of the system load shed.

I. INTRODUCTION

Power systems are among the largest and most complex systems created by mankind. The complexity of power grids keeps increasing as power grids are expanded and new functionalities are added, as with the current developments of the SmartGrid [1]. Since many vital parts of today’s society require reliable supply of electricity, the reliable and secure operation of power systems is indisputably essential [2], [3]. We give a brief overview of the research in the two distinctive areas of security against adversarial attacks and reliability of power systems against random failures. We conclude that correlated failures in power systems represent a gap between these two research areas.

In the area of security, research on characterizing optimal attack and defense strategies has gained momentum over the past years. In [4] the optimization problem of maximizing the power outage, for a given number of power transmission lines that an adversary is capable of disconnecting, is considered. The system operator is assumed to take the best action to minimize the damage in form of compulsory load shedding. The problem is game theoretic by nature and gives rise to a maximin optimization problem, where the outer maximization seeks the most disruptive attack for a given budget of the adversary, and the inner minimization solves the optimal load shedding problem which minimizes the consequences of an attack. Because of the non-convexity and the existence of integer variables, the problem is inherently hard to solve for large systems. [5] approximates the nonlinear mixed integer bi-level program by a mixed integer linear program, and derives an upper bound on the severity of adversarial attacks.

Traditionally, the reliability of power systems has often been characterized by deterministic means, such as the widely uses $N - k$ criterion [6], and in almost all cases $k = 1$ is used [7]. A power system satisfying the $N - k$ criterion is able to withstand any contingency consisting of $k$ outages. The main drawback of the $N - k$ criterion and other deterministic reliability criteria is that they do not take into account the probabilities of the contingencies. Furthermore, the number of events which have to be considered when evaluating the $N - k$ criterion grows exponentially in $k$, making the reliability evaluation computationally intractable. More recent research on the reliability of power systems has emphasized that many events governing the reliability of power systems are by nature stochastic, e.g. demands and generation capacities. Various statistical and sampling based methods for evaluating the reliability of power systems have been developed to analyze stochastic phenomena in power systems [8], [9]. In [10] a two state Markov model for the failure of various power system elements is considered, and the statistics of the power system are calculated using Monte Carlo techniques. However, the model does not take correlated failures into account. Other than failure correlations due to cascading failures [11], we found no model which attempts to model correlated failures in power systems.

This work aims at studying the effects of correlations between failures of power system components, and in particular power lines. In contrast to previous papers on the subject, we introduce a failure model explicitly taking into account correlated system failures. We evaluate the impact of correlations of failures by the covariances between the failures. Our research is motivated by the increased deployment of off-the-shelf hardware and software in SCADA systems governing the power systems. When similar or even identical
software is deployed in several system components, software failures are likely to be correlated between those components. Indeed, current literature suggests that bugs present in one system component are likely to also be present in a similar or identical components [12]. From a cyber security point of view, this work is motivated by the possibility of malicious code exploiting identical software bugs and security flaws. A computer virus spreading in the SCADA network is likely to affect multiple of its target components, and thus causing correlations between failures. The increased interconnection of control and communication systems as well as their connection to the Internet, facilitates the exploitation of software bugs. There are indications that software bugs caused failures leading to a blackout in the northeast blackout of 2003 [13]. We believe that correlated failures provides a good mean of understanding the affects of failures caused by malicious software affecting multiple system components. Correlated failures may also occur due to natural disasters such as earthquakes or hurricanes [14], [15]. Examples of major power system outages caused by natural disasters include the New York city blackout in 1977, where lightning struck a substation and a power line almost simultaneously [16].

We measure the impact of a system failure by the minimal system load shed required to restore the system to a safe state. This formulation gives rise to an optimization problem, which under simplified conditions can be made linear. For different values of the correlations of the failure distribution, we compute the sampled statistics of the total system load shed by Monte Carlo techniques, and provide guarantees on the convergence rate of the sampled statistics. In particular, we use a weighted sum of the mean and variance of the total system load shed as a risk measure of the failure statistics. To obtain statistical data from a realistic power system, we apply our techniques to a 470 bus model of the Nordic power system, acquired from publicly available sources. We have found that increasing correlations between Bernoulli failures of power lines lead to increased expected value and variance of the system load shed under various topological structures of the correlations.

The rest of the paper is organized as follows. In section II the optimal load shedding problem is presented and the total system load shed is defined. In section III a novel model of the Nordic power system is presented and evaluated. In Section IV a Monte Carlo sampling technique is presented and the effects of correlated failures on the Nordic power system are studied, followed by concluding remarks in Section V.

II. OPTIMAL LOAD SHEDDING

Optimal power flow (OPF) problems are in many ways analogous to transportation problems, with the only difference that the power flows obey the Kirchoff voltage law, and are proportional to the relative phase angle difference between the buses [17]. The optimal load shedding problem is a special case of OPF problems, where the load shed is minimized subject to physical constraints [18], [19]. OPF problems have been solved using a variety of optimization techniques, ranging from linear programming [20], Newton methods [21] to interior point methods [22]. While many techniques rely on the linearized power flow equations, there are OPF problems using the nonlinear power flow equations [23], [24]. While showing promising results, these methods suffer from general limitations of non-convex optimization such as convergence and computational complexity.

We will only consider the linearized power flow equations in our work, thereby ensuring robust and fast convergence. Since we will apply Monte Carlo techniques solving the optimal load shedding problem, computation speed is certainly of importance. By assuming that the admittance in the shunt branch of the power lines is negligible, and that the resistance-to-reactance ratio is sufficiently small, reactive power flows can be neglected, and the real power real power flows are described by the DC-model [25]:

\[ P^{\text{line}} = V^{\text{line}} B \sin (A \theta) \]  

where \( P^{\text{line}} \) is a column vector of active power flows in the transmission lines, \( V^{\text{line}} = \text{diag}(V_i V_j) \) where \( V_i \) is the voltage of bus \( i \), \( B = \text{diag}(b_{ij}) \) where \( b_{ij} \) is the admittance of the power line connecting bus \( i \) with bus \( j \), \( \theta \) is the vector of bus phase angles and \( A \) is the vertex-edge incidence matrix of the graph of the power system, defined as \( A_{ij} = 1 \) iff \( e_i = (v_j, u) \in E \), \( A_{ij} = -1 \) iff \( e_i = (u, v_j) \in E \) and \( A_{ij} = 0 \) otherwise. Here \( \sin(x) = [\sin(x_1), \ldots, \sin(x_n)]^T \) for a vector \( x \). By only considering sufficiently small phase angle differences, i.e. \( \Delta \theta_{\text{max}} = \|A \theta\|_\infty \) being sufficiently small, we may linearize (1) around \( A \theta = 0 \):

\[ P^{\text{line}} = V^{\text{line}} B A \theta \]  

By summing the power flows to each bus, we get the linearized equation for the net power flows into the buses:

\[ P = A^T V^{\text{line}} B A \theta =: L_B \theta \]

where \( P \) is a vector of real power injections to the buses. \( L_B \) can be interpreted as a weighted Laplacian matrix of the graph associated with the power system, with weights corresponding to the line admittances times the bus voltages. We may assume, wlog, that the buses of the power system are partitioned as \( P = [P_g^T, P_l^T]^T \), where \( P_g > 0 \) are generator buses and \( P_l \leq 0 \) are load buses. We consider the optimization problem of minimizing the total load shed of the system. The optimal load shedding problem can, for the linearized power flow equations, be formulated as a linear Program...
production node
400 kV power line
300 kV power line
220 kV power line
132 kV power line

Demand node

The voltage of the power lines and the number of parallel buses, the connectivity of the buses through power lines, were obtained from the respective TSOs websites. The power lines and HVDC links in the Nordic countries are public sources. To compensate for the lack of available data of power plants with generation capacity less than 100 MW, we have made assumptions about the remaining power plants. The remaining thermal power plants are assumed to be located in populated areas, and hence the thermal generation capacity is proportional to the demands. As for the remaining wind power capacity, we have assumed that the wind power generation is uniformly distributed over the land surface, and hence over the buses. These assumptions may appear crude, but considering that these assumptions only apply to power plants whose generation capacity is below 100 MW, the net effect of possible errors on the whole model is of minor importance.

A. Obtaining the network topology

The topology of the power system, i.e. the geographical positions of the main 400, 300, 220 and 132 kV power lines and HVDC links in the Nordic countries were obtained from the respective TSOs websites. The data obtained included the coordinates of the power buses, the connectivity of the buses through power lines, the voltage of the power lines and the number of parallel power lines, if applicable. The complete model has a total of 470 buses and 717 power lines. The power lines and buses of the Nordic power grid are illustrated in figure 1.

B. Estimating power generation capacities

Information about all power generation facilities with capacities of at least 100 MW were also acquired from public sources [27]. To compensate for the lack of available data of power plants with generation capacity less than 100 MW, we have made assumptions about the remaining power plants. The remaining thermal power plants are assumed to be located in populated areas, and hence the thermal generation capacity is proportional to the demands. As for the remaining wind power capacity, we have assumed that the wind power generation is uniformly distributed over the land surface, and hence over the buses. These assumptions may appear crude, but considering that these assumptions only apply to power plants whose generation capacity is below 100 MW, the net effect of possible errors on the whole model is of minor importance.

C. Estimating power demand data

There is no available electricity demand data, other than cumulative data for the Nordic countries. This data is too rough to be useful for our 470 bus model. Following [26] we have used population census data to estimate the
power demand. This methodology relies on the assumptions that household power demand is proportional to the population connected to a substation, as well as industry power demand, since the workforce will settle relatively close to industries. This may however not necessarily be the case for certain energy-intensive industries which are usually co-located with energy sources, nor for certain location-specific industries such as forestry or the oil industry. Population statistics were collected from the Bureau of Statistics of the respective countries. We have collected cumulated population statistics for the major administrative regions of each country, and assumed that the population (and hence the demand) is distributed uniformly over the load buses within each region. The number of administrative regions in each country was between 12 and 21. Using smaller regions would introduce difficulties in assigning the right population to each substation. To estimate the power demands, both the yearly average and yearly maximum of the daily maximum power consumption were used to create two different load situations.

D. Estimating power line parameters

The only known parameters of the power lines obtained from public sources are the line voltages. To solve the optimal load shedding problem, also the line admittances as well as the maximum transmission capacities of each line need to be known. The admittance of power lines can be estimated by the length of the power line. Typically the reactance of high voltage power transmission lines is approximately 0.20 Ω/km [28]. The lengths of a power line from a bus with coordinates \( x \) to a bus with coordinates \( y \) is estimated by the euclidean 2-norm as \( l = \text{dist}(x, y) = ||x - y||_2 = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \) which is always an underestimate of the actual line length. As for estimating transmission capacities, only cross-border transmission line capacity constraints are available from the Nordic TSOs. The transmission capacity of each power line of equal voltage is assumed to be the average transmission capacity of the cross-border lines, which are shown in Table I.

<table>
<thead>
<tr>
<th>Voltage</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>400 kV</td>
<td>1080 MW</td>
</tr>
<tr>
<td>300 kV</td>
<td>650 MW</td>
</tr>
<tr>
<td>220 kV</td>
<td>415 MW</td>
</tr>
<tr>
<td>132 kV</td>
<td>143 MW</td>
</tr>
</tbody>
</table>

E. Evaluating the model

The optimal load shedding problem was applied to the previously derived model of the Nordic power transmission grid. By using the YALMIP [29] interface with the GLPK [30] LP solver in MATLAB [31], the optimal load shedding problem was solved. When solving the linear optimal load shedding problem with the yearly maximum loads, the total system load shed was found to be 2% of the total power demand. When solving the optimal load shedding problem with the yearly average of the daily maximum loads, no system load shed was necessary. This demonstrates that our model is indeed usable for our study.

IV. Statistics of power system failures

A. Monte Carlo methods

In this paper we will consider stochastic failures of the power system, as in e.g. [8], [9]. To demonstrate the generality of our methods, we will not yet make any assumptions about these failures. Consider the matrices \( C \) and \( d \), associated with an arbitrary power system, as random variables endowed with a probability measure \( \mu^C \times \mu^d \). Since both the topology and load parameters of the power system are determined by \( C \) and \( d \), such a probability measure can represent any type of failures of the power system. It can be shown that for any probability measure \( \mu^C \times \mu^d \), the minimum total load shed \( S^*(C, d) \) is also a random variable. The total load shed is a commonly used measure of the severeness of a power system outage [32], [33].

We will consider the sampled probability distribution of the minimum total system load shed \( S^*(C, d) \), and in particular we will consider the mean and the variance of the sampled probability distribution. Because \( 0 \leq S^*(C, d) \leq -\sum P_i^d \), as seen from (4), the mean \( S^* \) and variance \( \sigma^2_{S^*} \) of \( S^*(C, d) \) always exist and are finite. We will use \( S^* + \alpha \cdot \sigma_{S^*} \), \( \alpha \in \mathbb{R}^+ \) as a risk measure for the distribution \( \mu^C \times \mu^d \). We show that \( S^* + \alpha \cdot \sigma_{S^*} \) is closely related to the commonly used risk measure value at risk (VaR), which for a random variable \( S^* \) is defined as follows [34]:

\[
\text{VaR}_\alpha(S^*) = \text{inf}\{l \in \mathbb{R} : \Pr(S^* > l) \leq 1 - \alpha\}
\]

The intuition of the expression \( \text{VaR}_\alpha(S^*) \) is that the maximum loss, in our case system load shed, is bounded by \( \text{VaR}_\alpha(S^*) \) with probability \( 1 - \alpha \). One serious computational drawback with using VaR on sampled probability distributions, is that it requires knowledge of the full probability distribution of the random variable \( S^* \). When dealing with samples of random variables, estimating VaR becomes hard since it requires estimation of the tail of the distribution \( S^* \). The following proposition allows us to obtain an upper bound \( \text{VaR}_\alpha(S^*) \) using a linear combination of the mean and the variance of \( S^* \), which can be estimated more robustly:

**Proposition 1.** The risk measure value at risk (VaR\(_\alpha\)) satisfies

\[
\text{VaR}_\alpha(S^*) \leq \bar{S}^* + \frac{1}{\sqrt{\alpha}} \cdot \sigma_{S^*}.
\]
The proof is given in the appendix. Since obtaining analytical expressions for $\hat{S}^*$ and $\sigma_{\hat{S}}^2$, is in general not possible, we will use Monte Carlo techniques [35] to estimate the mean and the variance of the load shed. By drawing $N$ samples from the distribution $\mu^C \times \mu^d$, we obtain the following approximations of $\hat{S}^*$ and $\sigma_{\hat{S}}^2$:

$$\hat{S}^* \approx \frac{1}{N} \sum_{i=1}^{N} S^*(C_i, d_i)$$

$$\sigma_{\hat{S}}^2 \approx \frac{1}{N-1} \sum_{i=1}^{N} (S^*(C_i, d_i) - \hat{S}^*)^2$$

(8)

(9)

Due to $S^*(C, d)$ being bounded, $\hat{S}^*$ and $\sigma_{\hat{S}}^2$ are guaranteed to converge to $S^*$ and $\sigma_{S^*}$ respectively.

**Proposition 2.** Given $\epsilon > 0$, $\delta > 0$, the number of samples $N_1$ and $N_2$ which assure that

$$\Pr \left[ \left| \hat{S}^* - S^* \right| \leq \epsilon \right] \leq \delta$$

$$\Pr \left[ \left| \sigma_{\hat{S}} - \sigma_{S^*} \right| \leq \epsilon \right] \leq \delta$$

are

$$N_1 \geq \frac{\hat{S}_2^2}{4\delta^2 \epsilon^2}$$

$$N_2 \geq \frac{\hat{S}_4^2}{8\delta \epsilon^4}$$

Proof: Follows by lemma 3 and lemma 5 in the appendix, and the fact that $0 \leq S^*(C, d) \leq -\sum P_i^d$. 

With proposition 2 we have guaranteed bounds of the estimation error of both the sampled expected value and the sampled variance of the load shed. The proposition can of course be used in the reverse direction. For given $N_1$ and $N_2$, we can obtain bounds on $\delta$ and $\epsilon$. With these explicit bounds on the error of the estimated mean and variance of the load shed, the number of samples can be chosen according to given accuracy requirements, and trade-offs between accuracy and the number of samples can be made a priory.

**B. Sampling of correlated system failures**

In this section we examine the effects of correlated system faults on the statistics of the minimum total system load shed. As discussed in the introduction, the study of correlated faults in power systems is motivated by the increased deployment of off-the-shelf hardware and software in SCADA systems governing the power systems. When identical software is deployed in several system components, software faults between these identical components are likely to experience correlation. In the following empirical study we will consider failures on the form of power line disconnections. We model the disconnection of power line $i$ as a binary random variable $X_i \in \{0, 1\}$ where $X_i = 0$ corresponds to line $i$ being fully functional with all parameters set to default, and $X_i = 1$ corresponds to line $i$ being disconnected. Thus, the failure statistics of the power system are given by

$$P(X_1 = Y_1, \ldots, X_{n_p} = Y_{n_p}) \forall Y_i \in \{0, 1\}$$

Since parameterizing the full joint Bernoulli distribution would require $n^{n_p} \approx 10^{216}$ variables, we will consider the Bernoulli distribution with the first two central moments given explicitly, i.e.

$$\bar{X}_i = E[X_i] \forall i \in \{1, \ldots, n_p\}$$

$$\sigma_{ij} = E[(X_i - \bar{X}_i)(X_j - \bar{X}_j)] \forall (i, j) \in \{1, \ldots, n_p\}^2$$

To consider the effects of increasing correlations $\bar{X}_i = 0.02$ is kept constant, while the covariances $\sigma_{ij}$ are increased. We consider two different scenarios where the correlation between a subset of the power lines is increased.

1) Correlations between incident power lines: We first consider the case where $\sigma_{ij}$ is increased equally for all incident power lines, from 0 to 0.016 in steps of 0.004. For each step, 1000 Monte Carlo simulations are performed with the Bernoulli sampling algorithm described in [36] to acquire sampled statistics $S^*$. By proposition 2 the relative error of $\hat{S}^*$ is guaranteed to be less than 7% with certainty 95%. In figure 2, the histograms of the sampling processes are shown for different $\sigma_{ij}$, together with fitted Weibull distributions. The mean and the variance of the load shed for different correlations are shown in figure 4. Clearly both $\hat{S}^*$ and $\sigma_{X^*}$ are strongly increasing in $\sigma_{ij}$.
2) Correlations between power lines incident to PMUs: We here consider the scenario of failures being correlated only between lines incident to nodes with phasor measurement units (PMUs). This scenario is motivated by the use of identical software and hardware in PMUs, which could cause correlations between failures of these nodes, and hence the incident lines. In figure 5, the histograms of the sampling processes are shown for different $\sigma_{ij}$, together with fitted Weibull distributions. The mean and the variance of the load shed for different covariances are shown in figure 7. While $\sigma_X^*$ is not increasing in $\sigma_{ij}$, $S^*$ is increasing by a factor 15 with increasing $\sigma_{ij}$.

3) Remarks: Although simulations indicate that correlations increase the expected value of the system load shed, it is easy to find counterexamples where increased correlation between power line failures decreases the expected load shed. The simplest possible counterexample is a 3-bus and 2-line power network shown in figure 8. Let the demand bus have demand $-1$, and the generation bus a capacity $\bar{g} \geq 1$, and the line parameters be such that the demand is satisfied under
normal operation. It can be shown that the expected load shed of the system is $E[X_1] + E[X_2] - \sigma_{12}$, where $\sigma_{12}$ is the covariance between the failures of power lines $l_1$ and $l_2$. The intuition behind this counterexample is that while the probability of both lines failing increases, the probability of each failing individually decreases, with the result that the total probability of any line failing decreases. We here state sufficient conditions under which increased correlations of power line failures imply increased expected load shed.

Proposition 3. Let the power system satisfy the $n - k$ criterion, i.e. the disconnection of any $k$ power lines does not induce any necessary load shedding. Furthermore, assume that all contingencies with at least $k + 1$ line failures induce a total system load shed $\bar{c}$. Assume, wlog, that the moment $\phi_1, \ldots, k+1 = E[X_1 \cdot \ldots \cdot X_{k+1}]$ increases by $\Delta \phi$, but all other moments $E[X_{i_1} \cdot \ldots \cdot X_{i_1}]$ are constant. Then

1) The central moment $\sigma_1, \ldots, k+1 = E \left[ (X_1 - X_1) \cdot \ldots \cdot (X_{k+1} - X_{k+1}) \right]$ also increases by $\Delta \phi$.
2) All other central moments of order less than or equal to $k + 1$ remain constant.
3) The expected load shed $\bar{S}^*$ increases by $\bar{c} \cdot \Delta \phi$.
4) If $E[X_i] < 1/2 \forall \phi$, the variance of the load shed, $\sigma_{S^*}$, increases by $\bar{c}^2 \cdot \Delta \phi$, where $0 < \bar{c} \leq \bar{c}$.

A proof is given in the appendix. The following corollary follows directly from proposition 3.

Corollary 1. Assume that all conditions of proposition 3 still hold, except that all contingencies with at least $k + 1$ line failures induce a system load shed of at least $\bar{c}$. In this case the results of proposition 3 hold instead for the lower bound $\bar{S}^* \leq S^*$ of the system load shed, which is the total system load shed assuming all line failures result in the same system load shed $\bar{c}$.

V. CONCLUSIONS AND FUTURE RESEARCH

In this work we have demonstrated that increased correlations between power line failures can dramatically increase the expected costs in terms of system load shed, although the expected value of the failure probabilities is kept constant. Furthermore we have demonstrated that increased correlations between power line failures can also increase the variance of the system load shed, thus increasing the risk of large system load sheds. We have demonstrated our results by the sampling of correlated power line failures, using a model of the Nordic power grid. We have furthermore provided sufficient conditions under which the mean and the variance of the total system load shed increase with increasing correlation between line failures.

The framework presented in this paper should be seen as a general framework for reliability evaluation of power systems where correlations are known a priori, either by empirical data or by improved failure models of power systems.

It should be clarified that the failures we consider do not correspond to cascading failures, but that they could represent potential causes of cascading failures. In many situations, cascading failures further aggravate the state of a partially failing power system, leading to even larger losses in terms of system load sheds. In future work, it would be of interest to consider the impact of correlated failures under power system on cascading failures. Also, it would be interesting to study if the conditions under which the expected value and the variance of the load shed are increasing in the correlations, can be relaxed.

REFERENCES

Appendix

Proof: (of proposition 1) Note that

\[ \text{Var}(X) = \frac{(b-a)^2}{4} \]

Proof: Consider the random variable defined by

\[ Y = X - \frac{a+b}{2} \]

By basic probability theory we have

\[ \text{Var}[X] = \text{Var}[Y] = \mathbb{E}[Y^2] - (\mathbb{E}[Y])^2 \]

\[ \leq \frac{(b-a)^2}{4} = \frac{(b-a)^2}{4} \]

Lemma 2. The variance of a random variable \( X \) with compact support \([a, b]\) is bounded by:

\[ \text{Var}[X] \leq \frac{(b-a)^2}{4} \]

Proof: Since the samples are iid, we have

\[ \text{Var}[\bar{X}_N] = \text{Var} \left[ \frac{1}{N} \sum_{i=1}^{N} X_i \right] = \frac{1}{N^2} \text{Var} \left[ \sum_{i=1}^{N} X_i \right] \]

\[ = \frac{N \sigma^2(X)}{N^2} \leq \frac{(b-a)^2}{4N} \]
By Chebyshev’s inequality we have
\[
\Pr \left\{ \left| \hat{X}_N - \bar{X} \right| \geq \epsilon \right\} \leq \frac{\text{Var} \left[ \hat{X}_N \right]}{\epsilon^2} \leq \frac{(b - a)^2}{4Ne^2} \leq \delta
\]

**Lemma 4.** Let \( \hat{\sigma}_{X_N} = \frac{1}{N} \sum_{i=1}^{N} (X_i - \hat{X}_N)^2 \) be the sampled variance of the random variable \( X \) with \( N \) samples. Let \( X \) have compact support on \([a, b]\), then for any given \( \epsilon > 0 \), \( \delta > 0 \)

\[
\Pr \left[ \left| \hat{\sigma}_{X_N} - \sigma_X \right| \geq \epsilon \right] \leq \delta
\]

for
\[
N \geq \left[ \frac{(b - a)^4}{8\delta e^4} \right]
\]

**Proof:** By [37], the variance of the sampled variance is given by
\[
\text{Var} \left[ \hat{\sigma}_{X_N} \right] = \frac{2\sigma_X^4}{N}
\]
By lemma 2, the variance \( \text{Var}[X] = \sigma_X^2 \) is bounded by
\[
\sigma_X^2 \leq \frac{(b - a)^2}{4}
\]
Thus, by Chebyshev’s inequality
\[
\Pr \left[ \left| \hat{\sigma}_{X_N} - \sigma_X \right| \geq \epsilon \right] \leq \frac{\text{Var} \left[ \hat{\sigma}_{X_N} \right]}{\epsilon^2} \leq \frac{(b - a)^4}{8Ne^2} \leq \delta
\]

**Lemma 5.** Given \( \epsilon > 0 \), \( \delta > 0 \), we have for a random variable \( X \) with compact support on \([a, b]\)

\[
\Pr \left[ \left| \hat{\sigma}_X - \sigma_X \right| \geq \epsilon \right] \leq \delta
\]

for
\[
N \geq \left[ \frac{(b - a)^4}{8\delta e^4} \right]
\]

**Proof:** By concavity of \( \sqrt{\cdot} \), Chebyshev’s inequality and lemma 4
\[
\Pr \left[ \left| \hat{\sigma}_X - \sigma_X \right| \geq \epsilon \right] \leq \Pr \left[ \left| \hat{\sigma}_{X_N} - \sigma_X \right| \geq \epsilon \right] \leq \frac{\text{Var} \left[ \hat{\sigma}_{X_N} \right]}{\epsilon^2} \leq \frac{2\sigma_X^4}{N^2} \leq \frac{(b - a)^4}{8Ne^2} \leq \delta
\]

**Proof:** (of proposition 3) The first part follows directly, since:
\[
\sigma_{1, \ldots, k+1} = E \left[ (X_1 - \bar{X}_1) \cdots (X_{k+1} - \bar{X}_{k+1}) \right] = E \left[ X_1 \cdots X_{k+1} \right] - \bar{X}_1 \cdot E \left[ X_2 \cdots X_{k+1} \right] + \cdots + (-1)^{k+1} \cdot \bar{X}_1 \cdots \bar{X}_{k+1}
\]

The second part also follows directly by calculation. Wlog, consider
\[
\sigma_{1, \ldots, l} = E \left[ (X_1 - \bar{X}_1) \cdots (X_l - \bar{X}_l) \right] = E \left[ X_1 \cdots X_l \right] - \bar{X}_1 \cdot E \left[ X_2 \cdots X_l \right] + \cdots + (-1)^l \cdot \bar{X}_1 \cdots \bar{X}_l
\]
which is constant for all \( l \leq k \) by the assumption that all other moments \( E[X_1 \cdots X_l] \) are constant.
As for the third part, let \( k = 1 \) and consider a network with 3 power lines. The expected value of the system load shed is:
\[
\bar{c} \cdot (Pr[X_1 = 1, X_2 = 1] + Pr[X_1 = 1, X_3 = 1] + Pr[X_2 = 1, X_3 = 1] - Pr[X_1 = 1, X_2 = 1, X_3 = 1]) = \bar{c} \cdot (E[X_1X_2] + E[X_1X_3] + Pr[X_2X_3] - Pr[X_1X_2X_3])
\]
which increases by \( \bar{c} \cdot \Delta \phi \) as \( E[X_1X_2] \) increases by \( \Delta \phi \).
One can generalize this and show that for arbitrary \( k \) and network size, the expected system load shed will still be proportional to \( \bar{c} \cdot E[X_1 \cdots X_{k+1}] \). By the assumption that all other moments \( E[X_{i_1} \cdots X_{i_{k+1}}] \) are constant.
To prove the last claim, we denote \( p_s = Pr[S^* = \bar{c}] \), and \( p_n = 1 - p_s = Pr[S^* = 0] \). By assumption \( p_s < \frac{1}{2} \).
For this case, the variance of the load shed is simply:
\[
\sigma_{S^*} = p_n (0 - \bar{S}^*)^2 + p_s (\bar{c} - \bar{S}^*)^2 = p_s \bar{c}^2 (1 - p_s)
\]
The latter expression is increasing since
\[
\frac{\partial}{\partial p_s} p_s \bar{c}^2 (1 - p_s) = \bar{c}^2 (1 - 2p_s) > 0
\]
for \( p_s < \frac{1}{2} \). Since \( 0 < \frac{\partial \bar{S}^*}{\partial p_s} \leq \bar{c}^2 \), \( \bar{S}^* = \bar{c} p_s, \bar{S}^* \) is constant + \( \bar{c} \Delta \phi \) and
\[
\Delta \sigma_{S^*} = \int_{\bar{c} \Delta \phi}^{\bar{c} \Delta \phi} \frac{d\sigma_{S^*}}{d\bar{c}} \frac{d\bar{c}}{d\phi_{1, \ldots, k+1}}
= \int_{\bar{c} \Delta \phi}^{\bar{c} \Delta \phi} \frac{\partial \sigma_{S^*}}{\partial p_s} \frac{d\bar{c}}{d\phi_{1, \ldots, k+1}}
= \int_{\bar{c} \Delta \phi}^{\bar{c} \Delta \phi} \frac{\partial \sigma_{S^*}}{\partial p_s} \frac{d\bar{c}}{d\phi_{1, \ldots, k+1}}
\]
it holds that
\[
\Delta \sigma_{S^*} = \int_{\bar{c} \Delta \phi}^{\bar{c} \Delta \phi} \frac{\partial \sigma_{S^*}}{\partial p_s} \frac{d\phi_{1, \ldots, k+1}}{d\bar{c}} > 0
\]
\[
\Delta \sigma_{S^*} = \int_{\bar{c} \Delta \phi}^{\bar{c} \Delta \phi} \frac{\partial \sigma_{S^*}}{\partial p_s} \frac{d\phi_{1, \ldots, k+1}}{d\bar{c}} = \bar{c}^2 \Delta \phi
\]
Resource Allocation Problems in Networked Cyber Physical Systems in Adversarial Scenarios

Sourabh Bhattacharya, Ali Khanafer and Tamer Başar
Coordinated Science Laboratory,
University of Illinois at Urbana-Champaign
{sbhattac, khanafe2, basar1}@illinois.edu

Abstract—In this paper, we address the issue of malicious intrusion in a network of a team of autonomous vehicles. We present our recent results on ‘smart’ strategies for teams of autonomous mobile platforms that mutually engage in a jamming attack against each other. Contrary to the existing work in jamming, we formulate the problem as a zero-sum differential game, and provide optimal motion, power allocation and communication strategies for the agents.

In our current scenario, we consider the special case of two teams with each team consisting of two mobile agents. Agents belonging to the same team communicate over wireless ad hoc networks, and they try to split their available power between the tasks of internal communication and jamming the nodes of the other team. The agents have constraints on their total energy and instantaneous power usage. The cost function adopted is the difference between the rates of erroneously transmitted bits of each team. We model the adaptive modulation problem as a zero-sum matrix game which in turn gives rise to a continuous kernel game to handle power control. Based on the communications model, we present sufficient conditions on the physical parameters of the agents for the existence of a pure strategy saddle-point equilibrium (PSSPE).

I. INTRODUCTION

The decentralized nature of wireless ad hoc networks makes them vulnerable to security threats. A prominent example of such threats is jamming: a malicious attack whose objective is to disrupt the communication of the victim network intentionally, causing interference or collision at the receiver side. Jamming attack is a well-studied and active area of research in wireless networks. Unauthorized intrusion of such kind has started a race between the engineers and the hackers; therefore, we have been witnessing a surge of new smart systems aiming in [12], [1] shed light on the issue of security in networked control systems, the subtle interplay between the limitations in [18], [2] on the mobility, power, and communication capability among agents in adversarial scenarios remains unaddressed. Our current work is a step towards bridging this gap. Finally, there have been recent discoveries of jamming instances in biological species. It has been reported that females in resident pairs of Peruvian warbling antbirds respond to unpaired sexual rivals by jamming the signals of their own mates, who in turn adjust their signals to avoid the interference [21]. In the future, we hope that our research yields clues to help understand such instances of complex behavior among social animals as well.

The rest of this paper is organized as follows. In Section II, we provide our problem formulation. In Section III, we present the key results associated with the optimal control problem. The saddle-point equilibrium properties of the team power control problem are studied in Section IV for the specific example of systems employing uncoded M-quadrature amplitude modulations (QAM). In Section V, we present our results on the adaptive modulation schemes. We conclude the paper and provide future directions in Section VI. An Appendix at the end includes explicit expressions for some of the variables introduced in the paper. In addition to various simulation scenarios, a thorough derivation of the results in this paper is presented in [8] and [14].

II. PROBLEM FORMULATION

Consider two teams of mobile agents. Each agent is communicating with members of the team it belongs to, and at the same time- jamming the communication between members of the other team. We consider a scenario where each team has two members, though at a conceptual level our development applies to higher number of team members as well. Team A is comprised of the two players \( \{1^a, 2^a\} \) and Team B is comprised of the two players \( \{1^b, 2^b\} \). The agents move on a plane and therefore, have two degrees of freedom \((x, y)\). The dynamics of the players are given by the following equations:

- Team A:
  \[
  \begin{align*}
  \dot{x}_i^a &= f_{x_i^a}(x_i^a, u_i^a, t) \\
  \dot{y}_i^a &= f_{y_i^a}(x_i^a, u_i^a, t) \\
  \end{align*}
  \]
  \( i \in \{1, 2\} \) \hspace{1cm} (1)

- Team B:
  \[
  \begin{align*}
  \dot{x}_i^b &= f_{x_i^b}(x_i^b, u_i^b, t) \\
  \dot{y}_i^b &= f_{y_i^b}(x_i^b, u_i^b, t) \\
  \end{align*}
  \]
  \( i \in \{1, 2\} \) \hspace{1cm} (2)

In the above equations, \( x_i \) and \( u_i \) denote vectors representing the state and control input of agent \( i \), with the superscript \((a \ or \ b)\) identifying the corresponding team. The state space of the entire system is represented by \( X \simeq \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 \).
Moreover, \( u_1 \in \mathcal{U}_i \simeq \{ \phi : [0, t] \rightarrow A_i | \phi(\cdot) \text{ is measurable} \} \), where \( A_i \subset \mathbb{R}^n \). \( f : \mathbb{R}^2 \times A_i \times \mathbb{R} \rightarrow \mathbb{R} \) is uniformly continuous, bounded and Lipschitz continuous in \( x_t \) for fixed \( u_1 \). Consequently, given a fixed \( u_1(\cdot) \) and an initial point, there exists a unique trajectory solving (1) and (2) [2].

Now, we describe the physical layer communications model in the presence of a jammer which is motivated by [20] and has also been discussed in [14]. For each transmitter and receiver pair, we adopt the following communications model. Given that the transmitter and the receiver are separated by a distance \( d \), and the transmitter transmits with constant power \( P_T \), the received signal power \( P_R \) is given by

\[
P_R = \rho P_T d^{-\alpha},
\]

where \( \rho \) depends on the antennas’ gains and the wavelength of the transmitted signal.

The signal-to-interference ratio (SINR) \( s \) is given by

\[
s = \frac{P_R}{I + \sigma},
\]

where \( \sigma \) is the ambient noise level and \( I \) is the total received interference power due to jamming. The Bit Error Rate (BER) is given by the following expression:

\[
p(t) = g(s),
\]

where \( g(\cdot) \) is a decreasing function of \( s \). The instantaneous BER depends on the SINR, the modulation scheme, and the error control coding scheme utilized. Communications literature contains closed-form expressions and tight bounds that can be used to calculate the BER when the noise and interference are assumed to be Gaussian [10]. For uncoded M-QAM, where Gray encoding is used to map the bits into the symbols of the constellation, the BER can be approximated by [18]

\[
p(t) = g(s) \approx \frac{1}{\pi} \frac{\zeta}{r} Q \left( \sqrt{\frac{2 \beta s}{r}} \right),
\]

where \( r = \log(M), \zeta = 4(1 - 1/\sqrt{M}), \beta = 3/(M - 1), \) and \( Q(\cdot) \) is the tail probability of the standard Gaussian distribution.

We also assume that players in each team have access to different M-QAM modulation schemes. We denote the set of available modulation sizes to the players in Team A by \( \mathcal{M}^a \) and that available to players of Team B by \( \mathcal{M}^b \). The sizes of the employed QAM modulation by the teams are \( M^a \in \mathcal{M}^a \) and \( M^b \in \mathcal{M}^b \). We assume that Team A can choose among \( n \) different modulation schemes, and Team B chooses from a set of \( m \) different schemes, i.e., \( |\mathcal{M}^a| = n, |\mathcal{M}^b| = m \).

To ensure a non-zero communication rate between the agents of each team, we impose a minimum rate constraint for each agent: \( R^a_i(t), R^b_j(t) \geq \bar{R} \), where \( \bar{R} > 0 \) is a threshold design rate, which we assume is the same for all agents. The results can be readily extended to networks of players having a different value of the minimum design rate.

For an initial position \( x_0 \in \mathbf{X} \), the outcome of the game \( \pi \), is given by the following expression:

\[
\pi(x_0, u^1_1, u^2_2, u^1_1, u^2_2) = N \int_0^T \left[ \frac{P^a_i(t) + P^b_j(t) - P^a_i(t) - P^b_j(t)}{L} \right] dt,
\]

where \( P^a_i(t) \) and \( P^b_j(t) \) are the BERs of agent \( i \) in Team A and agent \( j \) in Team B, respectively; \( u^a_i \) and \( u^b_j \) are likewise the control inputs of agents \( i \) and \( j \) in teams A and B, respectively; \( N \) is the total number of transmitted bits which remains constant throughout the game; and \( T \) is the time of termination of the game. \( p_i \) depends on \( s_i \), i.e, the SINR perceived by agent \( i \). From (3), \( s_i \) depends on the mutual distances between the players. Therefore, we can see that the outcome functional, \( \pi \), depends on the state of the players and hence, their control inputs. The outcome functional models the difference in the erroneous communication packets exchanged between the members of the same team during the entire course of the game. The objective of team A is to minimize \( \pi \) and the objective of team B is to maximize it.

Let \( P^a_i(t) \) and \( P^b_j(t) \) denote the instantaneous power levels for communication used by player \( i \) in Team A and player \( j \) in Team B, respectively. Since the agents are mobile, there are limitations on the amount of energy available to each agent that is dictated by the capacity of the power source carried by each agent. We model this restriction as the following integral constraint for each agent

\[
\int_0^T P_i(t) dt \leq E.
\]

The game is said to terminate when any one agent runs out of power, that is (6) is violated.

In addition to the energy constraints, there are limitations on the maximum power level of the devices that are used onboard each agent for the purpose of communication. For each player, this constraint is modeled by the following set of inequalities:

\[
0 \leq P^a_i(t), P^b_j(t) \leq P_{\text{max}}.
\]

At every instant, each agent has to decide on the fraction of the power that needs to be allocated for communication and jamming. Each player uses its power for the following purposes: (1) Communicating with the team-mate, and (2) Jamming the communication of the other team. We assume that \( f_a \) and \( f_b \) are the frequencies at which Team A and Team B communicate, respectively, and \( f_a \neq f_b \).

Table I provides a list of the decision variables for the players that models this allocation. Each decision variable is a non-negative real number and lies in the interval \([0, 1]\). The decision variables belonging to each row add up to one. The fraction of the total power allocated by the player in row \( i \) to the player in column \( j \) is given by the first entry in the cell \((i, j)\). This allocated power is used for jamming if the player in column \( j \) belongs to the other team; otherwise, it is used to communicate with the agent in the same team. Similarly, the distance between the agent in row \( i \) and the agent in column \( j \) is given by the second entry in cell \((i, j)\). Since distance
is a symmetric quantity, \( d_{ij} = d_{ji} \). Figure 1 summarizes the power allocation between the members of the same team as well as between the members of different teams.

<table>
<thead>
<tr>
<th>( b )</th>
<th>1</th>
<th>2</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \gamma_1^1, d_1^1 )</td>
<td>( \gamma_2^1, d_2^1 )</td>
<td>—</td>
<td>( \gamma^{12}, d^{12} )</td>
</tr>
<tr>
<td>2</td>
<td>( \gamma_1^2, d_1^2 )</td>
<td>( \gamma_2^2, d_2^2 )</td>
<td>( \gamma^{21}, d^{21} )</td>
<td>—</td>
</tr>
<tr>
<td>1</td>
<td>—</td>
<td>( \delta_{12}, d_{12} )</td>
<td>( \delta_1^1, d_1^1 )</td>
<td>( \delta_2^1, d_2^1 )</td>
</tr>
<tr>
<td>2</td>
<td>( \delta_{21}, d_{21} )</td>
<td>—</td>
<td>( \delta_1^2, d_1^2 )</td>
<td>( \delta_2^2, d_2^2 )</td>
</tr>
</tbody>
</table>

In the above game, each agent has to compute the following variables at every instant:
1. The instantaneous control, \( u_i(t) \).
2. The instantaneous power level, \( P_i(t) \).
3. All the decision variables present in the row corresponding to the agent in Table I.
4. The size of the QAM schemes, \( M_a \) or \( M_b \).

In the next section, we analyze the problem of computing the optimal controls for each agent.

### III. Optimal Control Problem

From the problem formulation presented in the previous section, we can conclude that the objective functions of the two teams are in conflict. The tuple \((u_1^{a*}, u_2^{a*}, u_1^{b*}, u_2^{b*})\) is said to be optimal (or, in pair-wise saddle-point equilibrium) for the players if it satisfies the following conditions:

\[
\begin{align*}
\pi[x_0, u_1^{a*}, u_2^{a*}, u_1^b, u_2^b] &\leq \pi[x_0, u_1^{a*}, u_2^{a*}, u_1^b, u_2^b] & (9) \\
\pi[x_0, u_1^{a*}, u_2^{a*}, u_1^b, u_2^b] &\leq \pi[x_0, u_1^a, u_2^a, u_1^{b*}, u_2^{b*}] & (10)
\end{align*}
\]

In simple terms, the above equations imply that agents in Team A are solving a joint optimization problem of minimizing the outcome. Similarly, agents in Team B are solving a joint optimization problem of maximizing the outcome. Moreover, the two teams are playing a zero-sum game against one another. In this case, the value of the game, denoted by the function \( J: X \rightarrow \mathbb{R} \), can be defined as follows:

\[
J(x) = \pi[x_0, u_1^{a*}, u_2^{a*}, u_1^{b*}, u_2^{b*}] \quad (11)
\]

The value of the game is unique at a point \( X \) in the state-space. An important property satisfied by the value of the game is the Nash equilibrium property. The tuple \((u_1^{a*}, u_2^{a*}, u_1^{b*}, u_2^{b*})\) is said to be in Nash equilibrium if no unilateral deviation in strategy by a player can lead to a better outcome for that player. Hence, there is no motivation for the players to deviate from their equilibrium strategies. In terms of the outcome of the game, the strategies \((u_1^{a*}, u_2^{a*}, u_1^{b*}, u_2^{b*})\) are in Nash equilibrium (for the 4-player game) if they satisfy the following property:

\[
\begin{align*}
\pi[x_0, u_1^{a*}, u_2^{a*}, u_1^b, u_2^b] &\leq \{ \pi(x_0, u_1^{a*}, u_2^{a*}, u_1^b, u_2^b) \} & (12)
\end{align*}
\]

In general, there may be multiple sets of strategies for the players that are in Nash equilibrium. Assuming the existence of a value, as defined in (11), we can conclude that the Nash equilibrium concept of person-by-person optimality given in (12) is a necessary condition to be satisfied for the value of the game. Further, obtaining the set of strategies that are in Nash equilibrium yields the optimal strategies for the players. In the following analysis, we assume the aforementioned conditions in order to compute the optimal strategies.

From Isaacs’ conditions [13], the optimal control \( u_i \) is obtained by the following expression:

\[
\begin{align*}
\delta u_i^{a*} &= \min_{u_i} \frac{\partial J}{\partial u_i} \cdot f_i(x_i^a, u_i^a, t) \quad \{ \text{i = 1, 2} \} \\
\delta u_i^{b*} &= \max_{u_i} \frac{\partial J}{\partial u_i} \cdot f_i(x_i^b, u_i^b, t)
\end{align*}
\]

Additionally, the gradient of the value function satisfies the retrogressive path equations (RPE) given by the following partial differential equation for the players.
Team A

\[ J_{x_i} = \nabla J \cdot \frac{\partial f_{x_i}^{\alpha}(x)}{\partial x_i} + \sum_{k=1,2} \left[ \frac{s_b^k g(s_k)(x_j - x_k^i)}{(d_{12})^2} \right] \]

\[ J_{y_i} = \nabla J \cdot \frac{\partial f_{y_i}^{\alpha}(y)}{\partial y_i} - \sum_{k=1,2} \left[ \frac{s_b^k g(s_k)(y_j - y_k^i)}{(d_{12})^2} \right] \]

Team B

\[ J_{x_i} = \nabla J \cdot \frac{\partial f_{x_i}^{\beta}(x)}{\partial x_i} + \sum_{k=1,2} \left[ \frac{s_b^k g(s_k)(x_j - x_k^i)}{(d_{12})^2} \right] \]

\[ J_{y_i} = \nabla J \cdot \frac{\partial f_{y_i}^{\beta}(y)}{\partial y_i} - \sum_{k=1,2} \left[ \frac{s_b^k g(s_k)(y_j - y_k^i)}{(d_{12})^2} \right] \]

Here, (\cdot) denotes derivative with respect to retrograde time. Since termination is only a function of the power of each player, \( J \) is independent of the position of the players on the terminal manifold. Therefore, \( \nabla J = 0 \) at termination. This forms the boundary condition for the RPE.

In the next section, we address the problem of power allocation.

IV. POWER ALLOCATION

Since the players do not communicate, they possess information only about their own decision variables. This makes the power allocation problem a continuous kernel zero-sum game between the two teams:

**Team A**: The objective of each agent is to minimize \( L \).

\[
\min_{P^a, \gamma^1, \gamma^2} L(M^a, M^b) \Rightarrow \min_{P^a, \gamma^1, \gamma^2} \left( p^a_l - p^a_i - p^a_k \right) \]

subject to:

\[ 0 \leq P^a_i(t) \leq P_{\text{max}}, \quad R^a_i \geq \tilde{R} \]

\[ \gamma^1 + \gamma^2 + \gamma^3 = 1, \quad \gamma^1, \gamma^2, \gamma^3 \geq 0 \]

**Team B**: The objective of each agent is to maximize \( L \).

\[
\max_{P^b, s^1, s^2, \delta_i} L(M^a, M^b) \Rightarrow \max_{P^b, s^1, s^2, \delta_i} \left( p^b_l + p^b_i - p^b_k \right) \]

subject to:

\[ 0 \leq P^b_i(t) \leq P_{\text{max}}, \quad R^b_i \geq \tilde{R} \]

\[ \delta^1_i + \delta^2_i + \delta_i = 1, \quad \delta^1_i, \delta^2_i, \delta_i \geq 0 \]

Note that the power allocation vector for \( i \) denoted by \( \gamma = (\gamma^1, \gamma^2, \gamma^3) \) belongs to the intersection between the three-dimensional simplex \( \Delta^3 \) and the plane \( r_0 \), where \( r_0 = \{ \gamma | \gamma^1 = \frac{1}{2}(\alpha - 1) \} \). The power allocation vectors of other players belong to similar sets.

Now we consider the problem of computing the optimal value of the decision variables for the players. In order to do so, we use preexisting results from continuous kernel games for the existence of a pure strategy saddle-point equilibrium (PSSPE).

**Theorem 1**: [3] Let \( U \) be a closed, bounded and convex subset of \( \mathbb{R}^m \), and for each \( i \in \mathbb{N} \) the cost functional \( J^i : U \rightarrow \mathbb{R} \) be continuous on \( U \) and convex in \( u^i \) for every \( u^j \not\in U^j \), \( j \in \mathbb{N}, j \not\in i \). Then, the associated \( N \)-person non-zero-sum game admits a PSNE.

In [8], we showed that the optimal value of the power consumption for each player is \( P_{\text{max}} \). We also showed that the entire game terminates in a fixed time \( T = T_{\text{RPE}} \) irrespective of the initial position of the agents. Moreover we provided a sufficient condition for the existence of a PSSPE for the power allocation game when uncoded M-QAM schemes are used by all agents using Theorem 1.

**Theorem 2**: The power allocation team game has a unique Nash equilibrium in pure strategies if the following conditions hold for Team A:

\[ g^i(s^a) > 0, \]

\[ g^i(s^a) + \frac{2}{d_i} (c_i + \gamma^1) g'(s^a) < 0, \]

\[ g^i(s^b) + \frac{2}{d_i} (c_i + \gamma^2) g'(s^b) < 0, \]

and equivalent conditions hold for Team B:

\[ g^i(s^b) > 0, \]

\[ g^i(s^b) + \frac{2}{d_i} (m_i + \delta^i) g'(s^a) < 0, \]

\[ g^i(s^a) + \frac{2}{d_i} (m_i + \delta^i) g'(s^b) < 0, \]

where \( i \in \{1, 2\} \).

The constants \( b_2, c_2, d_2, e_i, l_i, m_i, n_i, \) and \( o_i \) are obtained by re-writing the SINR expressions as done above; their expressions can be found in the Appendix.

**Theorem 3**: When all players employ uncoded M-QAM modulation schemes, the power allocation team game formulated above has a unique PSSPE solution if the following condition is satisfied:

\[ P_{\text{max}} \max \left\{ \rho_0(d_{12})^{-\alpha}, \frac{\rho_0(d_{12})^{-\alpha}}{M^a - 1} \right\} < \sigma^2. \]

For the special case of \( M^a = M^b = M \) and \( \rho_b \approx \rho_a = \rho \), the condition becomes

\[ \beta \rho P_{\text{max}} \min \{d_{12}, d_{12}\}^{-\alpha} < 3\sigma^2. \]
V. ADAPTIVE MODULATION

The time-varying nature of the channels due to mobility emphasizes the need for robust communications. Adaptive modulation is a widely used technique as it allows for choosing the design parameters of a communications system to better match the physical characteristics of the channels in order to optimize a given metric such as: minimizing BER or maximizing spectral efficiency. In this work, we model the adaptive modulation as a matrix zero-sum game between the two teams. We therefore look for an equilibrium solution which would dictate what modulations should be adopted by the teams at each time instant. The competitive nature of the jamming teams makes our approach to the problem most practical as any other non-equilibrium solution cannot produce an improved outcome, relative to that yielded by the equilibrium, for any of the teams.

The matrix game is given in (23). The rows are all the possible actions for players of Team A, and the columns are the different options available for Team B. The \( (i, j) \)-th element of the matrix is the value of the objective function \( L \) when Team A employs \( M^a = M^a(i) \), and Team B employs \( M^b = M^b(j) \).

A PSSPE does not always exist for the power allocation game. The condition for the existence of a PSSPE is \( \min \max A_{ij} = \max \min A_{ij} \) [3]. In case a PSSPE does not exist, we need to look for a solution in the larger class of mixed-strategies. A pair of strategies \( \{M^a, M^b\} \) is said to be a a mixed-strategy saddle point equilibrium (MSSPE) for the matrix game if [3]

\[
(M^a)^T A M^b \leq (M^a)^T A M^{b_1} \leq (M^a)^T A M^{b_2}
\]

For an \( n \times m \) matrix game, the following theorem from [3], which we state without proof, establishes the existence of an MSSPE for the adaptive modulation game.

Theorem 4: The adaptive modulation game admits an MSSPE.

In case multiple MSSPEs exist, the following corollary becomes essential [3].

Corollary 1: If \( \{M^a(i_1), M^b(j_1)\} \) and \( \{M^a(i_2), M^b(j_2)\} \) are two MSSPEs of the adaptive modulation game, then \( \{M^a(i_1), M^b(j_2)\} \) and \( \{M^a(i_2), M^b(j_1)\} \) are also MSSPEs.

This is termed the ordered interchangeability property and its importance lies in that it removes any ambiguity associated with the existence of multiple equilibrium solutions as the teams do not need to communicate to each other which equilibrium solution they will be adopting. Literature contains different efficient low-complexity algorithms that computes MSSPEs for matrix games, such as Gambit [16]. We refer the interested reader to [3] for a discussion of some of these approaches.

VI. FUTURE EFFORTS

This paper has studied the power allocation problem for jamming mobile teams. The motion of the teams was modelled using the framework of pursuit-evasion games and the optimal strategies were derived. An underlying static game was used to obtain the optimal power allocation, where the power budget of each user is split between communication and jamming powers. Further, a matrix game was formulated to solve the adaptive modulation problem. This work focused on the analysis of teams consisting of two players only. Potential future directions include:

- **Computation of Singular Surfaces**: In this work, we have computed the trajectories based on the necessary conditions of optimality imposed by the Isaacs’ conditions. In order to complete the construction of the optimal trajectories of the agents, we have to identify the singular surfaces in the state space [3]. This is an interesting future research direction since the construction and nature of the singular surfaces would depend on the value of the decision variables obtained from the power allocation game.

- **Scheduling Schemes**: An interesting direction would be exploring scheduling algorithms, similar to the one proposed in [9], in which players take turns in communicating or jamming. For example, the users of a given team that are closest in distance to the other team could allocate all their resources to jamming, while the other users allocate all their resources to communicating with each other.

- **Power Control**: When multiple users are present, and due to the broadcast nature of wireless systems, networks become interference-limited. The transmission power of one user can impede the links between other nodes due to the interference; hence, it is important to regulate the transmission power of the users in order to, for example, maximize the total capacity of the network.

- **Routing**: Multi-hop routing improves the total throughput and power efficiency of a network through relaying packets via intermediate nodes to their final destination. Because a portion of the energy of each node has to be allocated to jam the other team, determining the optimal route for transmission becomes a challenge, especially in the presence of mobility. An investigation of routing protocols in the context of games is therefore essential for studying the overall performance of the networks [19].

- **Eavesdropping**: When \( f_a = f_b \), another security issue arises as the ADMs of a given team can receive and decode messages intended for internal communications of other teams. To ensure secure communications, each team would need to allocate power to jam the eavesdroppers. In fact, a more general scenario is when adversarial teams consist of active eavesdroppers: malicious nodes that can act as jammers and eavesdroppers [17].

REFERENCES


\[ A = \begin{array}{cccc}
\mathcal{M}^a(1) & \mathcal{M}^b(1) & \ldots & \mathcal{M}^b(m-n) \\
\mathcal{M}^a(2) & \mathcal{M}^b(2) & \ldots & \mathcal{M}^b(m-n) \\
\vdots & \vdots & \ddots & \vdots \\
\mathcal{M}^a(n) & \mathcal{M}^b(n) & \ldots & \mathcal{M}^b(m-n) \\
\end{array} \]

Team A

Team B


APPENDIX

The following are the expressions of the quantities appearing in Theorem 2:

\[
\begin{align*}
a_1 &= \frac{1}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}}, \\
b_1 &= \delta_{21} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}, \\
c_1 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \gamma_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}}, \\
d_1 &= \delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}, \\
e_1 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \gamma_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}} + \frac{1}{\sigma}, \\
a_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}}, \\
b_2 &= \delta_{21} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}, \\
c_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \gamma_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}}, \\
d_2 &= \delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}, \\
e_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \gamma_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}}, \\
k_1 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \gamma_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \gamma_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}} + \frac{1}{\sigma}, \\
l_1 &= \gamma_{21} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}, \\
m_1 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}}, \\
n_1 &= \gamma_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}, \\
o_1 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}}, \\
k_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha} + \delta_{2}^{2} \left( \frac{d_{2}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}}, \\
l_2 &= \gamma_{21} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}, \\
m_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}}, \\
n_2 &= \gamma_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha}, \\
o_2 &= \frac{\sigma}{\delta_{12} \left( \frac{d_{12}^{\alpha}}{d_2^{\alpha}} \right)^{-\alpha} + \delta_{1}^{1} \left( \frac{d_{1}^{\alpha}}{d_1^{\alpha}} \right)^{-\alpha}},
\end{align*}
\]
Enhancing Cyber-Physical Security through Data Patterns

Richard Chow, Ersin Uzun
Palo Alto Research Center
Palo Alto, CA USA
{rchow, euzun}@parc.com

Alvaro A. Cárdenas, Zhexuan Song, Sung Lee
Fujitsu Laboratories of America
Sunnyvale, CA USA
{alvaro.cardenas-mora, zhexuan.song, sung.lee}@us.fujitsu.com

Abstract—In this position paper, we propose a data-driven approach for security management in a network that interacts or receives inputs from physical systems – including human behavior. Our goal is to leverage the unique features of cyber-physical systems. In particular we propose: (1) the use of historical data from physical systems and human behaviors to enable anomaly detection, (2) the use of contextual data from multiple and diverse sensor readings to obtain a higher-level collective vision of the network for better event correlation and decision analysis, and (3) the use of physical sensor data and human behavior to enable fine-grained, dynamic access control and implicit authentication. We outline use cases describing how our ideas can be applied in the Home Area Network (HAN).

Keywords—home area networking; authentication; security; privacy; anomaly detection

I. INTRODUCTION

As cyber-physical systems become more pervasive and important they will increasingly become the focus of attacks. One prominent recent example is Stuxnet. The Stuxnet worm targets industrial controllers and is believed to target the uranium enrichment infrastructure in Iran [6], [2], [3]. In addition, the rise of ubiquitous computing and the Smart Grid imply the deployment of billions of smart sensors and actuators embedded in our social infrastructures. By relying on information technology and networks, these new deployments will expose our social infrastructure to regular computer vulnerabilities available to an ever-growing set of motivated and highly-skilled attackers.

While many existing security mechanisms can be applied to cyber-physical systems, in this paper we explore some unique ways to enhance the security of these systems by leveraging the diverse physical and human behavior information collected by these systems. Examples include: (1) the use of historical data from physical systems and human behaviors to enable anomaly detection, (2) the use of contextual data from multiple and diverse sensors to obtain a higher-level collective vision of the network for better event correlation and decision analysis, and (3) the use of physical sensor data and human behavior to enable implicit authentication and fine-grained, dynamic access control.

For point (1), we propose the use of device and human profiles generated from a data driven approach. For example, a historical profile of the alarm system of a house that leaves the alarm on every night might generate an incident report if one day the alarm is shut off at 3 AM in the morning. In general, previous work has shown that cyber-physical systems might benefit from anomaly detection techniques, as physical processes give off large amounts of data that are clearly non-deterministic in nature, and yet somewhat predictable [7].

While the use of physical process data has already been proposed as a way to detect computer attacks on cyber-physical systems [9], we believe that in order to obtain a better and more complete view of the system, the data of multiple and diverse sensors needs to be aggregated and combined to generate usable models with low false alarm rates. Therefore, we propose for point (2), the use of a master controller that collects multiple data sources and integrates them into the proper context. For example, while shutting off the home alarm system at 3 AM in the morning might be anomalous in itself, it might not be anomalous if the electric car associated with the home has also just pulled into the garage and was plugged into its charger. We argue in this position paper, especially in the case of the Home Area Network (HAN), that higher level patterns that involve collective behavior of devices and users should also be analyzed for anomalies. User behavioral patterns are also non-deterministic and yet somewhat predictable.

Finally, for point (3), we believe that the user and device profiles obtained by (1), and the contextual information obtained by (2) can be used to enhance user authentication, dynamic access control, revocation, and fine-grained access control policies. For example, a typical home area network currently provides full security or no security at all. It is very difficult for users at home to set the appropriate fine-grained access control to devices at home, and the proper revocation mechanisms. For example, if a neighbor brings their laptop to a home and is given the keys to access the wireless network, the neighbor will remain a valid (authenticated) user of the network even in his own home. We propose the use of device profiles for implicit authentication, allowing the revocation of devices that do not match our experience.

In the remainder of this paper we explore in more detail our arguments by providing additional use cases, a general system description, and a discussion of the security, usability, and performance of the system.
II. ADDITIONAL USE CASES

Collective Device Behavior

Higher-level components of cyber-physical systems may also exhibit anomalous behavior, and this behavior is best analyzed given appropriate context. A simple example is that intensive operation of an air-conditioning system is not anomalous given a heat wave, but may be under normal weather conditions. A more complex example is that shutting off the home alarm system at 3 AM might be very normal if the electric car has just pulled into the garage and is plugged into its charger.

Finding these sorts of rules may require sophisticated machine learning apparatus, but the advantage is more intelligent security decisions and fewer false positives. In large control systems this feature is usually called situational awareness.

Consider for example a home network that controls appliances, heating and cooling, and lighting. In most networks available to consumers, there is typically a lack of fine-grained access control: access to the central controller implies total control of the system. However, adding such fine-grained access control runs the danger of making the system unusable.

Instead, we propose adding a behavioral analysis system on top of the controller security system. We amass a collective baseline of historical settings, readings, and network traffic. The baselines can be used to detect intrusion, both cyber and physical (as well as broken or misconfigured equipment). Detected anomalies in a device may result in revocation from the network, or a request for re-authentication or two-factor authentication. Revocation in home area networks is not an easy task to accomplish in current mass market deployments.

Collective contextual information can also be used to design more flexible access control mechanisms. For example, with the proliferation of surveillance cameras in everyday life and webcams at home computers, the number of unsecured cameras on the Internet has become an increasing cause of concern. Bloggers have reported the ability to tap into thousands of raw webcam feeds with a few simple Google searches, and the Spanish police arrested a suspect on charges of developing a computer virus that can activate a webcam without the owner’s permission [5]. We propose that the context for camera networks might be used in the access control policy. For instance, the context contains properties such as the content of the video stream (e.g., people or the type of events happening), when the access request is made, and location of the subject. These properties add the flexibility of describing rules such as “only people in a room should be able to control the camera located in that room.” Camera networks might also be part of complex networks including other sensors such as audio, temperature, humidity etc. The readings of these sensors might give additional context relevant to the access control policy. For example, emergency response teams (firefighters or paramedics) may be allowed to access any web camera if the fire alarm is on.

User behavior

The cyber-physical systems of tomorrow are all envisioned to be connected and remotely controllable. With the advent of the smart grid, smart appliances within a consumer’s HAN can be controlled remotely by consumers and potentially by utility companies. See, for example, [1] for the latest iPhone applications for remotely controlling the home and [4] for the PG&E SmartAC program. Given the ubiquity of Internet-connected smartphones, it is clear that cyberattacks against such devices is a way to attack the HAN. In fact, as argued by Neuman [10], creating a smartphone botnet may be a relatively easy way to generate traffic affecting the large scale power grid.

Given the possibility of direct intrusion into the home, the proper authentication of users becomes even more critical. One approach is to protect each remote control instance, for example requiring traditional authentication mechanisms (such as a password, one-time-password, or user certificate) for each remote control directive. This strategy may provide a reasonable level of security when used properly (for example, unpredictable passwords, secure storage of certificates, etc.), but does not scale well when the number of devices increases. Imagine, for a moment, the following common scenario: you have many personal Internet-connected devices such as a laptop, desktop, smartphone and even an Internet-connected TV that you use to control all the appliances in your HAN, such as the air-conditioning unit, alarm, electric car, lights and other smart appliances. Having a separate password for all these devices and authenticating to each every time you need access is very unusable while having the same password for all of them would significantly reduce the security.

Another approach is to authenticate the user once and provide general remote control capabilities after this authentication, at least for some limited period of time. These technologies reduce the burden on the user by requiring, say, only one password. However, these technologies not only ease access for legitimate users but ease it for attackers as well. A natural answer is to add an additional authentication factor, but traditional second factors such as hardware tokens or biometrics reduce usability, especially on a mobile platform.

We propose that patterns of user behavior can be used as a second factor, in line with the theme of this paper of using behavioral patterns to increase security. For mobile phones in particular, the behavioral patterns can be based from rich data, such as location, calls, SMS, and web site visits. See [8] and [13] for some work in this direction, called implicit authentication. This approach does not directly address malware on the phone, but reduces the risk of a
lost phone providing a gateway into the home network. One of the themes in this paper is to generalize the techniques of implicit authentication beyond humans to a collection of devices.

We remark also that improving authentication on mobile phones is critical because smartphones might become the de facto remote control device. We believe the phone will also be involved in various enrollment protocols in the HAN. For instance, in [12] the phone is the party that mediates the pairing between two devices.

III. System Description

We outline here one possible system architecture based on the above ideas. See Figure 1 for a representation in the home network. Appliances are enrolled into a star-shaped network centered at a Master Controller. Commands to each appliance go through and are vetted by the Master Controller. The Master Controller contains an Authentication Service to authenticate commands, and also a Pattern Analyzer to build data models and evaluate recent data based on the models.

Appliances periodically upload data to an authentication service. These include settings, sensor readings, status, etc. In the case of a device with a user interface, user-related data may be recorded as well. For instance, data such as location, call logs, SMS logs, and web sites visited (all suitably anonymized and obfuscated) might be collected for a cell phone. This data is stored in the Database and used by the Pattern Analyzer to generate a model for the data. For instance, a simple model might say that the air conditioner is usually on during the afternoon but off at night.

Note that the smart meter may also upload data to the Master Controller. In this way, patterns of household electric data may be incorporated into the Pattern Analyzer. As detailed in [11], these patterns can identify the use of even non-smart appliances, as well as reconstruct daily routines, including sleep habits of inhabitants.

When the user wishes to change a setting on a device, say, through an application on his phone, the application connects with the Master Controller with the usual password. Depending on the policy enforced for the device, the Master Controller may measure how well recent behavior on the phone matches historical behavior. If the behavior is very different, another credential may be requested. The policy may also request another credential if a change is requested that is unusual for that device, in conjunction with all other available data. For example, turning on the air conditioner in the middle of the night may be unusual, but especially if nobody is in the house.

We allow the possibility of a device directly interacting with another device, not going through the Master Controller. For instance, in Figure 1, a cell phone might be used to control a car without going through the Master Controller. In this case, the user has chosen to drop back to unaided traditional measures, without the added assurance provided by the Master Controller. The user may not want to rely on the Master Controller being operational, for instance.

A novel aspect of the system is that the data uploaded to the Master Controller must be treated as sensitive. Knowledge of the data would be equivalent to knowing a security key in a traditional system, since the algorithms used by the Master Controller must be considered public. Hence, communication channels to the Master Controller should be secured, and we expect that data will not reside in the long term on individual devices, limiting the risk of compromises of individual devices. We recognize, however, that for some devices historical data facilitates daily operation of the device (for example, the recent calls on a cell phone).

A. Anomaly Detection

One key question is how well anomaly detection works for this kind of data. Experiments described in [13] indicate that user modeling on cell phones is promising. With training data of around one or two weeks and four types of data collected (web sites, call logs, SMS, location), one can set thresholds such that an adversary would be detected within about 10 phone usages, while the legitimate user is identified as illegitimate about every 130 usages. It is reasonable to believe (but have no hard evidence) that most devices would have less variance and less richness in their data and so would be more predictable.

In [13], the approach is to treat each type of data collected separately. For each type of data, the software builds a model based on training data and then evaluates recent data against the model, deriving a score. See Figure 2. The scores for each data type are combined, assuming independence of each data type. To enable the discovery of the complex rules and interactions between HAN appliances, it would be necessary to detect and model the actual correlations between data types, going beyond the work in [13].

IV. Summary and Discussion

In this position paper, we propose data-driven security management for cyber-physical systems. We argue that in the cyber-physical systems of the near future, such as HANs, better and more usable anomaly/attack detection can only be built if the collective information from all devices as
well as the behavior of their user and the inferred context are integrated into the decision making process. From the examples given in previous sections, we indicate how this collective high-level vision can detect anomalies for devices that operate within usual limits when considered individually, or how false alarms can be prevented with a collaborative and contextual view.

On the other hand, there are some obvious limitations to such a system. For example, one real advantage of a collaborative view over a range of smart devices is the ability to capture the behavioral patterns of a human user and make contextual decisions based on these patterns. However, humans do not always follow established behavioral patterns, and in the case of multiple users interacting with the same system, the system may be slow or ineffective in detecting attacks/anomalies due to the lack of one clear behavioral pattern. Having one master controller is another weakness of the system as it may be a single point of failure, but this weakness can be easily overcome by employing fault-tolerance practices such as replication.

Note that decision making in the proposed system is based on automated modeling which requires sufficient initial training data and also dynamically evolves with time to be more effective. However, the ongoing training process makes the system vulnerable at the beginning and can possibly be exploited by smart attackers to slowly evolve the system to an insecure state if it is not designed carefully. In the case of user authentication with behavioral data, one important limitation is the reaction time of the system to a user change. In other words, it is not possible for the system to detect changes in the user behavior before certain number interactions between the system and an attacker. Thus, we only recommend this kind of implicit authentication as a second factor or as a low-security authentication mechanism.

One main motivation is usability. Since security is not the main objective when users interact with a system, they get irritated when they are bothered with security mechanisms (for example, requests for an additional credential) while trying to achieve their goal (for example, turning on the air-conditioner). With this system, the overall authentication can be made more usable by reducing the requests for additional credentials. False alarms by security systems are one of the biggest issues of current security systems, affecting both usability and security. Too many false alarms not only make the system less usable, but also seriously damages security (for example, nobody pays attention to car alarms). Hence, usability of our system is intimately tied to the rates of both false positives and false negatives of our anomaly detection algorithms; acceptable rates would need to be determined with user studies.

REFERENCES


ABSTRACT

Physical Unclonable Functions (PUFs) are novel circuit primitives which store secret keys in silicon circuits by exploiting uncontrollable randomness due to manufacturing process variations. Previous work has mainly focused on static challenge-response behaviors. However, it has already been shown that a reconfigurable architecture of PUF will not only enable PUFs to meet practical application needs, but also can improve the reliability and security of PUF-based authentication or identification systems. In this paper, we propose several novel structures for non-FPGA reconfigurable silicon PUFs, which do not need any special fabrication methods and can overcome the limitations and drawbacks of FPGA-based techniques. Their performances are quantified by the inter-chip variation, intra-chip variation and reconfigurability tests.

Keywords: Physical Unclonable Function, Reconfigurable Architecture, Hardware Security, Counterfeit IC Chip Prevention

1. INTRODUCTION

1.1 Physical Unclonable Function

In today’s world, as electronic devices become increasingly interconnected and pervasive in people’s lives, security, trustworthy computing, and privacy protection have emerged over the past decade as hardware design objectives of great significance. Traditionally, secret keys, which are used as unique identifiers, are embedded into integrated circuits (ICs) in a ROM immediately after manufacturing. Unfortunately, digital keys stored in a non-volatile memory are vulnerable to physical attacks. Several invasive and semi-invasive physical tampering methods have been developed, these include techniques such as micro-probing (access to the silicon to manipulate the internals of system), power analysis (predict the secret keys from power consumption analysis) and so forth. These approaches have made it possible to learn the ROM-based keys through attacks and compromise systems by using counterfeit copies of the secret information.

The described problem has become more intense recently, and this motivated the idea of using intrinsic random features of physical objects for identification and authentication. The concept of physical unclonable function (PUF) proposed in [1–3] has successfully addressed the problems faced by traditional techniques. PUF has been defined as a function that exploits the unique intrinsic uncontrollable physical features by process variations during manufacturing. Physical Unclonable Functions enable significantly higher secure authentication by extracting secrets from complex properties of a physical material rather than storing them in non-volatile memory. Due to the uncontrollable random components, PUFs are easy to measure but almost impossible to clone, predict, or reproduce. Furthermore, it is infeasible for an adversary to mount an attack to counterfeit the secret information without changing the physical randomness. Taking coating PUF as an example, which is a function built in the top layer of an IC by filling the space between and above the comb structure with an opaque material and randomly doping with dielectric particles, any physical attack on a coating PUF would damage the protective coating and destroy the cryptographic key.

1.2 Related Work and Our Contribution

The first PUF in the literature is the optical PUF [1], which utilizes the randomness in the placement of the light scattering particles and the complexity of the interaction between the laser and the particles. After that, several PUF hardware structures have been proposed [2–6]. Most PUFs use conventional silicon techniques so that they do not require any special fabrication and can be easily integrated into IC chips, except a few types such as coating PUF and magnetic PUF. Among these PUFs, silicon PUFs are of great interest, as these exploit manufacturing variability of wire delay to generate a unique challenge-response mapping for each IC. These unique properties of each IC are easy to measure through the circuits but hard to copy without changing the challenge-response pairs (CRPs).

The delay-based silicon PUFs in previous work have always considered a static challenge-response behavior. In those protocols, the PUF should always generate the same or error tolerated response. Unfortunately, recent analysis has demonstrated that those PUF structures are vulnerable to several attack methods including emulation, replay (man-in-the-middle attack), and reverse engineering [7]. Moreover, updatable cryptographic keys are very attractive in some applications [8]. Therefore, a dynamic PUF that can alter the CRPs every time the data is modified to prevent the hidden information leaked out is very desirable.

Our work builds on the prior work of the PUF community. In this paper, we mainly focus on the design of reconfigurable silicon PUFs. We propose several novel reconfigurable PUFs and analyze their performance. We also examine the security of different PUF structures. The key idea in our approach is that we try to make CRPs updatable. By doing this, the challenge-response behavior of a PUF can be altered to generate highly secure hardware system. Furthermore, we discuss the techniques to improve the reliability of silicon PUFs.

1.3 Paper Organization

The rest of the paper is organized as follows. In Section 2, we introduce the background of silicon PUFs, and then present a brief overview of previous works on reconfigurable PUFs and discuss their disadvantages and limitations. In Section 3, we describe our manufacturing process variation model for silicon PUFs and the experimental methods. Section 4 discusses several novel reconfigurable PUF designs and analyzes their efficiency. Section 5 demonstrates the performance of the discussed reconfigurable structures by providing experimental results on SPICE simulation. Finally, Section 6 concludes the paper.

2. BACKGROUND

2.1 Silicon Physical Unclonable Function
Silicon PUFs exploit the delay variations of CMOS logic components to generate a unique response for each IC. There are two main types of delay-based silicon PUFs: Ring Oscillator (RO) PUF [2] and Multiplexor (MUX) PUF [9]. However, the MUX PUF is more secure than the RO PUF, as the frequencies of the ring oscillators can be relatively easily attacked by attackers; moreover, a MUX PUF is more suitable for resource-constrained applications. Instead of duplicating the hardware N times as in a RO PUF, we can use N different challenges to obtain a N-bit long response in a MUX PUF, as illustrated in Figure 1. This kind of silicon PUF consists of N stages MUXs and one arbiter which connects the final stage of the two paths. MUXs in each stage act as a switch to either cross or straight propagate the rising edge signals, based on the corresponding challenge bit. Each MUX should be designed equivalently, while the variations will be introduced only during manufacturing process. Finally, the arbiter (always simply a D flip-flop) translates the analog timing difference into a digital value. For transistors, manufacturing randomness exists due to variations in transistor length, width, gate oxide thickness, doping concentration density, metal width, metal thickness, and ILD (inter-level dielectric) thickness, etc [10]. These manufacturing variations show a significant amount of variability, which are sufficient to generate unique challenge-response pairs for each IC by comparing the delays of two paths.

Figure 1: Silicon MUX Physical Unclonable Function.

3. METHODOLOGY

3.1 PUF Model

As shown in Figure 1, a MUX PUF consists of a sequence of N-stage MUXs and an arbiter. The rising edge signal will excite the two parallel paths simultaneously. The actual propagated paths will be determined by the external applied challenge bits. After the last stage, the arbiter will generate the output bit by comparing the arrival time of the two different paths. It has become standard to model the MUX PUF via an additive linear delay model. According to the efforts in the field of Statistical Static Timing Analysis (SSTA) [10], the manufacturing process parameter variations for transistors can be modeled by a Gaussian distribution. As a result, the variations of delay will also be approximately Gaussian.

Manufacturing process variations can be classified as the following two categories: inter-die variations and intra-die variations. Inter-die variations refer to parameter variations that affect all devices equally across a single die, while intra-die variations have different effects on the devices within the same chip. It is also imperative to consider the correlation of these variations to increase the accuracy of the model. A very widely used model for delay spatial correlation of process variations is the Grid model [10], which assume high correlations among the devices in nearby grids and low correlations in faraway grids, as manufacturing process variations are more likely to have similar effects on closer devices. Additionally, experimental results have already shown that the interchip variation across the wafer is similar to that within a single wafer [9]. Moreover, the output of the arbiter in silicon PUF is only based on the difference of two selected paths. Therefore, the inter-chip variations are the primary factors that contribute to the randomness of response for each IC, while these die-to-die and wafer-to-wafer manufacturing variations will have minimum effect on the output response.

For simplicity, as every MUX is designed equivalently in a MUX PUF, we can model the delay of each single MUX as i.i.d. random variable $D_i$, which follows $N(\mu, \sigma^2)$; therefore, the total delay of
the N stages will be $N(N\mu, N\sigma^2)$. Since the output of arbiter will only depend on the delay difference between the two paths, the time difference will also follow a Gaussian distribution $\Delta \sim N(0, 2N\sigma^2)$.

We denote the delay in the top path of the i-th stage as $Dt_i$, the delay in the bottom path of the i-th stage as $Db_i$, and the challenge bit for each stage as $C_i$. Thus the delay difference of the i-th stage will be:

$$Dt_i - Db_i \sim N(0, 2\sigma^2)$$

Then if the challenge is 0, then the delay difference added into the whole paths will be $Dt_i - Db_i$; otherwise, if the challenge bit for the i-th stage is 1, the additive delay difference will be $Db_i - Dt_i$. It can be expressed as:

$$\Delta_i = (-1)^{C_i}(Dt_i - Db_i) \sim N(0, 2\sigma^2)$$

As a result, the arrival time difference between the two inputs of the arbiter is:

$$\Delta_i = \sum_{i=1}^{N}(-1)^{C_i}(Dt_i - Db_i) \sim N(0, 2N\sigma^2)$$

Thus, the final response is:

$$r = \text{sign}(\Delta_i)$$

where we use the convention that $r = \text{sign}(a) = 0$ when $a < 0$, and $r = \text{sign}(a) = 1$ when $a \geq 0$.

### 3.2 Simulation Model

In our experiment, we use simulation method to test and analyze the performances of PUFs instead of fabrication method. There are several advantages of using simulation method: First of all, fabrication is relatively expensive. Second, a good simulation method can be used as a pre-fabrication test, which can predict the efficiency of a new PUF design before fabrication. Moreover, we can analyze all the possible properties and characteristics of the PUFs under different environmental conditions. Additionally, it is also convenient to follow the shrinking of technology scale.

In our simulation, we apply the Gaussian model which has already been described in Section 3.1 for manufacturing process variations. We set up the process parameters and their max percentages of deviations based on the predictions from [16, 17]. For spatial correlation, we assume perfect spatial correlations within one single MUX. The process variations will have the same effect on the PMOS and NMOS devices in each MUX, while the parameter variations among different MUXs have no correlation.

In our simulation result, the total delay deviation of 100 stages is $\leq \pm 0.4\%$. Since

$$\frac{\sigma_x}{\mu_x} = \sqrt{(1/N)(\sigma/\mu)}$$

and $\mu_x$ increases linearly with N, we can conclude that our result conforms with other published results of 65nm technology, based on the experimental results in [8] that $3\sigma/\mu \approx 5\%$ for a single stage of MUXs. Furthermore, our simulation result of inter-chip variation leads to a Hamming distance range from 22 to 59 bits for a total of 100 stages, while the intra-chip variation is 5.8 bits on average, with a maximum value 13 bits. These results are also in agreement with published results for fabricated chips. Thus, we believe that our simulation delay model is consistent with the industrial manufacturing process variations.

### 4. NOVEL RECONFIGURABLE PUFs

In order to add reconfigurable property into general MUX based silicon PUFs, we must make the challenge-response pairs (CRPs) reconfigurable, which can be used to update the database for an authentication system. The methods can be classified into two categories:

(a) Make the challenge-response pairs reconfigurable directly, by adding some extra circuits into the structure, but without configuring the main PUF circuit. This can be achieved by utilizing some techniques to pre-process the challenge before applying to PUF or pre-process the response before using it for authentication.

(b) Make the PUF circuit reconfigurable, therefore the challenge-response pairs will be reconfigurable as well.

We propose several novel non-FPGA reconfigurable PUFs implementations for the above two categories, which would be more suitable for practical use than FPGA-based techniques. Furthermore, we address the reliability and the security of the PUF performance, as some information of the hidden secrets that an adversary can take advantage of may leak out during reconfigurations.

#### 4.1 Reconfigurable Challenge and/or Response Structures

The reconfigurable structures of PUF are built on the prior work in Physical Unclonable Function, which can also be applied to various types of silicon PUFs as well as other challenge-response based PUFs. Our goal is to develop reconfigurable PUF which is a PUF with a mechanism to transform it into a new PUF with an unpredictable and uncontrollable challenge-response behavior, even if the challenge-response behavior of the original PUF is already known. Additionally, the new PUF inherits all the security properties of the original one.

An early reconfigurable design PUF [9] in the literature treated some challenge bits as the configure data. As an example, the last 10 bits of a 100-bit challenge can be fixed as the configure data, leaving only 90 bits for actual challenge. A user can update the CRPs by applying another 10-bit stream to the last 10 stages of the PUF. However, it is very clear that the reconfigured PUF will have high correlation between different configurations and will be vulnerable to attacks, as this method is similar to adding a certain time difference between the two paths or introducing an interval between the two rising edge signals. Even worse, the performance of the PUF will be greatly degraded, if the cumulative variations in the last 10 stages are relatively large. Due to these disadvantages, this architecture of reconfigurable PUFs cannot generate unpredictable challenge-response behaviors.

Intuitively, adding reconfigurable elements before the challenge applied to the PUF can definitely make the PUF reconfigurable. At the same time, the performance of the original PUF will be preserved. The main structure of this type of reconfigurable PUF is shown in Figure 3.

![Figure 3: Reconfigurable Challenge and Response PUF Structure.](image)

#### 4.1.1 PUF with LFSR

We can adopt the linear feedback shift register (LFSR) as the reconfigurable component. Such a structure is shown in Figure 4. LFSR is an important part of sequence cipher and can be used to generate pseudo-random key stream. We can apply different seeds to the IC to generate various random patterns. Furthermore, we can also alter the characteristic polynomial by utilizing the properties
of reconfigurable linear feedback shift register [18, 19]. Such capability makes it extremely difficult for adversaries to obtain PUF signature. It is important to point out that we can improve the security of the PUF system, by benefiting from the property of the LFSR in cryptography.

![Figure 4: PUF Structure of Using LFSR to Configure the Challenge.](image)

### 4.1.2 PUF with Hash Function

Hash function is a kind of "one-way" function, which means it is easy to compute the hash value for a given message, but hard to find a message with a given hash. Due to the random property of hash function, we can employ a hash function as the reconfigurable element to generate a reconfigurable PUF. This structure can be reconfigured very easily, such as by adding several different lengths of 0’s at the end of every challenge. Additionally, the security of PUF can be increased, due to the "one-way" property of hash function. Many hash algorithms have been investigated and developed in the last years. Currently, the SHA-1 algorithm is the National institute of Standards and technology (NIST) secure hash standard. Several reconfigurable hash function unit architectures have been published in past years [20].

In fact, this structure has already been named as Controlled Physical Unclonable Function in [21], which was described as adding control logic to a PUF structure to prevent an adversary from accessing the PUF directly. Instead of doing a simple hash before the challenges applied to the PUF, we can consider adding another control logic, which would make the CRPs updatable. We propose several reconfiguration methods:

(a) Adding different bit streams into the challenges, e.g., adding different numbers of 0’s at the end of the challenges.

(b) Reordering the challenge stream by certain rules.

(c) Reconfiguring the hash function, by using the reconfigurability of these reconfigurable hash function implementations.

Due to the property of hash function, it is extremely hard for an adversary to model the PUF, even after we configure it several times, since the output of hash function is unpredictable.

### 4.1.3 PUF with Output Recomposition

Another idea is to add an extra reconfigurable component to preprocess the output of the arbiter before using it as an authentication key. One simple example is to use two parallel MUX PUFs to update the CRPs, as shown in Figure 5. In this case, the signal (rising edge) will propagate through 4 paths which are selected by challenges. Then we can select two of the four paths using the configure data and forward to the arbiter to generate the response. We will have a total of 12 possible combinations if we use a 2 parallel MUX PUFs. Therefore, we can reconfigure this architecture 12 times. However, there will be very high correlations among these 12 different combinations. For example, if we know that path 1 is faster than path 2, and path 2 is faster than path 3, then we can conclude that path 1 will be faster than path 3. Therefore, there should be some constraints for the pre-processing, which will decrease the total number of reconfigurations. In fact, there are $N!$ possible cases for ordering N paths based on their arrival time. Therefore, $log_2(N!)$ independent bits can be produced by N paths. We can increase the number of parallel PUFs to obtain more possible combinations to meet the practical application needs. If we want to achieve the entropy limit as $log_2(N!)$, we need to choose the output comparison pairs adaptively, which would increase the design complexity and fabrication area significantly.

![Figure 5: Two Parallel MUX PUF Structure.](image)

However, there will be a problem by employing this structure, since the pre-processing component after the last stage also has variations, which will affect the performance of the PUF. To solve this problem, we can add pre-processing components after the arbiters, as in structure of Figure 6. If we use N parallel MUX-based PUF, we will need 2N-1 arbiters, where we only compare the neighbor paths. This is a concept borrowed from ring oscillator PUF which could ensure there will be no correlation between the output bits of the arbiters, as the comparison pairs are non-cyclic. Therefore, this structure can update its challenge-response behavior in an unpredictable manner.

![Figure 6: MUX PUF Structure of Output Recomposition.](image)

### 4.2 Reconfigurable Circuit Structures

Instead of only making the CRPs reconfigurable by processing the challenge and response directly, we can alter the main circuit to update the challenge-response behavior. This kind of reconfigurable PUFs will have better performance from the security perspective, since it leads to a different PUF circuit after reconfiguration, while the previous method only changes the CRP mapping.

The most important thing in these structures is to ensure the extra circuit will not affect the PUF performance, or more generally,
the extra circuit will have identical effect on the delay of different paths statistically. Otherwise, the behavior of the PUF can be easily predicted which leads to an insecure system.

4.2.1 Reconfigurable Feed-Forward PUF

It has been shown that the security of the MUX PUF in Figure 2 can be improved by adding feed-forward arbiters to it. However, in previous literature, how to choose the feed-forward stages and how many stages are chosen for feed-forward purpose have not been clearly presented. One constraint is trivial: the signal produced by the feed-forward arbiter should arrive earlier than the two signals propagating through the MUX paths. Therefore, we should ensure that there are at least 5-8 stages between stages connected to the input and the output of a feed-forward arbiter. We denote the stages from the input of a feed-forward arbiter to the output of the feed-forward arbiter as a feed-forward component. We consider the following three feed-forward structures:

(a) Feed-forward overlap: This structure has at least one stage overlap between two feed-forward components.

(b) Feed-forward cascade: In this structure, the last stage of a feed-forward component will be the first stage of another feed-forward component.

(c) Feed-forward separate: Here the different feed-forward components will be separated. Thus, there is no stage overlap between any two feed-forward components.

![Figure 7: Feed-Forward Silicon MUX PUF Overlap Structure.](image)

![Figure 8: Feed-Forward Silicon MUX PUF Cascade Structure.](image)

![Figure 9: Feed-Forward Silicon MUX PUF Separate Structure.](image)

In our experimental results, the intra-chip variations are increased by adding non-linearity to the circuits. Among the 3 different structures, the feed-forward cascade structure has the largest intra-chip variation, with 10.7 bit Hamming distance on average with response length of 100 bits, compared to 5.8 bits for non-feed-forward structure.

We can also examine the nature of these different structures theoretically. In the feed-forward structure, some of the challenge bits will be the intermediate stage arbiter outputs instead of the external bits. For example, if there is only one feed-forward component in a MUX PUF, which is from the a-th stage to the b-th stage, the time difference of the b-th stage could be expressed as:

$$\Delta_b = (-1)^{\text{sign}}(\sum_{i=1}^{c-1}(-1)^{C_i}(D_{t_i} - D_{b_i})) (D_{t_b} - D_{b_b})$$

An error occurred in the output of the feed-forward arbiter will also affect the time difference in the b-th stage. Therefore, the error probability of the final response is increased by adding nonlinearity.

In the feed-forward cascade structure, the noise from an earlier feed-forward component will directly affect the output of the next feed-forward arbiter. Therefore, this structure will have the least reliability. From above, we know the time difference of the last stage of the feed-forward arbiter is $\Delta_b$. We assume the c-th stage is the first stage of the next feed-forward component. Then the output of the second arbiter is:

$$C_c = \text{sign}(\sum_{i=1}^{c-1}(-1)^{C_i}(D_{t_i} - D_{b_i}) + \Delta_b)$$

As each output of feed-forward structures will not be affected by the noise from feed-forward arbiters, we expect this structure will have the best reliability.

For structure (c), since there are several stages between two feed-forward components, the noise effect from feed-forward bit will combine with the path difference before the beginning point of the next feed-forward component. If the process variations of these stages are more significant than the noise effect from the feed-forward arbiter, the output of next feed-forward arbiter will also not be affected. The second feed-forward arbiter output of this separate structure is:

$$C_c = \text{sign}(\sum_{i=1}^{c-1}(-1)^{C_i}(D_{t_i} - D_{b_i})) + \Delta_b$$

From above, it can be seen that the mathematical models for the 3 feed-forward structures are different. We find that feed-forward arbiters also enable us to reconfigure the circuit as well as to improve the performance from a security perspective. A basic reconfigurable feed-forward structure that combines overlap and separate approaches is shown in Figure 10.

The structure can be configured among the 3 different structures ((a) overlap, (b) cascade, (c) separate), which will increase the complexity of PUF model. By configuring the PUF, the mathematical model for the PUF will be altered. This makes it infeasible for attackers to break the PUF by only using one single uniform linear model. The delay of MUXs connected after the feed-forward structure (normally just an arbiter) may also affect the delay difference of the two paths. However, this time difference could add into the
total path delay difference both positively and negatively, depending on the select signal. Therefore, the effect of these MUXs would be statistically equivalent to the two paths of original MUX PUF, even if the delay of the added two MUXs vary quite significantly. From above, we conclude that the MUX based PUF will be more secure when feed-forward arbiters are reconfigurable.

4.2.2 MUX and DeMUX PUF

The function of MUX is multiplexing; it selects one of many input signals and forwards the selected signal into a single line. The DeMUX is a device that takes a single input signal that carries many channels and distributes them over multiple output signals. Using DeMUX enables us to select the direction of the propagating signal, and makes the PUF reconfigurable. A basic reconfigurable structure is shown in Figure 11. Instead of propagating the rising edge signal successively, we can choose to skip some stages by adding DeMUX components, which could make the challenge-response behavior reconfigurable and hard to predict. This structure will be harder for attackers to model than the silicon PUF only based on MUX.

5. EXPERIMENTAL RESULTS

All of our experiments have been carried out using SPICE simulations on a 65-nm technology process. We use Monte Carlo method to simulate the effect of process variations and environmental variations. In our simulation, we set up the transistor parameters and process variations based on a major industrial standard model. Each proposed structure has been simulated over at least 20 Monte Carlo runs in SPICE. We simulated 100 MUXs stages for each structure of these silicon PUFs. Accordingly, we need to apply a 100-bit challenge to the PUF to produce a 1-bit response, as a result, 100 different challenges were required to generate the final 100-bit digital signature for each IC.

Simulated PUF Structures: In our experiment, we added 10 feed-forward arbiters into each feed-forward structure of MUX PUF. For instance, the feed-forward arbiters were from stage 1 to stage 11, from stage 11 to stage 21 ... from stage 91 to stage 100 in a feed-forward cascade structure. The feed-forward arbiters were from stage 1 to stage 7, from stage 11 to stage 17 ... from stage 91 to stage 97 in feed-forward separate structure. In a feed-forward overlap structure, the feed-forward arbiters were from stage 1 to stage 51, from stage 6 to stage 56 ... from stage 46 to stage 96. For the reconfigurable feed-forward structure, we also added 10 such arbiters and MUXs structures (as discussed in Section 4.2.1) into the original PUF circuit, which can switch among the 3 different feed-forward structures. Moreover, we also simulated 10 DeMUX components in the MUX and DeMUX PUF. The inputs and the outputs of the DeMUXs were from stage 3 to stage 8, from stage 13 to stage 18 ... and from stage 93 to stage 98. Finally, we simulated an output recombination structure with 20 parallel MUX PUFs. We derived the digital signature by comparing adjacent paths among the total 40 paths. Therefore, except for the first and the last paths, each path was compared to two other paths.

Inter-chip Variations: The inter-chip variations were evaluated by the Hamming distance between two digital signatures which were generated by a same challenge and configure data from different chips. Since we simulated 20 chip instances, we had 20\(^4\)19/2, i.e., 190 possible digital signature comparisons. We provide the maximum and the minimum of these numbers for the inter-chip variations.

Intra-chip Variations: The intra-chip variations were determined by comparing the digital signatures of the same IC under different environmental conditions; in our case, we consider the temperature as the primary environmental factor. It has been shown in our experiment that the intra-chip variations introduced by different temperatures from 0\(^\circ\)C to 100\(^\circ\)C were more significant than the intra-chip variations caused by voltage varying from 1V to 1.2V. The digital signatures of the PUF at 0\(^\circ\)C, 20\(^\circ\)C, 40\(^\circ\)C, 80\(^\circ\)C, 100\(^\circ\)C were obtained; however, we only present the comparisons between 0\(^\circ\)C and 100\(^\circ\)C, as those exhibited the largest variations. We applied 10 different challenges for each IC, and simulated 20 different IC instances. Therefore we had 200 comparisons in total. We provide the maximum and the average of these values of Hamming distance for the intra-chip variations.

Reconfigurability: The reconfigurability was determined by the variations of digital signatures generated by different configure data in a same IC. We fixed the challenge for a reconfigurability test, while we fixed the configure data of the different structures when examining the inter-chip variations and the intra-chip variations. In fact, the challenge-bit lengths were decreased by adding reconfigurable components in the feed-forward structures; therefore, we need to adjust the challenge bits when simulating these reconfigurable structures. We also applied 10 different configure data for each IC, and simulated total 20 different IC instances, which are similar to intra-chip variation test. All the simulations were done under the environmental condition of 25\(^\circ\)C and 1.1V.

Table 1 presents the inter-chip variations and intra-chip variations for different MUX Physical Unclonable Function structures. First, it can be observed that the minimum inter-chip variations are larger than the maximum intra-chip variations for all of the simulated structures. Thus, we can conclude that the variations caused by the randomness in manufacturing process are more significant than the variations under different environmental conditions. Therefore, these PUFs can be used as reliable secret keys with some error correcting techniques. Second, it can also be observed that by adding feed-forward arbiters into the MUX PUF circuit, the inter-chip variations and intra-chip variations are both increased, since the noise can have influence on the select signals of some intermediate stages. By comparing the inter-chip variations and the intra-chip variations, we can say that the feed-forward separate structure is the most reliable structure while the feed-forward cascade is the least reliable one among the 3 feed-forward structures. The reconfigurable feed-forward structure has very close performance to the 3 types of feed-forward structures, since its functionality is switching among the 3. Moreover, the reconfigurable MUX and DeMUX PUF has similar inter-chip variation as the non-feed-forward structure, but the intra-chip variation is increased, as the number of stages may be reduced by configurations. Therefore, the reliability of this structure is decreased.
Table 1: Simulation Results: Variations

<table>
<thead>
<tr>
<th>Structures</th>
<th>Inter-chip Variation</th>
<th>Intra-chip Variation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max</td>
<td>Min</td>
</tr>
<tr>
<td>Non-feed-forward</td>
<td>59</td>
<td>22</td>
</tr>
<tr>
<td>Feed-forward Overlap</td>
<td>66</td>
<td>27</td>
</tr>
<tr>
<td>Feed-forward Cascade</td>
<td>64</td>
<td>25</td>
</tr>
<tr>
<td>Feed-forward Separate</td>
<td>65</td>
<td>26</td>
</tr>
<tr>
<td>Reconfigurable Feed-forward</td>
<td>65</td>
<td>25</td>
</tr>
<tr>
<td>MUX and DeMUX</td>
<td>57</td>
<td>25</td>
</tr>
</tbody>
</table>

Table 2 shows the reconfigurability of each reconfigurable structure. It can be seen that the output recombination structure has the best reconfigurability, i.e., by fixing the challenge bits and only changing the configure data, the digital signature of this structure has the most significant variations. In our simulation results, the average variation is 38.7 bits. The MUX and DeMUX PUF exhibits the least reconfigurability. This is because the function of the DeMUX is only to determine whether to skip some stages or not. When the process variations of other stages are relatively large, the difference of digital signatures with two different configure data may only vary a little bit. For the output recombination structure, it is similar to comparing different paths with different configurations. Therefore, its performance is close to the inter-chip variation of the non-feed-forward MUX PUF. It also can be observed that although the challenge hash structure and the challenge LFSR structure are both pre-processing the challenge before applying to the circuit, their reconfigurability still has some difference. As the challenge LFSR appears to have better reconfigurability, we can conclude that the number generated by the LFSR in our case may have better randomness than that of the hash function. Finally, the proposed reconfigurable feed-forward MUX PUF has the average Hamming distance 32.4 bits by different configurations, which will be sufficient to be used as a secure and reliable secret key storage method, considering its complex and nonlinear functionality.

Table 2: Simulation Results: Reconfigurability

<table>
<thead>
<tr>
<th>Structures</th>
<th>Variation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max</td>
</tr>
<tr>
<td>Challenge LFSR</td>
<td>44</td>
</tr>
<tr>
<td>Challenge Hash</td>
<td>45</td>
</tr>
<tr>
<td>Output Recombination</td>
<td>57</td>
</tr>
<tr>
<td>Reconfigurable Feed-forward</td>
<td>47</td>
</tr>
<tr>
<td>MUX and DeMUX</td>
<td>47</td>
</tr>
</tbody>
</table>

Overall, all the proposed reconfigurable structures have considerable reconfigurability, and can be used for reliable authentication and identification within certain error tolerance, as the minimum of the inter-chip variations is larger than the maximum of intra-chip variations. The output recombination structure has the best reconfigurability; however, the reconfigurable feed-forward MUX PUF has the best performance due to its security, as it is extremely hard to be modeled by linear modeling methods.

6. CONCLUSION

We have presented several reconfigurable silicon MUX Physical Unclonable Functions based on two major approaches and demonstrated their effectiveness by experimental results via inter-chip variation and intra-chip variation. We also have discussed the reliability perspective of PUFs and proposed several methods to increase the security. Ongoing work includes novel highly secure and reliable reconfigurable PUF designs and their mathematical analysis. Furthermore, we are also interested in developing an authentication scheme for reconfigurable PUFs, which will use several pairs of CRPs as a set for authentication by utilizing the reconfigurable property of reconfigurable PUFs.

7. REFERENCES

Verification of Information Flow Properties in Cyber-Physical Systems

Bruce McMillin and Ravi Akella
Department of Computer Science
Intelligent Systems Center
Rolla, MO, United States 65409-0350
Email: ff@mst.edu, ravi.akella@mst.edu

Abstract—Information flow typically refers to the explicit as well as implicit information resulting from the interaction of cyber processes constituting a system. Information flow also occurs in cyber-physical systems (CPSs). Information flow is difficult to detect in CPSs, due to their physical nature and complex interactions among various computational and physical components. In this work, formal methods of security specification and verification are extended to describe confidentiality in CPSs. This paper presents a general approach to specify and verify information flow properties, such as non-deducibility, in a CPS using bisimulation techniques.

I. INTRODUCTION

Information flow refers to the explicit as well as implicit information that could be the result of communication among various processes constituting the system. In multi-level systems, determining information flow from a high-level domain to the low-level domain violates confidentiality in most cases. Information flow properties like Non-interference, Non-deducibility [1] and extensions [2] are studied in literature that deal with preventing information from being downgraded through covert channels and other such potential causes. This work extends the application of these information flow properties to more complex cyber-physical systems (CPSs) which are integrations of physical and computational processes.

In CPSs, due to physically observable cyber and physical events, information flow is complex resulting in a greater risk of confidentiality and privacy violations. For example, “smart metering” in smart grids involves the collection of private data of consumers to manage the resources efficiently. Failure to monitor the usage of such information could pose an increased threat to the privacy of the consumers [3].

Cyber-physical interactions result from the coupling of the information and physical flows in a CPS. In a CPS, cyber processes interact with physical components for actuating control and monitoring. The key challenge is to represent the physical nature of the system. Invariance of flow, such as power flow that satisfies Kirchoff’s laws, forces execution of any event within the system to satisfy the invariant. Information flow vulnerabilities are a natural consequence of this interdependence of actions in the cyber and physical domains. In other words, an observation about physical flow could permit an observer to infer possibly sensitive cyber actions. The physical components that are exposed to any observer outside the CPS divulge some information regarding the system (physically observable behavior). For example, the operation of a wind turbine in a smart grid depends on its physical size, velocity of wind, etc., that are observable. Definitions of High and Low level domains change according to the physical location of the observer on the CPS; for example, an observer controlling a physical component knows more about the system than an external observer (with only physical observability). To completely analyze the information flow, various cases of such observers should be accounted for, that reveal the extent of confidentiality violation within the system [4] as in Fig. 1.

Security considerations for a CPS, therefore, depend on cyber information flow, physically observable behavior, and the interactions among the cyber and physical components of the system. Due to infrastructure interdependencies [5] [6], a compromise in the security of one system may threaten another system. For example, the information flow resulting from the composition of a power electric flow controller, with a distributed control, affects the security of the power grid. Timing, security [7] and frequency [8] are key properties that have an impact on the confidentiality of a system. The complexity of these interactions exceeds the ability of informal information flow analysis. Information flow theory [9] provides an attractive formal method to

![Fig. 1. Different levels of confidentiality violation possible in a CPS](image-url)
quantify information flow, but it is not automated. Process algebras [10] provide both a rigorous system specification and associated verification (model checking) procedures, but are rarely used because of their complexity.

In this work, a methodology has been adopted that addresses the aforementioned issues for the information flow verification of CPSs. Security process algebra (SPA) [2] is used to specify the CPS as a communicating set of concurrent processes and bisimulation techniques from literature are presented to be useful to verify non-deducibility in the composed system. Section II introduces some aspects of SPA and bisimulation-based non-deducibility on composition (BNDC) [2], which are vital to the approach presented. In section III, the proposed approach for the analysis of information flow is discussed. Finally, conclusions and future work are presented in section IV.

II. BACKGROUND

A. SPA

Security Process Algebra (SPA, for short) [2] is an extension of the Calculus of Communicating Systems (CCS) [10]. Any system can be defined as: \( E := 0 \cup E_1 + E_2 | E_1| E_2 | E_1 \setminus L | E_1 \setminus 1 | E_1 \setminus 2 | f | Z \), where 0 is the empty process, which cannot do any action; \( \mu.E \) can do action \( \mu \) and then behaves like \( E \); \( E_1 + E_2 \) can alternatively choose to behave like \( E_1 \) or \( E_2 \); \( E_1 | E_2 \) is the parallel composition of \( E_1 \) and \( E_2 \), where the executions of the two systems are interleaved, \( E \setminus L \) can execute all the actions \( E \) is able to do, provided that they do not belong to \( L \cup \tilde{L} \) (\( \tilde{L} \) refers to the output). The operation \( E_1 \parallel E_2 \) represents the synchronized parallel composition of \( E_1 \) and \( E_2 \) upon the events from set A.

B. Bisimulation-based Non-Deducibility on Composition Model

Bisimulation [10] is an equivalence technique based on the idea that two states of the system can be distinguished if the distinction can be detected by a process interacting with the system. A system is considered to have the BNDC property if it can preserve its security after composition [2]. A system \( ES \) is BNDC if for every high-level process \( \Pi \), a low-level user cannot distinguish \( ES \) from \( ES||\Pi \) (\( ES \) composed with process \( \Pi \)). In other words, a system \( ES \) is BNDC if what a low-level user sees in the system is not modified by composing any high-level process \( \Pi \) with \( ES \). \( BNDC(ES) \equiv \forall \Pi \in E_H, ES \setminus H \approx_B (ES||\Pi) \setminus H \) where \( ES \setminus H \) changes all the H events in \( ES \) into internal silent actions represented as a sequence of \( \tau \) actions. A system is BNDC-preserving if the above property holds for all possible behaviors of the system.

III. ADVANCED ANALYSIS

A formal methodology to automate the process of verifying confidentiality of information flow within a CPS involves addressing three main issues.

A. Representation of cyber and physical processes and their interactions into computational framework

A process algebra (as in section II-A) can be used to model the CPS as a composition of cyber and physical processes that communicate concurrently, if possible, in a synchronized manner. Each process is defined as a sequence of events within the system which determine different states the system could transition into. In [7], SPA has been used to represent the physical actions interacting with the computational elements in a gas pipeline network. A similar approach has been taken in [4], to analyze information flow within a more complex smart grid that uses advanced distributed algorithms to manage the underlying physical resources like renewable energy sources, house loads, power storage etc.

The physical network in a CPS forms a continuous time subsystem and the computational part forms a discrete event subsystem. SPA is not equipped to model the continuous-time nature of physical processes in a CPS. To capture the information flow of the combined system thereby forces the modeling of the continuous physical subsystem to be event-based, so that the physical events can be captured using process algebra. Physical events include 1) a local state change of the physical subsystem resulting from a cyber component controlling it (for example, a power flow controller increases/decreases voltage on the power line causing a flow change) or 2) a local physical state change brought by the dynamics of the physical network (for example, load on a power line increases/decreases as a stochastic process to which the power electronics react by making a setting). Invariance on physical flow can be modeled such that events that change the flow at various physical components are reflected in an aggregate flow that satisfies the invariant. The impact of physically observable behavior cannot be ignored to study information flow in CPSs. This forces the observable actions to be considered as events that are used as building blocks of process specification.

Cyber events within a CPS involve in distributed computation based on 1) communication with other cyber components or 2) communication with the physical component that it controls. Composition of cyber processes result in the transformation of complementary actions of the processes into internal silent actions in the composed process, defined by the SPA ‘\( \parallel \)’ operator as below:

\[
E_1 \parallel_{\alpha} E_1 \xrightarrow{\alpha} E_2 \xrightarrow{\beta} E_2' = E_1'| E_2' \\
E_1 \parallel E_2 \xrightarrow{\sigma} E_1'| E_2'
\]

(1)

The communication between physical processes is different from that between cyber processes; in the former case, the pair of processes make a synchronized physical change on the shared network (such as power transfer on the shared power bus from a component with high potential to a component with lower potential) and in the latter case, the pair of processes synchronize on complementary request/response type
messages. Methods to counter interception of messages on the communication channel exist, validating the assumption that cyber processes can be securely composable as long as they perform complementary actions. By contrast, physical change between two physical processes is observable by an intermediary in the path of their ‘direct communication’, making it difficult to securely model such composition. Using the proposed approach, CPSs can be modeled in terms of SPA followed by bisimulation-based equivalence testing of the processes as outlined in section III-B.

B. Adequacy of Bisimulation-based Non-deducibility properties for CPS Models

According to the definition of BNDC (II-B), the SPA specification of the system has to be composed with all the high-level processes (II) that can be modeled using the high-level actions of the system. However, this would significantly increase the complexity of verification of BNDC property since it should be verified that \( E \setminus H \approx_B (E \cup H) \setminus H \), for all \( H \). This definition of SBNDC implies that the system before and after executing a high-level action remains indistinguishable.

To avoid such universal quantification on \( H \), a strong form of BNDC called strong BNDC (or SBNDC) has been proposed in [11]. SBNDC states that if \( E' \) reachable from \( E \), then \( E' \setminus H \approx_B E'' \setminus H \). This definition of SBNDC implies that the system before and after executing a high-level action remains indistinguishable.

Such a definition avoids the fact that the property should hold for all possible high-level processes within the system, transforming the bisimilarity relation between \( E \) and \( E \cup H \), with \( E \setminus H \) i.e., it will be verified that \( E \approx_B \setminus H, E' \setminus H \) with the high-level actions replaced with silent internal action, \( \tau \). The bisimilarity up to \( H \) relation for SBNDC \( \approx_B^{\tau} \setminus H \) transforms the high-level events in \( E' \) into a sequence of \( (Z^0) \) or zero actions. An exhaustive study of BNDC and its variants is presented in [11]. The impact of silent internal actions on weak bisimulation relation is equivalent to that defined in CCS [10].

1) SBNDC verification on a test CPS model: In this section, the approach outlined above is generalized for an informally specified CPS. Assuming a homogeneous CPS with identical cyber and physical components on the system, we can define the events as below:

Events at a given cyber process (represented as Cyber):
- \( RS \): Read local physical state, \( CO \): Compute, \( IC \): Issue command to a local physical controller, \( Send \): Send message to peer cyber components, \( Recv \): Receive message from peer cyber components.

Events at a given physical process (represented as Physical):
- \( IN \): Change due to invariant maintenance, \( PO \): Physical Observability, \( SC \): Local state change, \( EC \): Execute command from cyber component.

The rest of the system can be built up from these events in a bottom-up fashion as shown in Equations 2 through 6.

\[
\begin{align*}
Cyber & \cong RS.CO.IC.Cyber + RS.CO.Send.Cyber + \\
& Recv.CO.IC.Cyber \\
Physical & \cong PO.SC.IN.Physical + PO.EC.Physical \\
Node & \cong Cyber|Physical \\
Invariant & \cong (IN_1.Invariant + IN_2.Invariant) \\
& + \tau.Invariant \\
System, E & \cong (Node_1|Node_2...)Invariant
\end{align*}
\]

\( (IC, EC \) are complementary Input/Output pair. Similarly, \( SC \) and \( RS \) form a complementary I/O pair.) For an observer internal to the system the events pertaining to rest of the system can be classified as, \( High = \{ RS, CO, IC, EC, Send \} \) and \( Low = \{ PO, IN, Recv \} \).

To verify whether this system satisfies SBNDC, we proceed as follows: Unwinding \( E \) in terms of the events that define it and using the definition of composition (as in Equation 1), a possible state \( E' \) (such that \( E \rightarrow E' \)) can be defined as:

\[
\begin{align*}
E' & \cong PO.\tau.IC.Node + \tau.CO.IC.Node + \\
& EC.\tau.t.PO.CO.IC.Node + PO.\tau.CO.Send.Node \\
& + \tau.CO.Send.Node + EC.\tau.CO.Send.\tau.PO.Node \\
& + Recv.\tau.SC.\tau.PO.Node
\end{align*}
\]

Now,

\[
\begin{align*}
E' \setminus H & \cong PO.\tau.Node + Recv.Node
\end{align*}
\]

The bisimulation up to \( H \) on \( E' \) yields

\[
\begin{align*}
E' & \cong 0_H \setminus H PO.\tau.Node + \tau.Sc.PO.\tau.Node
\end{align*}
\]

From Equations 8 and 9, \( E' \not\cong 0_H \setminus H \). This proves that the generic CPS defined above does not satisfy SBNDC. The trace that resulted in the failure of SBNDC is \( \tau.Sc.PO.\tau.Node \) implying that on receiving a message, the \( Node \) performs an internal action, a State Change event, followed by an internal action to maintain the Invariant which is physically observable (for example, due to the voltage drop at a node on the power line, a small change is observed by a neighboring node sharing the physical line). In practice, such a physical change can be hidden through coordination with other nodes in which the following takes place: if one node makes a change, the other node(s) perform(s) a compensating event [12] [13]. This process \( E' \) can now be made SBNDC by adding a complementary
event such that the effect of the PO event is nullified. Therefore, the system trace \( \text{Recv}.\tau.\text{SC}.\tau.\text{PO}.\text{Node} \) in Equation 7 can be modified as \( \text{Recv}.\tau.\text{SC}.\tau.\text{PO}.\text{Node} \cong \text{Recv}.\tau.\text{SC}.\tau.\text{Node} \). The modified \( E' \) will have the following characteristics.

\[
E'_\text{Modified} \cong H \cong \text{PO}.\tau.\text{Node} + \text{Recv}.\tau.\text{Node} \tag{10}
\]

\[
E'_\text{Modified} \cong H \cong \text{PO}.\tau.\text{Node} + \text{Recv}.\tau.\text{Node} \tag{11}
\]

Thus, \( E'_\text{Modified} \) satisfies the SBNDC property. Similarly, it is verified for every \( E' \) reachable from \( E \) whether \( E' \) and \( E' \setminus H \) belong to the bisimilarity up to \( H \) relation. The possibility of multiple observers coordinating in an effort to deduce more information pertaining to the system is a challenging task that needs to be well addressed. Thus, the SBNDC property and its weak forms are sufficient for CPS verification (in many cases). This process reduces the problem of verifying the BNDC property on the SPA model of the CPS into verifying a bisimulation relation between all the reachable states of the system. The above approach was performed on the SPA model of a two node smart grid (such as in [14]) that includes renewable energy sources, power electronics and battery to define the Physical process that satisfies a global invariant function of physical flow and optimization algorithms that define the Cyber process. Such a complex interaction of cyber and physical processes resulted in over 3600 states (using an automated model checker) the system could transition into. The problem of verifying the bisimilarity equivalence between \( E \) and \( E' \setminus H \) is the next logical step to perform complete system evaluation.

C. Testing for Bisimulation Equivalence of Processes

Two processes are bisimilarly equivalent if there exists a bisimulation relation including both the processes as a pair. This problem of equivalence testing has been well studied in literature [15] [16] as a relational coarsest partition problem: given a relation, \( R \) (Bisimilarity) and an initial state, \( E \) over a global set of states \( \xi \), find the coarsest stable refinement which is such that either \( E \subseteq R^{-1}(E' \setminus H) \) or \( E \cap R^{-1}(E' \setminus H) = \phi \). This verification is performed for all the states \( E' \in \xi \) such that \( E \rightarrow E' \). The efficiency of equivalence testing can be improved by the development of algorithms that minimize the state space using advanced techniques of bisimulation and partial order reduction, as in [17].

IV. Conclusions and Future work

In this work, information flow analysis, with its origins in computational systems, has been extended to the realm of cyber-physical systems to verify their security, thereby exposing potential confidentiality violations. In [4], such an analysis has been shown to uncover various levels of confidentiality violation within a smart grid architecture (called FREEDM [14]). The approach presented provides a preliminary but powerful method of verifying the confidentiality within a CPS. Future work involves development of generalized bisimulation-based security properties and development of algorithmic techniques to reduce the state space for equivalence testing in cyber-physical systems.

REFERENCES

Secure Data Transmission Protocol in Multi-Hop Sensor Networks
Yilin Mo, Bruno Sinopoli

Abstract—In this paper, we discuss how to design secure data transmission protocol in wireless sensor networks. The network is assumed to have \( p \) sensors and \( n-p \) routers which relay the observations from the sensors to the fusion center. A maximum of \( f \) routers can be compromised by an adversary. The fusion center wants to detect and identify malicious nodes in the system and reconstruct the observations. Due to computational constraints, we could not use advance information security technique, such as digital signature to protect the integrity of the data. Instead, we model the whole network as a linear system. By leveraging fault detection and identification theory and generic properties of structured system, we can provide a necessary and sufficient condition for generic detectability of the malicious nodes and reconstructability of the observations, which is related to the topology of the network. We also show that resilience can be further improved by using trustworthy nodes.

I. INTRODUCTION

Design and analysis of systems based on sensor networks involve cross disciplinary research spanning domains within computer science, communication systems and control theory. A sensor network is composed of low-power devices that integrate computing with heterogeneous sensing and communication. Sensor network based systems are usually embedded in the physical world, with which they interact by collecting, processing and transmitting relevant data.

Sensor networks span a wide range of applications, including environmental monitoring and control, health care, home and office automation and traffic control [1]. Many of these applications are safety critical. Any successful attack may significantly hamper the functionality of the sensor networks and lead to economic losses. In addition, sensors in large distributed sensor networks may be physically exposed, making it difficult to ensure security and availability for each and every single sensor. The research community has acknowledged the importance of addressing the challenge of designing secure estimation and control systems [2] [3].

The impact of attacks on control systems is discussed in [4]. The authors consider two possible classes of attacks on CPS: Denial of Service (DoS) and deception (or false data injection) attacks. The DoS attack prevents the exchange of information, usually either sensor readings or control inputs between subsystems, while a false data injection attack affects the data integrity of packets by modifying their payloads. A robust feedback control design against DoS attacks is discussed in [5]. We feel that false data injection attacks can be a subtler attack than DoS as they are in principle more difficult to detect. In this paper we want to analyze the resilience of data transmission protocol against such types of attacks.

Secure data transmission protocols have been extensively studied by the information security community. Many tools, such as digital signature, have been developed to protect data integrity. However, these cryptographic methods are usually computationally expensive and may not be applicable in sensor networks, in which sensors usually have limited computational power.

Another approach is to model the data transmission protocol as a linear system and malicious behavior in the network as an external input. Therefore the whole problem of detection and identification of malicious nodes can be reformulated as a fault detection and identification (FDI) problem. Over the past few decades, a significant amount of research effort has been spent on FDI problems [6], [7]. Recently, Pasqualetti et al. [8] and Sundaram et al. [9] show how to use FDI to detect and identify malicious behavior in consensus algorithm and wireless control networks. In this paper, we discuss how to use FDI to design a secure data transmission protocol in sensor networks. The network is assumed to have \( p \) sensors and \( n-p \) routers which relay observations from the sensors to the fusion center. A maximum of \( f \) routers can be compromised by an adversary. The fusion center wants to detect and identify malicious nodes in the system and reconstruct the observations. We show that the achievability of such goals is determined by the topology of the network. We also provide a way to increase the resilience of the network by using trustworthy nodes.

The rest of the paper is organized as follows: in Section II, we introduce the sensor network model and the attack models. We also introduce the concepts of weak and strong resilience. In Section III, we prove a necessary and sufficient condition for the network to be weakly or strongly resilient to the attack based on network topology. In Section IV, we propose a way to enhance the resilience of the network by using trustworthy routers. Finally Section V concludes the paper.

II. PROBLEM FORMULATION

In this section we want to introduce the system which will be discussed in the rest of the paper.

A. System Description

Consider a set of \( p \) sensors \( S = \{1, \ldots, p\} \) monitoring the environment. At each time step \( k \), each sensor makes a scalar observation denoted as \( w_{k,i} \). To simplify notation, let us define the measurement vector \( w_k = [w_{k,1}, \ldots, w_{k,p}]' \in \mathbb{R}^p \).

The sensors need transmit their measurements back to the fusion center. However, due to certain constraints, such
as energy or bandwidth, they cannot directly communicate with the fusion center. As a result, a multi-hop network is used to relay the observations from the sensors to the fusion center. We assume that the network consists of \( n - p \) routers \( \{p + 1, \ldots, n\} \), where \( n \geq p \) and the fusion center is listening to the last \( m \) \((m \leq n)\) nodes \( \{n - m + 1, \ldots, n\}\), the set of which is denoted as \( T \).

We model the whole network (both the routers and sensors) as a directed graph \( G = (V, E) \). \( V \triangleq \{s_1, \ldots, s_n\} \) is the set of vertices\(^1\). \( E \subseteq V \times V \) is the set of edges. \((i, j) \in E \) if and only if node \( i \) can transmit to node \( j \) directly. We denote the set of incoming neighbors of node \( i \) as

\[
N_i^I = \{ j \in V : (j, i) \in E \},
\]

and the set of outgoing neighbors as

\[
N_i^O = \{ j \in V : (i, j) \in E \},
\]

The topology of the network is illustrated in Fig 1.

Let \( W \) and \( W' \) be two subset of \( V \). A path from \( W \) to \( W' \) is a sequence of vertices \( i_1, \ldots, i_k \), where \((i_j, i_{j-1}) \in E, i_1 \in W \) and \( i_k \in W' \). A path is called simple if there is no repetition of vertices. Two paths are disjoint if they do not share common vertex. We call \( l \) paths from \( W \) to \( W' \) disjoint if they are mutually disjoint, i.e. any two of them are disjoint. A set of \( l \) disjoint and simple paths from \( W \) to \( W' \) is called a linking of size \( l \) or an \( l \) linking from \( W \) to \( W' \).

We assume that at each step, a node can only broadcast one scalar to its outgoing neighbors due to the bandwidth and energy constraints. One way for the fusion center to recover the observations \( w_k \) is to construct a \( p \) linking from \( S \) to \( T \). Each node in the \( p \) linking simply forwards the messages from the incoming neighbor to its unique outgoing neighbor in the linking.

In this paper we want to study a more general transmission scheme. Instead of simply relaying the messages, each sensor computes a linear function of the messages from its incoming neighbors and its own state and broadcasts the result to the outgoing neighbors. To be specific, suppose each node keeps a state \( x_{k,i} \), where \( k \) is the time index and \( i \) is the node index. At each time step, each node \( i \) broadcasts its state to its outgoing neighbors,

\[
z_{k,i,j} = x_{k,i}, j \in N^O(i),
\]

where \( z_{k,i,j} \) is the data transmitted from node \( i \) to node \( j \) at time \( k \). Each node \( i \) receives the data from all its incoming neighbors, it performs an update as follows:

\[
x_{k+1,i} = a_{i,i}x_{k,i} + \sum_{j \in N^I(i)} a_{i,j}z_{k,j,i} + \sum_{j \in S} \delta_{j,i}w_{k,j},
\]

with initial condition \( x_{0,i} = 0 \), and \( \delta_{j,i} = 1 \) if \( i = j \) and is 0 otherwise.

To simplify notation, let us define \( x_{k} = [x_{k,1}, \ldots, x_{k,n}]' \in \mathbb{R}^n \). \( A \triangleq [a_{i,j}] \in \mathbb{R}^{n \times n} \) and \( B \triangleq [e_1, \ldots, e_p] \in \mathbb{R}^{n \times p} \), where \( e_i \triangleq [\delta_{1,i}, \ldots, \delta_{n,i}]' \in \mathbb{R}^n \). (4) can be written in the matrix form as

\[
x_{k+1} = Ax_k + Bw_k, x_0 = 0.
\]

\(^1\)We use vertex or node to denote both sensors and routers.

Define \( C = [e_{n-m+1}, \ldots, e_n]' \in \mathbb{R}^{m \times p} \). At each time the fusion center receives

\[
y_k = [x_{k,n-m+1}, \ldots, x_{k,n}]' = Cx_k.
\]

\( S \)

\( T \)

Fig. 1. Multi-Hop Sensor Networks

B. Attack Model

In this section we describe the attack model. We assume that several routers are compromised\(^2\). We model the malicious behavior of a compromised router as an external input. To be specific, we assume the compromised router follows the following update rule

\[
x_{k+1,i} = a_{i,i}x_{k,i} + \sum_{j \in N^I(i)} a_{i,j}z_{k,j,i} + u_{k,i}.
\]

Remark 1. If a compromised router chooses \( u_{k,i} = 0 \) for all \( k \), then there is no chance for the fusion center to detect it since it behaves exactly as a benign node. Moreover the compromised router does no damage to the network. Therefore, we assume that each compromised router uses a non-zero \( u_{k,i} \) for at least once.

The set of compromised routers is denoted as \( F \), which is assumed to be unknown to the fusion center in the beginning. However, we assume that \(|F| \leq f \), where \( f \) is known to fusion center. Let us denote \( F \) as the set of all possible \( F \), which is denoted as\(^3\)

\[
F = \{ F \subseteq V : |F| \leq f, \bigcap F = \emptyset \}.
\]

It can be seen that the capability of the attacker is completely characterized by \( F \). As a result, we will call such attack an \( F \)-attack.

Define \( B^F = [e_{i_1}, \ldots, e_{i_j}] \), where \( F = \{i_1, i_2, \ldots, i_j\} \). Then the update equation can be written as

\[
x_{k+1} = Ax_k + Bw_k + B^F u_k^F.
\]

\(^2\)We assume the sensors are always benign in the whole paper.

\(^3\)Note that the empty set \( \phi \) also belongs to \( F \).
Next we define the concept of resilient to $F$-attacks:

**Definition 1.** The system is called weakly resilient to the $F$-attacks if and only if

\[ \Phi(w, u^F, F) = \Phi(0, 0, \phi) \]

implies that $F = \phi$ and $w = 0$.

**Definition 2.** The system is called strongly resilient to the $F$-attacks if and only if

\[ \Phi(w, u^F, F) = \Phi(w', u'^F, F') \]

implies that $w = w'$, $u^F = u'^F$, and $F = F'$.

The following theorems relate the weak and strong resilience to the detectability of the attack and reconstructability of the sensor measurements.

**Theorem 1.** If the system is weakly resilient to the $F$-attacks, then the system can successfully detect any $F$-attack.

*Proof:* If there is no attack, then the trajectory of the output will be in the following set

\[ \mathcal{Y}_\phi = \{ y = \Phi(w, 0, \phi) \} \]

When an attack is present, the trajectory will be in the following set

\[ \mathcal{Y}_F = \{ y = \Phi(w, u^F, F) \} \]

The system can detect the attack if and only if $\mathcal{Y}_\phi \cap \mathcal{Y}_F = \phi$. Now suppose the opposite, i.e., $\mathcal{Y}_\phi \cap \mathcal{Y}_F \neq \phi$. Then there exists $w, w', u^F, F \neq \phi$, such that

\[ \Phi(w, 0, \phi) = \Phi(w', u^F, F) \]

By linearity of the system, we have

\[ \Phi(0, 0, \phi) = \Phi(w' - w, u^F, F) \]

which further implies that $F = \phi$ due to the weak resilience. However, that contradicts the assumption that $F \neq \phi$. Thus $\mathcal{Y}_\phi \cap \mathcal{Y}_F = \phi$ and the system is able to detect the attack. 

**Theorem 2.** If the system is strongly resilient to the $F$, then given $y$, the system can successfully identify the set of malicious nodes $F$ and reconstruct the input $w$.

*Proof:* Suppose $F$ is the set of compromised nodes. Define

\[ \mathcal{Y}_F = \{ y = \Phi(w, u^F, F) \} \]

The set of malicious nodes can be identified if and only if $\mathcal{Y}_{F'}$, for all $F \in \mathcal{F}$ are mutually disjoint. Now consider the opposite, there exists $F_1 \neq F_2$ and $\mathcal{Y}_{F_1} \cap \mathcal{Y}_{F_2} \neq \phi$, which implies that

\[ \Phi(w, u^{F_1}, F_1) = \Phi(w', u^{F_2}, F_2) \]

for some $w, w', u^{F_1}, u^{F_2}$. However, due to strong resilience, $F_1 = F_2$, which contradicts the assumption that $F_1 \neq F_2$. Hence, the system can identify the set of malicious nodes.

The reconstructability follows directly from the fact that $w$ is uniquely determined by $y = \Phi(w, u^F, F)$.

In the next section we will relate the concepts of weak and strong resilience to the topology of the network.

### III. Main Result

In this section we will characterize the resilience of the network by studying its topology.

#### A. Algebraic Conditions

First, we wish to relate the concepts of strong and weak resilience via the following theorem.

**Theorem 3.** A system is strongly resilient to the $F$-attacks if and only if it is weakly resilient to the $G$-attacks, where the set $G$ is defined as

\[ G = \{ P \subset V : P = F_1 \cup F_2, F_1, F_2 \in \mathcal{F} \} \]

*Proof:* First let us prove that $F$ strong resilience implies weak resilience to $G$-attacks. We prove that by contradiction. Suppose not, then there exists $G \in G$ and $G \neq \phi$, such that

\[ \Phi(w, u^G, G) = \Phi(0, 0, \phi) \]

From definition, we know that $G = F_1 \cup F_2$, where $F_1, F_2 \in \mathcal{F}$ and $F_1 \neq F_2$. It can be shown that

\[ u^G = u^a + u^b \]

where $u^a$ ($u^b$) is non-zero only for the nodes that belong to $F_1$ ($F_2$). By linearity, it can be proved that

\[ \Phi(w, u^a, G) = \Phi(0, -u^b, G) \]

Moreover, we can find $u^{F_1}$ and $u^{F_2}$ such that

\[ \Phi(w, u^{F_1}, F_1) = \Phi(0, -u^b, F_2) = \Phi(0, -u^b, G) \]

which contradicts the fact that the system is strongly resilient to $F$-attacks.

The proof of the converse is similar and hence is omitted.

As a result, we only need to consider weak resilience. The following definition is needed:

**Definition 3.** Consider a linear system $(A, B, C)$ of the following form:

\[
\begin{align*}
x_{k+1} &= Ax_k + Bu_k, \quad x_0 = 0, \\
y_k &= Cx_k.
\end{align*}
\]

The system is called left-invertible if $y_k = 0$ for all $k$ implies that $u_k = 0$ for all $k$.

From the definition, it is easy to see that the following theorem holds.

**Theorem 4.** The network is weakly resilience to $F$-attacks if and only if for all possible $F \in \mathcal{F}$, the system $(A, [B B^F], C)$ is left-invertible.

The following theorem characterize the relationship between the left invertibility and $(A, [B B^F], C)$. 


4Note that we assume that for each compromised node, $u_{k,i}$ will be non zero for at least once.
Theorem 5 ([10]). The following statements are equivalent:

1) The system \((A, B, C)\) is left invertible.
2) The transfer function \(K(z) = C(zI - A)^{-1}B\) has normal rank\(^5\) \(m\).

Once the matrix \(A\) is specified, one can use the above theorem to check if the system is weakly or strongly resilient to \(F\)-attacks. However, this could be cumbersome since one needs to check for all the possible \(F \in F\). Moreover, the above theorem does not provide any insight on the relationship between network topology and resilience. In the next subsection, we characterize such relationship, based on the generic properties of structured systems.

B. Topological Conditions

In this subsection, we want to relate weak and strong resilience with the topology of the network. We first introduce the concept of structured system. Consider the linear system

\[
x_{k+1} = Ax_k + Bu_k, \quad y_k = Cx_k.
\]

The system is structured if the elements of matrices \(A, B, C\) are either fixed zeros or free parameters. Suppose that there are \(l\) elements in \(A, B, C\) matrices that are not fixed zeros. We can parameterize the system by a vector \(\lambda \in \mathbb{R}^l\). As a result, we will write the structured system as

\[
x_{k+1} = A_\lambda x_k + B_\lambda u_k, \quad y_k = C_\lambda x_k.
\]

A structured linear system can be represented by a directed graph \(H = (V_H, E_H)\), where \(V_H = U \cup X \cup Y\). \(U = \{u_1, \ldots, u_p\}\), \(X = \{x_1, \ldots, x_n\}\) and \(Y = \{y_1, \ldots, y_m\}\) represent the inputs, states and outputs respectively. \(p, n, m\) are the dimensions of inputs, states and outputs. The edge set is defined as

\[
E_H = \{(u_j, x_i) : B_{ij} \text{ is not a fixed zero.}\} \cup \{(x_j, y_i) : C_{ij} \text{ is not a fixed zero.}\} \cup \{(x_j, y_i) : A_{ij} \text{ is not a fixed zero.}\}.
\]

For a structured system, we have the following theorem:

Theorem 6 ([11]). Let the transfer function be \(K_\lambda = C_\lambda(zI - A_\lambda)^{-1}B_\lambda\) and let \(\text{rrank}(K_\lambda)\) denote its normal rank. Define

\[
r = \max_{\lambda \in \mathbb{R}^l} \{\text{rrank}(K_\lambda)\}, \quad R = \{\lambda \in \mathbb{R}^l : \text{rrank}(K_\lambda) \neq r\}.
\]

Then \(R\) has Lebesgue measure 0.

\(r\) is the generic normal rank of the transfer function \(K_\lambda\). The above theorem indicates that for almost all possible realizations of the structured system, the normal rank of the transfer function will be \(r\). We can further relate the generic normal rank with the graph associated to the structured system.

Theorem 7 ([11]). The generic normal rank of the transfer function \(K_\lambda\) equals the maximal size of linking in \(H\) from \(U\) to \(Y\).

For our system, the \(A\) matrix is structured. The matrices \(B, B^F, C\) have fixed zeros and ones. However, the fixed ones can be changed to free parameters by proper scaling. Therefore, the system is structured. We are now ready to prove the main theorem

Theorem 8. If for all \(F \in F\), there exists a \(p + |F|\) linking from \(S \cup F\) to \(T\), then for almost all possible realizations of \(A\), the system is weakly resilient against \(F\)-attacks. If there exists an \(F \in F\), such that there does not exist a \(p + |F|\) linking from \(S \cup F\) to \(T\), then the system is not weakly resilient against \(F\)-attacks regardless of \(A\).

Proof: Consider the graph \(H = (V_H, E_H)\) associated with the structured system \((A, B, B^F, C)\). It can be easily seen that \(H\) is an augmented graph of the original topology \(G = (V, E)\). To be specific, \(V_H = V \cup U \cup Y\), where \(U\) contains \(p + |F|\) vertices and \(Y\) contains \(m\) vertices. Each vertex in \(U\) is connected to a vertex in \(S \cup F\) and each vertex in \(Y\) is connected by a vertex in \(T\). As a result, for every linking in \(H\) from \(U\) to \(Y\), there exists a linking from \(S \cup F\) to \(T\) and vice-versa. Therefore, by Theorem 5, 6 and 7 we can complete the proof.

Combining Theorem 8 and 3, we have the following corollary:

Corollary 1. If for all \(F_1, F_2 \in F\), there exists a \(p + |F_1 \cup F_2|\) linking from \(S \cup F_1 \cup F_2\) to \(T\), then for almost all possible realizations of \(A\), the system is strongly resilient against \(F\)-attacks. If there exist \(F_1, F_2 \in F\), such that there does not exist a \(p + |F_1 \cup F_2|\) linking from \(S \cup F_1 \cup F_2\) to \(T\), then the system is not strongly resilient against \(F\)-attacks regardless of \(A\).

Since the generic resilience of the system is only related to the topology of the system, as shown in Theorem 8, we have the following definition:

Definition 4. A topology \(G = (V, E)\) is said to be weakly (strongly) resilient to \(F\)-attacks, if and only if for any \(F \in F\) \((F_1, F_2 \in F)\), there exists an \(p + |F|\) \((p + |F_1 + F_2|)\) linking from \(S \cup F\) \((S \cup F_1 \cup F_2)\) to \(T\).

To illustrate Theorem 8, let us consider the network shown in Fig 2. Suppose at most two nodes can be compromised. There are 4 possible scenarios due to symmetry shown in Fig 2(a)(b)(c)(d) respectively. The compromised nodes are denoted as the red nodes and the linking is marked with red lines. It can be seen that the topology is weakly resilient to two compromised nodes and is strongly resilient to one compromised node.

In the next section we propose a technique to improve the resilience of the system using trustworthy nodes.

IV. ENHANCING THE RESILIENCE WITH TRUSTWORTHY NODES

It is clear from the Section III that the resilience of network is directly related to the connectivity of the topology. As a
result, one trivial way to improve the resilience is to add more communication links to the network. However, such a solution is not always feasible due to various constraints such as bandwidth and energy. Another approach is to augment some routers with more states without modifying the topology, which will be discussed in this section.

To be specific, let us assume that a router $i$ has $n_i^O$ outgoing neighbors. We assume that router $i$ updates a vector state $X_{k,i} \in \mathbb{R}^{n_i^O}$ using the following update equation:

$$X_{k+1,i} = A_{i,i} X_{k,i} + \sum_{j \in N_i^I} A_{i,j} z_{k,j,i},$$

where $A_{i,i} \in \mathbb{R}^{n_i^O \times n_i^O}$ and $A_{i,j} \in \mathbb{R}^{n_i^O}$. The router sends its outgoing neighbors a scalar message, which is a linear combination of all its states:

$$z_{k,i,j} = D_{i,j} X_{k,i}, j \in N_i^O,$$

where $D_{i,j} \in \mathbb{R}^{1 \times n_i^O}$.

**Remark 2.** An augmented node needs more computational power to update its states. Also more bandwidth is needed since the node needs to singlecast instead of broadcasting.

Since each state variable is a vertex in graph $H$ associated with the structured linear system, an augmented node $i$ will be represented by a collection of $n_i^O$ nodes in $H$, all of which are connected from the incoming neighbors and to the outgoing neighbors of $i$ and interconnected with each other. As a result, augmented nodes increase the connectivity of the graph $H$. However, it is harder to detect an attack when the attacker compromises augmented nodes. As a result, it is important that such nodes are well protected, which leads to the following definition:

**Definition 5.** An augmented node is called trustworthy if it does not belong to $T$ or $S$ and is guaranteed to follow the update equation (13) and the transmission equation (14).

**Remark 3.** Tamper-resistant microprocessors can be used for augmented nodes to prevent the adversary from compromising them.

In the rest of the paper we will assume that all the augmented nodes are trustworthy.

Given a graph $G$ and the set of trustworthy node $Q$, we can define a new graph $G' = \{V', E'\} = \mathcal{M}(G, Q)$ by removing trustworthy nodes. To be specific, first suppose there is only one trustworthy node in the network. As a result, $Q = \{q\}$, where $p < q < n - m + 1$. Then

$$V' = V \setminus \{q\}.$$  

Define the set of incoming edges of $q$ as $E_i^T(q) = \{(i, q) \in E : i \in N_q^I\}$ and set of outgoing edges as $E_q^O = \{(q, i) \in E : i \in N_q^O\}$. Also define the set $E_q^{IO} = \{(i,j) : i \in N_q^I, j \in N_q^O\}$, which connects all the incoming neighbors of $q$ to its outgoing neighbors. Note that $E_q^{IO}$ may not be a subset of $E$, which means some of the links may not exist in $E$. Then $E'$ can be defined as

$$E' = (\{E \cup E_q^{IO} \} \setminus (E_q^{I} \cup E_q^{O})).$$

In other words, $E'$ is defined as removing all the edges containing $q$ and then directly connecting all the incoming neighbors of $q$ to its outgoing neighbors. Suppose $Q$ contains more than one trustworthy node, then the function $\mathcal{M}$ can be defined recursively as

$$\mathcal{M}(G, Q) = \mathcal{M}(\mathcal{M}(G, Q \setminus \{q\}), \{q\}),$$

where $q \in Q$. We call $G' = \mathcal{M}(G, Q)$ the reduced topology. Now we have the following theorem to characterize the effect of trustworthy node on the network.

**Theorem 9.** The sensor network with a set of trustworthy nodes $Q$ is generically weakly(strongly) resilient to $F$-attacks if the reduced topology $G' = \mathcal{M}(G, Q)$ is weakly(strongly) resilient to $F$-attacks, where $F$ is given by

$$F = \{F \subset V : |F| \leq f, F \cap S = \phi, F \cap Q = \phi\}.$$

**Proof:** The proof can be carried out by constructing a one to one correspondence of a linking in $H$(from $U$ to $Y$) to a
linking in $G'$ (from $S \cup F$ to $T$). The technical details of the proof is omitted.

The effect of trustworthy node can be illustrated by the following example. Consider the network shown in Fig 3. Suppose that each node updates the state according to the following equation:

$$x_{k+1,i} = \sum_{j \in N^i(i)} x_{k,j} + \delta_{1,i} w_{k,1}.$$ 

In other words, each router updates its state to the sum of states of its incoming neighbors. Suppose that the red node 2 is compromised. The fusion center cannot detect that (see Theorem 8). In fact, if the attacker injects a sequence $u$, it can be proved that

$$\Phi(w, u, \{2\}) = \Phi(w + u, 0, \phi).$$

![Fig. 3. Wireless Sensor Network with Trustworthy Node](image)

Such vulnerability is caused by the blue node 4 which acts as a bottle-neck for the network. If we instead replace node 4 with a trustworthy node, and change its update equation to

$$X_{k+1,4} = [x_{k,2}, x_{k,3}]',$$

and transmission equations to

$$z_{k,4,5} = [1, 0]X_{k,4}, \quad z_{k,4,6} = [0, 1]X_{k,4},$$

then it can be proved that the system is weakly resilient to one malicious node by Theorem 9. The reduced topology is illustrated in Fig 4.

![Fig. 4. Reduced Topology of the Sensor Network after Removing of Trustworthy Node](image)

### V. CONCLUSION AND FUTURE WORK

In this paper we propose a secure data transmission protocol for sensor networks. We define the resilience of the protocol against malicious attacks and relate it with the topology of the network. We further discuss how to improve the resilience of the network by using trustworthy sensors. Future work includes the development of efficient algorithms to identify the set of malicious nodes and reconstruct the input. We would also like to generalize the results to distributed control systems.

### REFERENCES

Towards A Unifying Security Framework for Cyber-Physical Systems

Quanyan Zhu and Tamer Başar

Abstract—The critical infrastructures that support major industries are increasingly dependent on information systems for their command and control. The migration of legacy control systems to new communication technologies enables more robust data, quicker time to market and interoperability but also introduces new cyber-related vulnerabilities and risks. The security solution to control systems needs to be built based on the understanding of the trade-off between system security and accessibility. We propose a unifying theoretical framework that addresses the cross-layer design of security architecture and its configurations from its interactions with the physical layer plant and the security mitigation strategies from the perspective of controller design as well as cyber security defense strategies. Our holistic viewpoint on the cyber-physical systems allows us to understand the fundamental limitations and design principles for secure control systems.

I. INTRODUCTION

The integration of IT infrastructure with industrial control systems has created a closed network of systems embedded in the publicly accessible network. The integration brings many cost and performance benefits to the industry as well as arduous challenges of protecting the automation systems from security threats [3]. IT networks and automation systems often differ in their security objectives, security architecture and quality-of-service requirements. Hence, the conventional IT solutions to security cannot be directly applied to control systems. It is also imperative to take into account many control system specific properties when developing new network security solutions. In this paper, we study the influence of cyber security policies on various control system performances and develop an optimal security policy for a networked control systems.

Due to the total isolation of control systems from the external networks, control system security has historically been defined as the level of reliability of the system, with designs aimed at increasing the reliability and the robustness of the system, rather than considering the network security. Hence, merging a modern IT architecture with an isolated network that does not have built-in security countermeasure is a challenging task. From a mitigation perspective, simply deploying IT security technologies into a control system may not be a viable solution. Although modern control systems use the same underlying protocols that are used in IT and business networks, the very nature of control system functionality may make even proven security technologies inappropriate. Sectors such as energy, transportation and chemical, have time-sensitive requirements. Hence, the latency and throughput issues with security strategies may introduce unacceptable delays and degrade acceptable system performance. The requirement of accessibility of control systems is a distinct factor that distinguishes it from its IT counterpart. Understanding the system tradeoff between security and system accessibility would enable us to learn the fundamental limitations and design principles for secure control systems.

Security solutions at the physical and the cyber layer of an integrated control system need to take into account the interaction between these two layers. Figure 1 illustrates the concept of security interdependence between the cyber system and the physical plant. In this paper, we adopt a holistic cross-layer viewpoint towards a hierarchical structure of control systems. The physical layer is comprised of devices, controllers and the plant whereas the cyber layer consists of routers, protocols, and security agents and manager. The physical layer controllers are often designed to be robust, adaptive, and reliable for physical disturbances or faults. With the possibility of malicious behavior from the network, it is also essential for us to design controllers that take into account the disturbances and delay resulting from routing and network traffic as well as the unexpected failure of network devices due to cyber attacks. On the other hand, the cyber security policies are often designed without consideration of control performances. To ensure the continuous operability of the control system, it is equally important for us to design security policies that provide maximum level of security enhancement but minimum level of system overhead on the networked system. The physical and cyber aspects of control systems should be viewed holistically for analysis and design.
II. A UNIFYING SECURITY MODEL

The cyber infrastructure serves as an interface between the controller and the physical plant. Depicted in Figure 3, the control signals are sent through a security enhanced IT infrastructure such as wireless networks, the Internet and local area networks (LANs). The security architecture of the IT infrastructure is designed to enable the security practice of defense in depth for control systems [3]. Figure 2 illustrates the concept of in-depth defensive strategies. The cascading countermeasures using a multitude of security devices and agents, ranging from physical protections to firewalls and access control, can offer the administrators more opportunities for information and resources control with the advent of potential threats. However, it also creates possible issues on the latency and the packet drop rate of communications between the controller and the plant. We propose a unifying security model for this cyber-physical scenario and investigate the mitigating strategies from the perspectives of control systems as well as of cyber defenses. At the physical layer, we often aim to design robust or adaptive controllers that take into account the uncertainties and disturbances in the system to enhance robustness and reliability of the system. At the cyber level, we often employ IT security solutions by deploying security devices and agents in the network. The security designs at the physical and the cyber layers usually follow different goals without a unifying framework. In this section, we describe a cross-layer security model that connects the cyber security with the physical layer control system.

We model the physical plant with the following continuous-time dynamics:

\[ \dot{x}(t) = A(t)x(t) + B(t)u(t) + D(t)w(t), \quad x(0) = x_0, \quad t \geq 0. \]

where \( x_0 \in \mathbb{R}^n \) is the initial condition; \( x(t) \in \mathbb{R}^n \) is the system state; \( u(t) \in \mathbb{R}^m \) is the control variable; \( w \in \mathbb{R}^l \) is the disturbance variable; \( A(t) \in \mathbb{R}^{n \times n}, B(t) \in \mathbb{R}^{n \times m}, D(t) \in \mathbb{R}^{n \times l} \) are system parameters defined for \( t \geq 0 \). In order to enhance the system’s response to uncertainties, faults, and disturbances, we adopt an \( H_\infty \) optimal control approach to design robust controls for the system in (1) [6]. The goal of the control design is to find an optimal control \( u^*(t) \) that optimizes the performance index in the worst-case of \( u^*(t) \)

\[ L_u(u, w) = |x(t_f)|^2_{Q_f} + \int_0^{t_f} \left\{ |x(t)|^2_{Q(t)} + |u(t)|^2 - \gamma^2|w(t)|^2 \right\}, \]

(2)

where \( Q_f \geq 0, Q(t) \geq 0, t \in [0, t_f], \gamma > 0, t_f \) is the terminal time, all matrices have piecewise-continuous entries, and so do \( u \) and \( w \). The cost criterion (2) is the performance index of the soft-constrained differential game associated with the performance index (3) of the disturbance attenuation problem [6], [7]:

\[ L(u, w) = |Q(t_f)|^2_{Q_f} + \int_0^{t_f} \left\{ |x(t)|^2_{Q(t)} + |u(t)|^2 \right\}. \]

The associated differential game has two players. One player (P1) is the controller who minimizes (2) and the other player (P2) is the disturbance who maximizes it.

The control signals of the system (1) are sent over a security-enhanced communication network where security devices such as intrusion detection systems (IDSs), intrusion prevention systems (IPSs), firewalls, authentication servers, etc. are deployed. Figure 4 describes a simple security architecture for the access of the control system LAN from the Internet. A control signal packet has to pass many security zones to reach the local network. We model the security process in a given architecture by a queuing network. Each queue represents a device or a checkpoint where control signal traffic has to go through. Hence, the entire security architecture can be represented by a queuing network. Let \( \mathcal{N} = \{ n_1, n_2, \ldots, n_N \} \) be the set of \( N \) security devices that form an acyclic network of queues. The connection of the

Fig. 2. Defense in-depth strategies for control systems: a multitude of security devices and agents are cascaded to offer countermeasures against potential threats.

Fig. 3. Security architecture of control systems serves as an interface between the physical plant and the controller.
queues is represented by a graph \( G := (N, E) \), where \( E \) is the set of directed edges that connect between two queues. Denote by \( N_i \subset N \) the set of devices that \( n_i \) connects to after its service, i.e. \( N_i := \{ j \in N : (i,j) \in E \} \). We assume that the external packet arrival to a device \( n_j \in N \) follows a Poisson process of rate \( \lambda \), and the service time of the device follows an exponential distribution with rate \( \mu_i \). Packets are examined on a first-come, first served basis. A packet completing the scan or inspection at \( n_i \) will move to some new device \( n_j \) with probability \( p_{ij} \) or will be dropped with probability \( \bar{p}_i := 1 - \sum_{j \in N_i} p_{ij} \). Under these assumptions, the set of security agents form a Jackson network in which each device operates as an M/M/1 queue [4], [5].

At a finer level of granularity, within a security device, for example, an IDS/IPS, the process of comparing network traffic against a pre-defined rule set or a set of known attack signatures can also be viewed as a queueing system. In the following, we study the configurations of IDS/IPS systems and their effects on the design of the control system. Let \( L = \{ l_1, l_2, \cdots, l_L \} \) be the set of \( L \) rules in an IDS/IPS system. A rule has its predefined signatures against which an IDS/IPS makes a comparison. An IDS raises an alert to a system administrator once it recognizes an attack pattern or will be dropped with probability \( \bar{p}_i \). The probability \( p_{ij} \) captures the rate of a legitimate packet passing from \( l_i \) to \( l_j \), \( p_{ij} = 1 \) if the rule \( l_i \) is an IDS rule whereas \( p_{ij} \leq 1 \) if the rule belongs to an IPS. The probability \( 1 - p_{ij}, l_i, l_j \in L \), is the false negative rate of an IPS rule, i.e., packet dropping rate of legitimate traffic. Figure 6 depicts the block diagram that characterizes a single IDS/IPS system by its arrival rate \( \lambda \), service rate \( \mu \) and packet drop rate \( \bar{p} \). Henceforth we drop the \( j \) index of the probability \( p_{ij} \) for simplicity, because of the series connection of the queues.

We consider two major effects from IDS/IPS: delay and packet loss. Previous research on packet loss in network control systems include [1], [2]. Let \( \tau \) be the time delay for the state information to reach the controller. The admissible control policies for P1 will hence be of the form

\[
u(t) = \mu(t, x_{[0,t-\tau]}), \quad t \geq \tau = \mu(t, x_0), \quad 0 \leq t < \tau,
\]

and the control policies for P2 will be of the form

\[
w(t) = \nu(t, x_{[0,t-\tau]}), \quad t \geq \tau = \nu(t, x_0), \quad 0 \leq t < \tau.
\]

We denote the class of such controllers for P1 and P2 by \( \mathcal{M}_{\tau,D}^i, i=1,2 \). The delay from IDS/IPS is given by the mean sojourn time

\[
\tau = \frac{1}{\mu_1} + \sum_{j=2}^{L} \frac{p_{j-1}}{\mu_j}.
\]

Let \( \Theta(t) = \text{diag}(\theta_1(t), \theta_2(t), \cdots, \theta_m(t)) \in \mathbb{R}^{m \times m} \) be the packet drop rate as a result of the IDS/IPS system. A diagonal entry \( \theta_i(t), i=1,2,\cdots,m \), is a Bernoulli random variable that denotes the packet drop rate of \( i \)-th control input. \( \theta_i(t) = 1 \) with probability \( 1 - p \) and \( \theta_i = 0 \) with probability \( p \). Note that different control inputs may go through different routes or different IDSs/IPSs to reach the control system and hence \( \theta_i \) can take different forms for each control input \( i \). The control system dynamics (7) can be modified into

\[
\dot{x}(t) = A(t)x(t) + B(t)\Theta(t)u(t) + D(t)w(t), t \geq 0,
\]

and the performance index becomes

\[
\mathcal{T}_{\gamma}(u, w) = \mathbb{E}_{\Theta}[L_{\gamma}(u, w)].
\]

For simplicity, we can assume all control inputs to have the same packet drop rate \( \theta \), i.e., \( \Theta(t) = \theta \mathbf{I} \), which is given by

\[
\theta = 1 - \prod_{j=1}^{L} p_j
\]
It is easy to deduce from (6) and (9) that if we enhance the security by loading a larger set of IDS rules, it will result in longer delays; and if we secure the system with more IPS rules, it will be more likely to incur a higher level of packet loss. Given the IDS/IPS configuration, an optimal control to achieve disturbance attenuation for a given $\gamma$ is

$$u = u_\gamma(x - \tau, t) = -E[\Theta(t)]B^T(t)Z_\gamma(t)\eta(t), 0 \leq t \leq t_f,$$

$$\text{(10)}$$

where $Z_\gamma$ is a solution to the following generalized Riccati equation (GRDE):

$$\dot{Z} + A^TZ + ZA + Q - Z(E[\Theta^2])BB^T - \gamma^{-2}DD^TZ = 0; \text{ (11)}$$

$$Z(t_f) = Q_f,$$

and $\eta(\cdot)$ is generated by the (infinite-dimensional) compensator

$$\eta(t) = \Phi(t, t - \tau)x(t - \tau) - \int_{t-\tau}^{t} \Phi(t, s) \cdot (E[\Theta^2]B)B^T(s) - \gamma^{-2}D(s)D^T(s)) \cdot Z(s)\eta(s)ds, \quad \eta(s) = 0, 0 \leq s < \tau,$$

$$\text{(12)}$$

with $\Phi(\cdot, \cdot)$ being the state transition matrix associated with $A(\cdot)$.

For every $t' \geq \tau$, we have an open-loop type of Riccati equation defined on $[t' - \tau, \tau]$:

$$\dot{S}_\nu + A^T S_\nu + S_\nu A + Q + \gamma^{-2}S_\nu D^T D S_\nu = 0; \text{ (13)}$$

$$S_\nu(t') = Z(t'); \quad t' - \tau \leq t \leq t', \quad t' \in [\tau, t_f].$$

Each time point $t' \geq \tau$ corresponds to one Riccati differential equation. Let $\hat{\gamma}^{CL}_D$ be the optimal attenuation level under closed-loop information pattern. We define

$$\hat{\gamma}^{\tau D} := \inf\{\gamma > \hat{\gamma}^{CL}_D : \text{For every } t' \geq \tau, \text{(13) does not have a conjugate point on the corresponding interval}\}.$$  

$$\text{(14)}$$

**Theorem 1 ([6]):** Consider the linear-quadratic zero-sum differential game associated with (7) and (9), with delayed-state information (4) and (5). Let $\hat{\gamma}^{\tau D}$ be defined by (14). Then:

1. If $\gamma > \hat{\gamma}^{\tau D}$, the game admits a unique noise-insensitive saddle-point solution, which is given by the policies (10).

   The saddle-point value is given by

   $$L^*_\gamma := L_\gamma(u^*, w^*) = x^T_0Z(0)x_0.$$  

   $$\text{(15)}$$

2. If $\gamma < \hat{\gamma}^{\tau D}$, the differential game does not admit a saddle point and has unbounded upper value.

The preceeding theorem reveals the following separation principle regarding the effect of cyber security on control systems:

1. For a given $\gamma > \hat{\gamma}^{\tau D}$, the optimal saddle-point value is only dependent on the packet loss rate $\Theta(t)$ as in (11).

2. For a given packet loss rate $\Theta(t)$ and its corresponding $Z(\cdot)$, the optimal attenuation level is only dependent on the delay as in (13).

We can make use of the above observation to find an optimal cyber security policy by taking into account the performance index of control systems. Let $\alpha_i \in \mathbb{R}_+\cup L$ be the utility associated with each IDS/IPS rule. The total rule set $L$ can be partitioned into a set of IDS rules $L_{IDS}$ and a set of IPS rules $L_{IPS}$. According to the first principle, we can find an optimal configuration $L_{IPS} \subset L_{IPS}$ on the set of IPS rules that maximizes the total security utility subject to the control system constraints for a sufficiently large $\gamma$, i.e.,

$$\text{(IPS-OPT)} \max_{\sum_{i \in L_{IPS}} \alpha_i} \sum_{i \in L_{IDS}} \alpha_i$$

$$\text{s. t. } x^T_0Z(0)x_0 \leq \mu_L,$$

$$\text{(17)}$$

where $\mu_L$ is the maximum acceptable cost on the performance index so that the feasible set of $L_{IPS}$ is not empty. The constraint in (IPS-OPT) essentially can be turned into a constraint on the packet loss rate. The next level of optimization is to find a configuration of IDS rules such that $\gamma$ is satisfied given the packet loss rate as a result of the IPS configuration, i.e.,

$$\text{(IDS-OPT)} \max_{\sum_{i \in L_{IDS}} \alpha_i} \sum_{i \in L_{IDS}} \alpha_i$$

$$\text{s. t. } \hat{\gamma}^{\tau D}(\Theta(t)) \leq \gamma.$$  

$$\text{(19)}$$

Every delay $\tau$ corresponds to a $\hat{\gamma}^{\tau D}$. The constraint in (IDS-OPT) gives bounds on the range of feasible $\tau$ to choose from.

**III. CONCLUSION**

In this paper, we have proposed a unifying framework to address security issues in cyber-physical systems. We have modeled the cyber security architecture by Jackson networks and the security devices by tandem queueing networks. We have studied two effects of the cyber architecture on control systems: delay and packet drop rate. We have incorporated these two factors into the $H^\infty$ controller design and proposed a cross-layer optimization framework for the design and configuration of cyber security.

**REFERENCES**


Management of Control System Information Security: Control System Patch Management

Quanyan Zhu, Miles McQueen, Craig Rieger and Tamer Başar

Abstract—The use of information technologies in control systems poses additional potential threats due to the frequent disclosure of software vulnerabilities. The management of information security involves a series of policy-making decisions on the vulnerability discovery, disclosure, patch development and patching. In this paper, we use a system approach to devise a model to understand the interdependencies of these decision processes. Specifically, we establish a theoretical framework for making patching decisions for control systems, taking into account the requirement of their functionality. We illustrate our results with numerical simulations and show that the optimal operation period of control systems given the currently estimated attack rate is roughly around a half a month.

I. INTRODUCTION

The integration of new information technologies into control systems in critical infrastructures enables more efficient methods of communication as well as more robust data and interoperability [6]. However, the usage of technologies with known vulnerabilities exposes control systems to potential exploits. Information security management becomes a crucial issue for control systems. The timing between the discovery of new vulnerabilities and their patch availabilities is crucial for the assessment of the security risk exposure of software users [1], [3], [4], [5]. The security focus in control systems is different from the one in computer or communication networks. The application of patches for control systems needs to take into account the system functionality, avoiding the loss of service due to unexpected interruptions. The disclosure of software vulnerabilities for control systems is also a critical responsibility. Disclosure policy indirectly affects the speed and quality of the patch development. Government agencies such as CERT/CC (Computer Emergency Response Team/Coordination Center) currently act as a third party in the public interest to set an optimal disclosure policy to influence behavior of vendors [7].

The decisions involving vulnerability disclosure, patch development and patching are intricately interdependent. In this paper, we introduce a model for information security management of control systems. We investigate the decision processes of vulnerability discovery, disclosure, patch development and control system patching. In Figure 1, we illustrate the relationship between these decision processes. A control system vulnerability starts with its discovery. It can be discovered by multiple parties, for example, individual users, government agency, software vendors or attackers and hence can incur different responses. The discoverer may choose to not disclose to anyone, may choose to fully disclose through a forum such as bugtraq [2], may report to the vendor, or may provide to an attacker. Vulnerability disclosure is a decision process that can be initiated by those who have discovered the vulnerability. A patch development starts when the disclosure process reaches the vendor and finally a control system user decides on the application of the patches once they become available. An attacker can launch a successful attack once it acquires the knowledge of vulnerability before a control system patches its corresponding vulnerabilities. The entire process illustrated in Figure 1 involves many agents or players, for example, system users, software vendors, government agencies, attackers. Their state of knowledge has a direct impact on the state of the vulnerability management.

We propose to compartmentalize the task of vulnerability management into different submodules: discovery, disclosure, development and patching. The last two submodules are relatively convenient to deal with since the agents who involved in the decision making are very specific to the process. The models for discovery and disclosure can be more intricate in that these processes can be performed by many agents and hence specific models should be used for different agents to capture their incentives, utility, resources and budgets. In the subsequent sections, we establish models for control system patching to assist users to make optimal patching decisions.

II. USER PATCHING

In this section, we establish a model for users to determine the optimal time to patch for their control systems. In control systems, it is known that the attack rate is low and the patching rate is low as well. It often occurs that users do not patch until there is a security alert, an available patch announcement or an experienced security breach. The operation of control system is separated into several operating periods. A control system cannot halt its operation until the end of an operating period. Let $B_k$, $k = 1, 2, \cdots$ denote the $k$-th operating period since the last patching and $T_k = T_{k-1} + B_k = \sum_{i=1}^{k} B_i$, where $T_0$ is the beginning of the first operation period. Let $\tau$ be the time length between the start of the first operation period and a security alert or an attack. Let $f_{\tau}(t)$, $t \geq 0$, be its probability density function, which is taken to be hyper-exponential with $n$ phases and parameters $\lambda = (\lambda_1, \cdots, \lambda_n)$ and normalized.
weighting factor \( q = (q_1, \ldots, q_n) \), i.e.,
\[
f_r(t) = \sum_{i=1}^{n} q_i g_i(t) = \sum_{i=1}^{n} q_i \lambda_i \exp(-\lambda_i t), \quad \sum_{i=1}^{n} q_i = 1. \tag{1}
\]

Each phase \( i \) can be interpreted differently. For example, let \( g_1(t) \) be the distribution of the arrival rate of alerts; \( g_2(t) \) be the arrival rate of an attack; \( g_3(t) \) be the arrival rate of an announcement of an available patch. We illustrate this model in Figure 2. At every \( T_{k-1}, k \geq 1 \), a control system starts to operate for a period of \( B_k \) and then stops for monitoring and patching.

The decision of an administrator is to determine \( B_k \) so that the risk of an unpatched control system subject to potential attacks is minimized. The decision-making process can be viewed as a black box as in Figure 3, where the decision input is the knowledge of the arrival rates of an attack; the intrinsic system parameters are the monitoring cost \( c_m \) and the production cost parameters \( c_0 \) and \( c_1 \); and the decision output is the operation period \( B_k \). The input and output characteristics of the decision process assist us in integrating it into the system model in Figure 1.

A. A General Model

In this section, we introduce a generalized model for control system patching. Let \( c_m \in \mathbb{R}_+ \) be the monitoring cost at the end of each operation period and \( c_p(t_k, b_{k+1}) : \mathbb{R}_+^2 \rightarrow \mathbb{R}_+ \) be the operation cost of running the plant for \( b_{k+1} \) starting from \( t_k \). We have the following dynamic programming (DP) equation to find the optimal decision policy to be taken at each period, taking into account the whole lifetime of the system:
\[
V_k^*(t_k) = \min_{b_{k+1} \geq 0} \left\{ \mathbb{E}[c(t_k, b_{k+1}) + \mathbb{P}(\tau_k > b_{k+1}) V_{k+1}^*(t_{k+1})] \right\}, \tag{2}
\]
where \( b_k \) is the decision variable of operating time; \( V_k^*(t_k) \) represents the optimal cost at time \( t_k \). The term \( \mathbb{P}(\tau_k > b_{k+1}) \) represents the transition probability given by the conditional probability
\[
\mathbb{P}(\tau_k > b_{k+1}) := P(\tau > t_k + b_{k+1} | \tau > t_k). \tag{3}
\]
The term \( \mathbb{E}[c(t_k, b_{k+1})] \) is the stage cost at \( t_k \) given by
\[
\mathbb{E}[c(t_k, b_{k+1})] = \gamma \mathbb{E}[(b_{k+1} - \tau_k) 1(\tau_k < b_{k+1}) + c_m + c_p(t_k, b_{k+1})], \tag{4}
\]
where \( \gamma \) denotes the unit cost of untimely patching; \( \tau_k \) is the conditional residual time counting from \( t_k \) given that \( \tau_k > t_k \). By solving the DP equation, we can find a dynamic policy for the operation of the plants at each starting time \( t_k \).

B. A Simplified Model

In this subsection, we simplify the general model by invoking the following assumptions.

Assumption 1: (A1) The arrival of security alerts or breaches form a single Poisson process with rate \( \lambda \) and the arrival time \( \tau \) and the conditional residual time \( \tau_k \) are exponentially distributed with parameter \( \lambda \).

Let \( C_k^0 = \frac{1}{2} c_0 b_k^2 \) be the cost for operating a plant non-stop for a period of time \( b_k \). Denote by \( C_k^1 = c_1 b_k \) the linear gain
or profit from running the plant. Hence, we can impose the following assumption:

**Assumption 2:** (A2) The cost $c_p$ is given by

$$c_p(t_k, b_{k+1}) := C_k^0 - C_k^1 = \frac{1}{2} c_0 b_k^2 - c_1 b_k$$

Under assumptions (A1) and (A2), due to the memoryless property of exponential distribution, the DP equation in (2) can be simplified to

$$V^*(\lambda) = \min_{b \geq 0} \{ \gamma \mathbb{E}[(b - \tau(\lambda))1_{(\tau(\lambda) \leq b)}] + \frac{1}{2} c_0 b^2 - c_1 b + P(\tau(\lambda) > b)V^*(\lambda) \} .$$

(6)

For each fixed $b \geq 0$, $V(\lambda)$ can be solved from (6) (without the minimum) to yield

$$V(\lambda, b) = \frac{\gamma \mathbb{E}[(b - \tau(\lambda))1_{(\tau(\lambda) \leq b)}] + \frac{1}{2} c_0 b^2 - c_1 b}{1 - P(\tau(\lambda) > b)}. \tag{7}$$

Note that in the above,

$$\mathbb{E}[(b - \tau(\lambda))1_{(\tau(\lambda) \leq b)}] = \frac{\lambda b - 1 + \exp(-\lambda b)}{\lambda}; \tag{8}$$

and the term in the denominator of (7) is as follows:

$$P(\tau(\lambda) > b) = \exp(-\lambda b). \tag{9}$$

Hence, to solve the DP is equivalent to finding a solution to the optimization problem (R-OPT) that takes into account the risk factor of potential threats and attacks\textsuperscript{1}:

$$(\text{R-OPT}) \quad V^*(\lambda) = \min_{b \geq 0} V(\lambda, b) \tag{10}$$

Note that a simple solution for operation time $b$ without security risk consideration, i.e., ignoring the potential costs that can be incurred by attacks in (R-OPT), is based on a cost and benefit analysis solving the risk-free optimization problem (NR-OPT)\textsuperscript{2}:

$$(\text{NR-OPT}) \quad \min_{b \geq 0} \frac{1}{2} c_0 b^2 - c_1 b + c_m, \tag{11}$$

which yields a benchmark solution $b^* = c_1/c_0$.

**Theorem 1:** Optimization problem (10) is a strictly convex program and admits a unique solution.

**Proof:** We can show this property by taking first and second order derivatives of the objective function. \hfill \blacksquare

The problem formulation can be further generalized to include additional features such as law of small numbers and noncooperative behavior between the attacker and the defender.

**Remark 1:** In the DP formulation, we can add a discount factor $\delta \in (0, 1)$ in (2) to capture the short-sightedness of the control system users. In addition, we can have another similar DP to model the attacker’s response to user’s decision making. The attacker may reduce the attack rate when he becomes less successful and foresees increasing efforts in attacks. Hence, we

\textsuperscript{1}“R-OPT” stands for risk-based optimization.

\textsuperscript{2}“NR-OPT” stands for no-risk-based optimization.

will have a game-theoretical situation between the attacker and the defender [8].

$$V^*(b) = \min_{\lambda \geq 0} \left\{ -\beta \mathbb{E}[(b - \tau(\lambda))1_{(\tau(\lambda) \leq b)}] + c_a(\tau(\lambda), b) \right\} + P(\tau(\lambda) > b)V^*(b), \tag{12}$$

where $\beta \in (0, 1)$ is the discount factor of the attacker; $c_a(\tau(\lambda), b)$ is the cost of an attacker when he attacks with rate $\lambda$.

**Remark 2:** We can employ the same technique to study the vendor’s decision-making on patch development and also the government’s disclosure process. The government may wait for a period of $B_k$ to review its decision on whether to disclose a certain vulnerability and $\lambda$ can be viewed as the rate of reports of cases to the agency.

**III. Simulation**

In this section, we numerically solve the DP equations for a given scenario of control systems. Set the parameters $c_1 = 10, c_0 = 0.1, \gamma = 10, c_m = 10, \lambda = 0.001$ as the nominal case. In Figure 4, we show the optimal operation period versus the monitoring cost. It can be seen that when the cost gets higher, the control system cannot afford a frequent checking and monitoring and hence the operation period increases. In Figure 5, we show the optimal operation period versus the attack rate. We observe that when the attack rate is high, the control system need to decrease its operation period to monitor and update its system more often.
In the next numerical simulation, we examine the cost of the attacker and its impact on its attack rate. We let \( c_a(\tau(\lambda), b) = c_{1,a}\lambda + c_{m,a} \) where \( c_{1,a} \) is the unit cost on an attempted attack and \( c_{m,a} \) is a fixed cost for an attacker to be able to launch an attack. Set \( c_{1,a} = 200000, k_a = 1, b = 40, c_{m,a} = 10 \). In Figure 6, we show the attacker’s response to the patching rate of a control system. It can be seen that the higher the patching rate, the less frequent an attack will happen.

Combining the response of an attacker and a control system, we examine the best response dynamics of the two players and find the Nash equilibrium strategies of the attacker and defender. We start with the patching rate of a control system set to be \( b_0 = 1 \). Within two iterations, we observe that \( b_1 = b_2 = 14 \) which gives the equilibrium patching strategy \( b^* = 14 \) for a control system. On the other hand, we start with the attack rate \( \lambda_0 = 1 \). By iterations, we observe \( \lambda_1 = 0.00536, \lambda_2 = 0.00269, \lambda_3 = 0.00267 \) which gives an equilibrium strategy for an attacker to choose an attack rate of \( \lambda^* = 0.00267 \). In Figures 7 and 8, we illustrate the attacker’s response to the control system patching strategy and the defender’s response to attack rate at each iteration respectively. We can see that after two or three iterations, both players reach their Nash equilibrium.

IV. Conclusion

In this paper, we have proposed a systematic approach to tackle the management of control system information security by compartmentalizing the processes into multiple input-output blocks. We have investigated in detail the decision process of control system patch management and established a theoretical model to find an optimal operation period of a control system taking into account the risks of potential threats and the operation costs. A similar framework can be employed to study the disclosure process. From the simulation results, we notice that an optimal operation period of control systems given the currently estimated attack rate is roughly around half a month.

It is important for us to point out that the model described in the paper is idealized in that we have assumed that an attack can be prevented by a timely patching decision. However, in reality, for zero-day vulnerabilities, an attack can be successfully made regardless of patch rate. Hence, it is also essential to study the resilient control design in the event of unanticipated or rare attacks. As future work, we intend to extend the theoretical framework here to study the decisions involving vulnerability disclosure and the R&D development of control patches.

REFERENCES

Secure Routing in Smart Grids

Quanyan Zhu, Dong Wei and Tamer Başar

Abstract—The migration of power grids from an isolated network to a public communication network has created many challenging issues in the security of smart grids. One of them is the assurance of secure routing of PMU and smart meter data in the open network, which is enabled by the adoption of IP-based network technologies. The quality-of-service in routing is measured by the data integrity, latency and packet loss rate. We leverage the hierarchical structure of power grids and propose a routing protocol that maximizes the quality-of-service along the routing path to the control room. In addition, we optimize the data communication rates between the super data concentrator and the penultimate level with the control center. We propose a routing protocol that maximizes the quality-of-service along the routing path to the control room. In addition, we optimize the data communication rates between the super data concentrator and the penultimate level with the control center. We propose a hybrid structure of routing architecture to enable the resilience, robustness and efficiency of the smart grid.

I. INTRODUCTION

To meet the challenge of climate change, Smart Grid (SG) is evolving rapidly from a relatively closed communication network to an open network. Wide use of Phasor Measurement Units (PMUs) and smart meters (SMs) will help electricity power transmission and distribution system operators understand better power usage pattern and delivery of electricity energy to end users in a cost-effective way. It is forecasted that 276 million smart grid communication nodes will be shipped worldwide during the period from 2010 to 2016, with annual shipments increasing dramatically from 15 million in 2009 to 55 million by 2016 [1]. The current dedicated network or leased line communication methods are not cost-effective to connect large number of PMUs and SMs. Thus, it is foreseen that IP-based network technologies are widely adopted since they enable data to be exchanged in a routable fashion over an open network, such as the Internet [2]–[6]. This will bring benefits such as efficiency and reliability, and risks of cyber attacks as well. Without doubt, SG applications based on PMUs and SMs will change the current fundamental architecture of communication network of power grid, and bring new requirements for communication security. Delay, incompleteness and loss of PMU and SM data will adversely impact SG operation in terms of efficiency and reliability. Therefore, it is important to guarantee integrity and availability of those PMUs and SMs data. To meet the Quality-of-Service requirements in terms of delay, bandwidth and packet loss rate, QoS-based routing technologies have been studied by both academia and the telecommunications industry [7]–[10]. Unlike video and voice, data communications of PMUs and SMs have different meanings of real-time and security, especially in terms of timely availability [2], [11]–[15]. Therefore, QoS-based and security-based routing schemes for smart grid communications should be studied and developed to meet Smart Grid application requirements in terms of delay, bandwidth, packet loss and data integrity.

In this paper, we leverage the hierarchical structure of SG and propose a secure routing protocol for the emerging applications in SG. In Section II, we establish a hierarchical routing framework for local household data to reach a super data concentrator. In Section III, we propose an optimal mechanism for the communication between super data concentrators and the control room. We conclude in Section V with future work and challenges.

II. SECURE HIERARCHICAL ROUTING

SG has a hierarchical structure that is built upon the current hierarchical power grid architecture. The end-users, such as households, communicate their power usage and pricing data with a local area substation which collects and processes data from SMs and PMUs. In SGs, the path for the measurement communications should be studied and developed to meet Smart Grid application requirements in terms of delay, bandwidth, packet loss and data integrity. The physical structure of the SG communication network. The PMUs and SMs send data to DCs through a public network. DCs process the collected data and send the processed data to SDCs through (possibly) another public network.

The physical communication structure from local meters to the control room can be logically divided into several levels. Figure 2 illustrates a snapshot of routing paths in a simplified example of the hierarchical structure of the physical communication architecture, which is divided logically into 5 levels. For simplicity, we only depict only level of routers in Figure 2. In practice, there can be multiple levels of routers and they can be found in the public network between DCs and SDCs as well as SDCs and the control room. In the depicted SG, the data from a PMU or a SM has to make four hops to reach the control room. The decision for a meter to choose a router depends on the communication delay, security enhancement level and packet loss rate. In addition, the decisions for a DC to choose a SDC also depends on the same criteria. The communication security at a node is

Q. Zhu and T. Başar are with the Department of Electrical and Computer Engineering and Coordinated Science Laboratory, University of Illinois, 1308 West Main St., Urbana, IL, 61801, USA. E-mail: {zhu31,basar1}@illinois.edu; D. Wei is with Siemens Corporation, Corporate Research, Princeton, NJ, USA. E-mail: dong.w@siemens.com. The research of Q. Zhu and T. Başar was supported in part by a grant from DOE.
measured by the number of security devices such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) deployed to reinforce the security level at that node. We assign higher utility to network routers and DCs that are protected by a larger number of firewalls, IDSs/IPSs and dedicated private networks in contrast to public networks. This relatively simple metric only considers one dimension of the control system cyber security. It can be further extended to include more security aspects by considering the authorization mechanisms, the number of exploitable vulnerabilities, potential damages as well as recovery time after successful attacks. The readers can refer to [16]–[19] for more comprehensive metrics.

A trade-off with higher security is the latency and packet loss rate incurred in data transmission. A secure network inevitably incurs delays in terms of processing (encrypting/decrypting) and examining data packets. We can model the process of security inspection by a tandem queueing network. Each security device corresponds to an M/M/1 queue whose service time follows an exponential distribution. The latency caused by the security devices such as IDSs/IPSs, are due to the number of pre-defined attack signatures and patterns to be examined. In addition, devices such as IPSs can also lead to a high packet loss due to their false negative rates in the detection.

Furthermore, a node with higher level of security may be preferred by many meters or routers, eventually leading to a high volume of received data and hence higher level of congestion delay. This fact motivates us to employ a game-theoretical approach to analyze the distributed routing decisions in SGs. We are interested in mixed Nash equilibrium as a solution outcome for two reasons. Firstly, mixed Nash equilibrium always exists for a finite matrix game and many learning algorithms such as fictitious play and replicator dynamics find mixed Nash equilibrium [22]. Secondly, the randomness in the choice of routes makes it harder for an attacker to map out the routes in SGs.

A. Game-Theoretic Model

Let $\mathcal{M} = \{m_1, m_2, \cdots, m_M\}$ be the set of $M$ meters in a local area SG. Let $\mathcal{N} = \{n_1, n_2, \cdots, n_N\}$ be the set of routers, DCs and SDCs in SG. Let $C_S$ denote the control station. The entire communication infrastructure is represented by $\mathcal{I} := (\mathcal{N}, \mathcal{M}, C_S)$. Let $\mathcal{L} = \{1, 2, \cdots, L\}$ be the set of $L$ hierarchies in the infrastructure $\mathcal{I}$. Denote by $N_l, l \in \mathcal{L}$, the set of nodes at level $l$. By default, the terminal level $L$ consists of only the control station $C_S$ and the initial level 1 consists of $M$ meters. The devices in $\mathcal{N}$ form layers between levels 1 and $L$. Denote by $l_i \in \mathcal{L}$ the level where a node $n_i \in \mathcal{N}$ resides. A meter $m_i$ chooses a node $a(m_i, 2) \in N_2$ at level 2. The chosen node $a(m_i, 2)$ picks the next hop $a(m_i, 3) \in N_3$ and a similar decision is made by node $a(m_i, 3)$ at level 4. The process ends at penultimate level $L-1$ where every node chooses to send to $C_S$. The path $P_i, m_i \in \mathcal{M}$ formed by $m_i \rightarrow a(m_i, 2) \rightarrow a(m_i, 3) \cdots a(m_i, L-1) \rightarrow C_S$ is the route taken by the meter $m_i$ to reach $C_S$. Denote by default that $a(m_i, 1) := m_i$. Let $u_{a(m_i, j)}(a(m_i, L-1)) = a(m_i, L-1), m_i \in \mathcal{M}$, be the stage utility of node $a(m_i, j)$ choosing a route between $a(m_i, j)$ and $a(m_i, j+1)$, where $a(m_i, j)$ denotes the set of choices made at the other meters at the same level, more precisely,

$$a(m_{j-1}, j) := \{a(m_{j-1}, j) \in N_{j}, j \neq i, m_1, m_j \in \mathcal{M}\}.$$

The utility along the path $P_i$ for $m_i$ is given by the sum of the stage utilities

$$U_i(P_i) := \sum_{j=2}^{L} u_{a(m_i, j)}.$$

The goal of a meter $m_i$ is to maximize its total utility $U_i$. Note that the utility depends on not only its own choice but the paths of other meters as well. Since the routing decisions at the levels beyond the second one are made by the relay nodes in the set $\mathcal{N}$, the total utility maximization can be decomposed as follows:

$$\max_{P_i} U_i(P_i) = \max_{a(m_{j-1}, j) \in \mathcal{N}_j} u_{a(m_{j-1}, j)} + \max_{P_{a(m_{j-1}, j)}} U_i(P_{a(m_{j-1}, j)}).$$

Fig. 1. An example of the physical structure of the hierarchical SG communication network.

Fig. 2. A snapshot of routing paths in hierarchical SGs.
Such a decomposition allows us to find the optimal path using a backward induction from the last stage $L$. The mixed strategies yielded by this method belong to a class of behavioral strategies and carry the property of strong consistency [20].

We choose the stage utility as a ratio between the security performance index and the delay.

$$ u_{a_{(m_i,t+1)}}(a_{(m_i,t+1)}, a_{(m_{-i},t)}) = p_{a_{(m_i,t+1)}} r_{a_{(m_i,t+1)}} p_{a_{(m_{-i},t+1)}} r_{a_{(m_{-i},t+1)}} m_i \in \mathcal{M}_i $$

(3)

where $r_{a_{(m_i,t+1)}}$ is the security index at the node $a_{(m_i,t+1)}$ chosen by user $a_{(m_i,t)}$, which is measured by the number of built-in security devices and features. An alternative measure is by security investment in dollars at the node, $\tau$ is the sojourn time experienced by node $a_{(m_i,t)}$ in the queue of $a_{(m_i,t+1)}$.

$$ p_{a_{(m_i,t+1)}} \text{ is the packet loss rate at } a_{(m_i,t+1)}. $$

III. FLOW CONTROL IN SMART GRID

In Section II, we have proposed a mechanism for meter data to reach the SDCs and then the control station. The decision at the penultimate level is trivial as all the data should route to the control station. In reality, a local control station pulls data from its communicating SDCs. SDCs cannot send data to the control station at an arbitrary rate. The bandwidth and communication resources of a control station are often constrained. We next formulate a game-theoretical problem where SDCs choose data rates to communicate with the control room similar to the framework described [21].

Let $\mathcal{N}_s = \mathcal{N}_{Lux} = \{n_1, n_2, \ldots, n_{N_s}\}$ be the set of $N_s$ SDC substations. A SDC substation $n_i \in \mathcal{N}_s$ serves a load of $L_i(t)$ at time $t$ and communicates with the control center $C_S$. Let $d_i(t)$ be the data rate at which SDC $n_i$ decides to send and the service rate at the control room is $s_r(t)$. We assume that all the data come into one server and the control center allocates its resources to monitor the data from the substations. Different SDCs have different levels of significance $w_i \in (0, 1)$ to the control center. A substation with higher values of $w_i$ are often the ones that serve a large area. The control center processes the data by differentiating their sources. The data from each substation is served at a service rate $s_i(t) = a_i s_r(t)$, where $a_i \in [0, 1]$ denotes the fraction of service capacity dedicated to CPS substation $n_i$, satisfying $\sum_{n_i \in \mathcal{N}_s} a_i = 1$. Let $q(t)$ be the queue length of the server and $u_i(t) = d_i(t) - s_i(t)$. The queue evolves according to the following dynamics

$$ \dot{q}(t) = \sum_{n_i \in \mathcal{N}_s} d_i(t) - s_i(t) = \sum_{i=1}^{N} u_i. $$

(4)

The objective of the control problem is to ensure queue length to stay around some desired level $\bar{Q}$. The choice of $\bar{Q}$ has a direct impact on loss probabilities and throughput the communications between SDCs and the control room. Denote by $x(t) = q(t) - \bar{Q}$ the shifted queue length with origin at $\bar{Q}$. Then, the dynamics in (4) become

$$ \dot{x} = \sum_{i=1}^{N} u_i(t). $$

(5)

We consider two problems. The first one is a centralized problem where the control center makes data rate decision for each SDCs to achieve the optimal “social welfare”. The second one is a decentralized problem where each SDC decides on its own data rate sent to the control station.

In the centralized problem, the control room makes a global planning on the sending rates $d_i(t)$ and hence $u_i(t)$. The goal of each SDC is to minimize its cost functional

$$ J_i = \int_0^{\infty} c_i |x(t)|^2 + r_i |u_i(t)|^2 dt, $$

(6)

where $r_i$ is the cost on the control action $u_i$. The higher the sending rates will consume a high bandwidth at cost $r_i$ inversely proportional to the load $L_i$ and $w_i$, i.e., it is relatively less expensive for more important SDC to send information. The cost $r_i$ can be seen as a variable controlled by the control center that provides incentive for SDCs to respond in an efficient way. $c_i$ is the cost on the queue length such that $\sum_{n_i \in \mathcal{N}_s} c_i = 1$. Each substation with higher data rate $d_i(t)$ or $L_i(t)$ also shares a higher responsibility of keeping the queue away from overflow.

A centralized planning seeks $u_i^* = \{u_1^*, u_2^*, \ldots, u_N^*\} \in \mathcal{U}^I$ that maximizes the social welfare $J := \frac{1}{2} \sum_{i=1}^{N} J_i$, where $\mathcal{U}^I$ is a set of admissible control under information structure $I$. Denote by $J^*_I$ the optimal welfare achieved under the optimal control $u^*_I$. On the other hand, the decentralized problem constitutes a differential game $\Xi := \langle \mathcal{N}_s, \{J_i\}_{n_i \in \mathcal{N}_s}, \{U_i\}_{n_i \in \mathcal{N}_s} \rangle$, where $\mathcal{N}_s$ is the set of the players; $U_i^I$ is the set of admissible controls of a player $n_i$, which depends on the information structure $I$ of the game; $J_i$ is the cost functional that player $n_i$ attempts to minimize independently of the other players. We denote the set of equilibrium solution to $\Xi$ by $U^*_I$ and the social welfare achieved under an equilibrium $u^*_I \in U^*_I$ by $J^*_I(u^*_I)$. The measure of efficiency loss can thus be described by the price of anarchy

$$ \rho_I := \min_{u_I^* \in U^*_I} \frac{J^*_I(u^*_I)}{J^*_I}, $$

which is always upper bounded by 1.

IV. SECURE ROUTING ARCHITECTURE

A centralized routing architecture ensures the global efficiency and it is robust to small disturbances from SMs and individual DCs or SDCs. However, it is costly to implement a centralized planning on a daily basis for a large-scale SG. In addition, global solutions can be less resilient to unexpected failures and attacks as it is less nimble for changes in routes and it takes time for the centralized planning to respond in a timely manner.

On the other hand, decentralized decision-making can be more computationally friendly based on local information and hence the response time to emergency is relatively fast. The entire system becomes more resilient to local faults and failures, thanks to the independence of the players and the reduced overhead on the response to unanticipated uncertainties. However, the decentralized solution can suffer from high
loss of inefficiency. Hence, we need to assess the tradeoff between efficiency, reliability and resilience for designing the communication protocol between the control stations and the SDCs.

In this work, we propose a hybrid architecture of the communication infrastructure $I$ as illustrated in Figure 3. We adopt a centralized planning at the top levels $L-1$ and $L$ while building a decentralized routing protocol between levels 1 and $L-1$. Such an architecture can enable the robustness at the critical data centers and the resilience at the lower user level.

From the problem formulation in Section III, the final stage utility $u_{(a_i, L-1)}$ of node $(a_i, L-1) \in \mathcal{N}_{L-1}$ can be written as

$$u_{(a_i, L-1)} = -J_{(a_i, L-1)}(u^*_L).$$

(7)

Hence, the last stage utility has been determined in a centralized manner by the control room based on their priority and load. The resource allocation at the last level is robust to small parametric disturbances and is independent of routing decisions between level 1 and level $L-1$. The routing decisions of the meters are resilient to router failures in a public network. The proposed learning algorithm can respond to a dysfunctional router by selecting a new router once the one in use is compromised.

### A. Reliability Analysis

We can analyze the reliability of the hierarchical routing architecture in Figure 3. We assume that each device $n_i \in \mathcal{N}$ has a failure rate of $\lambda_i$, which is highly dependent on the security index $r_i$. We let $\lambda_i = g_i(r_i)$, where $g_i(\cdot) : \mathbb{R} \to [0, 1]$ is a monotonically decreasing and continuous function. Denote by $\Gamma$ the unreliability of the hierarchical routing architecture. It can be estimated by its unreliability lower bound $\Gamma_L$, i.e.,

$$\Gamma \geq \Gamma_L := \prod_{i=2}^{L-1} \prod_{n_i \in \mathcal{N}_i} \lambda_i t_i.$$

(8)

Assuming that components at each level have the same failure rate $\lambda_i$ for $n_i \in \mathcal{N}_i$, then we arrive at

$$\Gamma_L \leq \Gamma_\mathcal{U},$$

(9)

where

$$\Gamma_L := \sum_{l=2}^{L-1} (\lambda_l t)^{N_l},$$

(10)

and

$$\Gamma_\mathcal{U} := \sum_{l=2}^{L-1} N_l (\lambda_l t)^{N_l-1}.$$  

(11)

### V. Conclusion

Secure routing is a pivotal problem in smart grids as the power infrastructure is migrating to new communication technologies. In this paper, we propose a hybrid routing protocol that enables the resilience, robustness and efficiency of routing in smart grids. The smart meter data are routed to the control room in a hierarchical manner, where decisions are made in a decentralized manner between the first level and the penultimate one. We show that the mixed Nash equilibrium can be computed using backward induction and it can be achieved through learning algorithms such as fictitious play and best response dynamics. The data rates between the penultimate level and the control center are determined in a centralized way to achieve Pareto efficiency as well as the robustness of smart grids. Future work will be aimed at the implementation of the routing algorithm on a small testbed as well as the study of a more refined and more comprehensive security metric that incorporates potential threats and attacks.

### References


