ISSN 2186-7437

NII Shonan Meeting Report

No. 2015-3

Systems Resilience - Bridging the Gap Between Social and Mathematical

Hiroshi Maruyama
Günter Müller
Kazuo Furuta

February 23–26, 2015

National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-Ku, Tokyo, Japan

Systems Resilience - Bridging the Gap Between Social and Mathematical

Organizers:
Hiroshi Maruyama (The Institute of Statistical Mathematics)
Günter Müller (The University of Freiburg)
Kazuo Furuta (The University of Tokyo)

February 23–26, 2015

Overview

The goal of this meeting was to bridge the gap between the "social" and "mathematical" camps of resilience research so that the social aspects of resilience are more appropriately incorporated into the mathematical models and at the same time the mathematical models can provide practical guidance to the design, policy making, and operations of real-world societal systems.

Resilience is said to be the ability of a system to absorb and recover from perturbations. It is considered to be a critical characteristic for a system to survive, especially for social systems like organizations, communities, cities, and our civilization as a whole. Resilience has been studied in many different domains, such as psychology, biology, ecology, engineering, and social sciences, but often their approaches are widely different. We observe that there are at least two seemingly incongruent approaches – social and mathematical.

The social camp, mainly dealing with problems such as socio-ecological resilience and urban resilience, is concerned with resilience as a social norm. Their research approaches are based on case studies, best practices, processes, communication, decision making, consensus building, and other disciplines, and little mathematical models are used except for relatively simple system dynamics to compare different scenarios. Policy makers can learn from these studies to make better decisions in the face of possible disruptions. However, these approaches do not guarantee nor give quantitative assurance to how much the resilience strategies can contribute to the survivability of the system.

The mathematical camp, on the other hand, is interested in the mechanisms of how systems can collapse and in what conditions resilience strategies work for recovery. The well-known Bak-Tang-Wiesenfeld sandpile model [1] and the study on early-warning signals by Scheffer, et al. [2], as well as the SR-Model [3] built by the Systems Resilience project of ROIS, are good examples of mathematical approaches to resilience. They use abstract mathematical models to describe the internal workings of a system, and thus, we can draw logical conclusions in what conditions catastrophe can occur, at least probabilistically, and what strategies are effective to make the system resilient. However, their interests are often limited to the abstract models, and the results of these studies are

rarely applied to real-world problems. Also these mathematical models are usually not capable of the adaptation (or innovation) aspect of resilience, meaning that the system will evolve to something new after the shock.

The goal of this meeting is to bring researchers in these two camps and to explore common grounds so that the social and mathematical approaches are integrated to make objective and practical resilience strategies. In order to make our discussions focused, we selected cyber security as our domain of interest, which is known to have deep technical (and thus mathematical) issues as well as concerns with how the society and the people interact with cyber systems. In this process of defining the domain, we keep the essential aspects of socio-technical systems, including human behaviors, social and economic factors, and technical and systems workings intact so that the microcosm at the top still retains similar (albeit not the same) characteristics of the real world.

The meeting was organized with three parts. The first part was to "cast the anchor," meaning that we first presented the overall systems resilience landscape and then some experts in cyber security shared their experiences of real-world issues. The second part consisted of a series of presentations by participants, trying to apply their own research ideas to resilience of cyber security. Finally we had free discussions on four sub domains, namely, businesses, cyber currency, cyber security, and IoT (Internet of Things) systems. This report tries to capture the essential ideas presented by the participants and the discussions throughout the workshop.

Agenda

The essential aspect of the meeting is two-fold. First, the goal is to bring the social and mathematical camps of resilience research together and explore possible integrated approaches to achieve objective and practical resilience strategies. The second is to base our discussions on concrete domains of cyber-security using the three-layered target model, i.e., real world applications (bottom layer), cyber-physical systems (middle layer), and cyber-security (top layer). With this in mind, we separated our agenda into four parts, as follows:

Part I. Cast Anchor: Situating Real World Contexts

The objective here is to cite real incidents that threaten the resilience of the target domains. For example, at least three things come to mind, namely, Edward Snowden's whistleblowing, the Sony hack, and the resilience (or vulnerability) of the bitcoin as virtual currency. Throughout the discussions, the presenters should give the feel of real-world resilience problems so that the succeeding discussions will "anchor" our theories, formulations, concepts and frameworks to real problems where these may be applied realistically, and that the application is significant, relevant and compelling.

Part II. Explore Uncharted Grounds: Sharing our Novel Perspectives

This will occupy much of the meeting schedule. Presenters in both camps, each with even diverse disciplines, shall discuss their novel research works relevant to resilience. It may even make sense that each camp's presenter provides insights as to what is the gap that needs to be bridged with the other camp and how their work will benefit or can be applied by the other camp. This will pave the way for discussing plausible integrated approaches.

The goal here is to learn the depth and breadth, especially the latter, in resilience research. Even focusing on a single domain, the participant will hopefully realize the diversity of perspectives to the same set of problems. The organizers are expecting that at the end of this 1.5 days, the participants will come up with specific "themes" that may integrate some of the presented ideas.

Part III. Find Common Grounds: Establishing Integrated Approaches

In this session, the organizers will facilitate discussions around the themes identified in the previous parts, focusing on how the approaches by the two camps can be synthesized or amalgamated, hence, bridging the gap. The discussions among all present will be free-flowing. At the end, the organizers as moderators shall present the proposed integrations.

Anchors A-weigh: Upholding Concrete Action Plans Sailing Forward

To assure lasting fruits for the meeting, the organizers and participants will identify concrete actionable items, which may be short-term and/or long-term (e.g., future projects, workshops or joint publications).

Meeting at a Glance

February 22, 2015 (Sunday) 19:00 – 21:00

Welcome Banquet @ Restaurant Katsura

February 23, 2015 (Monday) 09:00 – 17:30
Venue: Research Wing, Room 208

Introductory Video of the NII Shonan Meeting

Welcome Address by the Organizers

Part I. Cast Anchor: Situating Real World Contexts

A contribution to generalize the scenarios, Hiroshi Maruyama and Günter Müller
Resilience of cryptocurrencies, Christian Brenig
Bitcoin: the reason why the decentralized currency achieves justice as fairness, Hitoshi Okada
Invited Presentation: Recent incidents and trend of cyber security, Shiroh Ohtsuru

Part II. Explore Uncharted Grounds: Sharing our Novel Perspectives

Privacy-preserving spot checking – a new kind of license plate, Florian Kerschbaum
Socio-technical analysis of resilience in secure, verifiable voting systems, Peter Ryan
Mathematical modeling for resilient energy system, Ryoichi Komiyama
Resilient graph partitioning for electrical grids, Kazuhiro Minami
Robust multi-team formation and its application to robot rescue simulation, Tony Ribeiro
Resilience and Intelligence, Katsumi Inoue

February 24, 2015 (Tuesday) 09:00 – 17:30
Venue: Research Wing, Room 208

Part II. Explore Uncharted Grounds: Sharing our Novel Perspectives (Continued)

Securely leaking a secret, Sven Dietrich
Impact on capabilities in enterprises exemplified by ooRexx, Rony Flatscher
Resilience in business process management, Günter Müller
Towards a resilience oriented decision support system for business processes, Richard Zahoransky
Benefits of parametric model-checking to assess the resilience of mammalian circadian rhythm, Morgan Magnin
Understanding human behaviors through plan recognition, Taisuke Sato
False rumor diffusion analysis based on the SIR-extended information diffusion model, Satoshi Kurihara
Perception-based resilience: Theories and models of human perception for resilience thinking, Rungsiman Nararatwong and Roberto Legaspi

On the evolution of beliefs in social networks, Nicolas Schwind
Limiting perturbations in dynamic DCOP: model with quality guarantee, Maxime Clement
Measuring a concept that has gone mustang, Patricia Longstaff

February 25, 2015 (Wednesday) 09:00 – 12:00
Venue: Research Wing, Room 208

Part III. Find Common Grounds: Establishing Integrated Approaches

13:30 – 18:00 Excursion @ Kamakura

18:00 – 21:00 Main Banquet @ a Japanese restaurant

February 26, 2015 (Thursday) 09:00 – 12:00
Venue: Research Wing, Room 208

Part IV. Anchors A-weigh: Upholding Concrete Action Plans Sailing Forward

Participants

Scholars from diverse disciplines were invited to attend the meeting. Resilience domain in itself is multidisciplinary, i.e., relating to several disciplines, as well as *transdisciplinary*, i.e., using approaches that transcend specialization boundaries. Secondly, these scholars have shown significant interest and contributions to advancing resilience thinking as they have demonstrated in international meetings that our team members also attended. We also invited PhD candidates who have demonstrated in our previous meetings critical thinking and research communication skills. Hence, we leveraged this diversity of participants to achieve the goals we set for the workshop.

Christian Brenig, The University of Freiburg
Hei Chan, The Institute of Statistical Mathematics (Transdisciplinary Research Integration Center)
Maxime Clement, National Institute of Informatics
Sven Dietrich, The City University of New York, John Jay College of Criminal Justice
Rony G. Flatscher, Wirtschaftsuniversitt Wien (Vienna University of Economics and Business)
Kazuo Furuta, The University of Tokyo
Günter Müller, The University of Freiburg
Katsumi Inoue, National Institute of Informatics
Florian Kerschbaum, SAP Applied Research
Ryoichi Komiyama, The University of Tokyo
Satoshi Kurihara, The University of Electro-Communications
Roberto Legaspi, The Institute of Statistical Mathematics (Transdisciplinary Research Integration Center)
Patricia Longstaff, Syracuse University
Morgan Magnin, École Centrale de Nantes, Institut de Recherche en Communications et Cybernétique de Nantes/ National Institute of Informatics
Hiroshi Maruyama, The Institute of Statistical Mathematics
Kazuhiro Minami, The Institute of Statistical Mathematics
Rungsiman Nararatwong, National Institute of Informatics
Hitoshi Okada, National Institute of Informatics
Tony Ribeiro, National Institute of Informatics
Peter Y. A. Ryan, University of Luxembourg, LU
Taisuke Sato, Tokyo Institute of Technology
Nicolas Schwind, National Institute of Informatics (Transdisciplinary Research Integration Center)
Tomoya Tanjo, The Institute of Statistical Mathematics
Richard Zahoransky, The University of Freiburg

Summary of Presentations and Discussions

Part I. Cast Anchor: Situating Real World Contexts

A contribution to generalize the scenarios

Hiroshi Maruyama and Günter Müller

*Abstract.*This two-fold presentation will discuss the Cyber-Physical-Systems (CPS) framework in light of these incidents, as well as position the incidents within an over-all resilience concept while making connections to various resilience techniques.

Discussion. Cognizant of the fact that resilience has been defined by various disciplines (e.g., social, ecological, biological, and engineering) and in different application domains, but most of the time partial and overlapping, a taxonomy and set of strategies for general resilience were presented to contextualize resilience. The presentation also highlighted a Systems Resilience (SR) model that can be viewed as a two-player, i.e., system and attacker (e.g., perturbations and disaster) game theoretic framework, where the goal is the system being resilient over the attacker. The presentation was able to elucidate how the SR model can be applied in the cyber-physical (as the system) domain.

Resilience of cryptocurrencies

Christian Brenig, The University of Freiburg

Abstract. Cryptocurrencies, like Bitcoin, are intended as innovative means to conduct transactions and are even considered as substitute for traditional fiat based currencies by some proponents. Our ongoing research is targeted at the economic opportunities and challenges associated with cryptocurrencies. How resilient are they against threats and attacks from inside and outside the system? Do they have the potential to serve as currency?

Discussion. The discussion centered on the three roles of currency, namely, account, exchange, and store, and the threat to these roles could include volatility, theft, and trust. Among the three, the issue of trust was highlighted as it related to discussions on beneficiary perceptions of the system.

Bitcoin: the reason why the decentralized currency achieves justice as fairness

Hitoshi Okada, National Institute of Informatics

Abstract. Bitcoin is a decentralized virtual currency based on P2P technology. It enables the unique distribution of electronic value from one person to another without the existence of a centralized issuer. Virtual currency circulates in an open-looped system as if it were real money, whereas existing electronic money circulates in a closed-looped system. The decentralization issue of virtual currency raises a question concerning the seigniorage profit, which ought to be under state monopoly. This presentation discusses the state for what reason currency issuance should be decentralized. We also discuss the ideal public

policy for virtual currency in order for decentralized currency to achieve justice as fairness.

Discussion. The problem with decentralized virtual currency is that seigniorage profit obviously no longer resides with the state and the real threat is that any individual user may actually monopolize (or the "51% attack") the entire virtual currency system. The proposed solution is *co-regulation*, which is the co-existence of market self-regulation (libertarianism) and government regulation (paternalism) that therefore establishes a complementary relationship that prevents any unwarranted monopoly from both sides.

Invited Presentation: Recent incidents and trend of cyber security

Shiroh Ohtsuru, Executive Architect, Global Technology Service, IBM Japan

Discussion. An interesting point that was raised is virustotal.com - although it provides a free service to check if a binary file contains a known virus, an attacker can use this service to make sure that his malware will not be detected by any existing antivirus software. A sample incident is that of Japan Airlines wherein a malware that was trying to convert mileage to amazon points was only discovered due to an unusual SQL load and not by any antivirus software. An implication of this is that there is no systematic method to discover an unforeseen attack. One solution that was stressed is to use big data analytics to monitor the total system behavior. Another interesting issue raised was on recovery, i.e., the point at which system service resumes - even if we are certain that every component of the system is clean (which is most of the time not the case unless there is some continuation), the question is whether stakeholders confidence can actually be obtained before the system restarts.

Part II. Explore Uncharted Grounds: Sharing our Novel Perspectives

Privacy-preserving spot checking A new kind of license plate

Florian Kerschbaum

Abstract. We show using a simple game-theoretic model that current solutions to spot checking for electronic invoicing require to survey all transactions and hence are not resilient at all. Then we present a cryptographic solution where users carry a device that randomly authenticates. We show that we can achieve a socially acceptable, resilient balance between privacy and the need for surveillance.

Discussion. In order to keep drivers honest in paying for their usage of the roads, toll collection systems rely on spot checks, i.e., roadside sensors, to catch potentially cheating drivers. The issue, however, is two-fold. First, the sensors clearly pose privacy problem as it informs where drivers (good and bad alike) are. Secondly, there is the collusion attack as a threat to the unpredictability of these spot checks - an attacker can reveal to drivers the locations of spot-check cameras, which is an information that drivers can then use to avoid paying road

fees. Although the attacker pays the penalty for recording the locations, he actually receives a kickback from the colluding drivers from the toll they saved. The proposed solution is a device that is cheap to manufacture and unobtrusive in operation but can reconcile privacy and spot checking with socially acceptable observation and penalties.

Socio-technical analysis of resilience in secure, verifiable voting systems

Peter Ryan

Abstract. Voting systems are typically large, complex socio-technical systems. Recently, significant progress has been made towards developing voting systems that provide so-called end-to-end verifiability (E2E V), typically using techniques and mechanisms from modern crypto. But like all large, security critical systems, the security and resilience depend not only the technical components but also on humans, procedures, etc. The properties that voting systems much satisfy are very subtle, including accuracy, ballot privacy, resilience, receipt-freeness and coercion resistance, accountability, etc., and they must be robust insider and outsider threats. In this talk I will sketch how such E2E V systems work and the challenges of analysing them w.r.t. the above properties.

Discussion. The aim of E2E V is to overcome "scalability bound", or wholesale corruption as threat to a voting system. With E2E V voters can confirm that their vote is accurately counted without violating the secrecy of their ballot. Voters get an encrypted or encoded version of their vote, or a "protected receipt", that are cast on a secured bulletin board for them to verify. The real challenge is to provide the voter with a usable way to encrypt her vote in a way that gives her confidence that her vote is correctly encoded while not providing a means to prove this to a third party. Further challenges include the resilience of this system as an open problem, as well as obtaining voter trust, i.e., voters need to feel secured with the system, as being a major issue.

Mathematical modeling for resilient energy system

Ryoichi Komiyama

Abstract. This presentation attempts to discuss the potential mathematical modeling for the evaluation of resilient energy system. The case study will be presented about energy security and power grid issues through applying mathematical methods such as stochastic dynamic programming.

Discussion. The fundamental argument was that resilience in energy systems needs to handle both structural (e.g., energy resource constraints, energy imbalance, climate change, etc.) and contingent (e.g., shocks in energy supply chain, military and political risks in energy production, panic behavior among energy consumers, etc.) risks. Furthermore, enhancing energy systems resilience can be achieved through diversification, redundancy, and strengthening emergency response.

Resilient graph partitioning for electrical grids

Kazuhiro Minami

Abstract. We introduce a graph partitioning problem for electrical grids such that a given grid is partitioned into multiple ones that are self-contained concerning electricity balance. Our goal is to find a resilient partition against time-changing power demand and supply over the year.

Discussion. Since a centralized electrical grid is vulnerable to unexpected events, a decentralized grid with renewable energy sources allow isolation of localized damages. Isolation is a promising strategy for building resilient systems. However, finding a resilient partitioning of the electric grid to allow efficient and effective isolation is not a trivial problem. The proposed solution is to study the graph clustering problem for decentralized energy management.

Robust multi-team formation and its application to robot rescue simulation

Tony Ribeiro

Abstract. In many multi-agent applications forming teams, which can accomplish given missions, is a key issue. In a dynamic environment that offers the possibility of losing agents during a mission, e.g. an agent is injured in a rescue mission, robustness of team is crucial. How to form robust teams that can continue to perform their own mission in the face of agents lost is what we try to tackle in our work.

Discussion. The goal is to form teams of agents to achieve given missions while considering the risk of losing agents during the missions. The mission should be achieved efficiently with the robustness of teams being crucial. Lastly, in constructing timely plans, there certainly are trade-offs between optimality of the solution and the computation time.

Resilience and Intelligence

Katsumi Inoue

Abstract. I will discuss the relationship between Systems Resilience and (Artificial) Intelligence. The relationship is multifold. Resilience can be formalized in terms of AI methodology, and AI can benefit from the concept of resilience. Moreover, future work on resilience should rely on the progress of AI.

Discussion. The proposed multifold relationship between Resilience and (Artificial) Intelligence is in terms of:

(a) *intelligence into resilience* (e.g., SR-Model): involves suitable abstraction of problems, logic for systems resilience, computation of resilience and the design of resilient systems;
(b) *resilience into intelligence*: selection of models that are robust, diverse, and adaptable, as well as design agent systems that are enforced stabilizability;
(c) *intelligence as resilience*: due to intelligence, humans are capable of thriving after extremely adverse events while trying to make (explain) and maintain (endure) sense in the midst of adversity; and

(d) *resilience as intelligence*: if humans are considered resilient due to their intelligence, future resilient systems should be designed to be intelligent too.

Furthermore, while it was raised that resilience and AI are worth exploring, one interesting topic can be the innovative or creative AI that can do scenario planning (e.g., AI acts as the perturbation or attacker in the scenario planning).

Securely leaking a secret

Sven Dietrich

Abstract. The risk taken by whistleblowers can be enormous, both in magnitude of their revelations and for their livelihood. In order for their secret leak messages to get through to the secure repository, they need a resilient and secure infrastructure. That infrastructure keeps it indistinguishable as to whether important information or just chaff is being broadcast over it, but also adds enough resilience to the transmission to tolerate bad actors interfering with the messages. We discuss such an infrastructure based on online ads.

Discussion. The intriguing idea here is to learn from your enemies. An example would be to embed command and control mechanism into the existing non-interruptable fabric.

Impact on capabilities in enterprises exemplified by ooRexx

Rony Flatscher

Abstract. Employing the "human-centric" programming language ooRexx (acronym for "Open Object Rexx") for modelling of services, to empower end-user programmers to define and implement algorithms for their work-domain to improve resilience. To exemplify the ideas a demonstration of this approach will be given.

Discussion. The main take-away here is that empowering employees with good tools makes the organization react more smoothly.

Resilience in business process management

Günter Müller

Abstract. Workflows are small computer programs that require fixed resources. Resilience is shown here that results can be guaranteed even if resources lack to be available. Three cases of resilience will be identified, where always one part of the specified resources fail. In computer science this leads to a stop and a non-termination. It will be demonstrated that bridging the gap is possible.

Discussion. The focus of resilience varies between (a) social science and (b) computer science and information science design. Resilience in the first is viewed as bouncing back from challenges or dangers that the individual or system could not resist due to lack of persistence over time when there is surprise, discontinuity and uncertainty. In the second, resilience is viewed in terms of the level of complexity that results often in undecideability, adaptive capability that

changes system properties (stability and equilibria), and the degree of normativity (assumptions about wanted or not wanted). The proposed solution is a layered definition of resilience that integrates technical, behavioral and political aspects. Furthermore, proposed resilience metrics are in terms of complexity, management, and normativity. Lastly, in terms of the workflow authorization with missing resources, resilience is viewed as the workflow not being disrupted.

Towards a resilience oriented decision support system for business processes

Richard Zahoransky

Abstract. This ongoing work demonstrates the possibility for IT-Systems to evaluate the resilience of business processes. First, data from process logs is examined. Operating on this data, in a second step, the resilience oriented decision support system assists humans by finding optimal strategies for processes facing failures or losses, thus increasing robustness and agility.

Discussion. Time distribution from process logs are seen as resilience indicator. By evaluating the process model using data from process logs, increase in resilience can be attained through proactive, i.e., enhance the model by adding alternative paths during development time, and reactive, i.e., intervene in process operation during runtime via decision support on critical instances. Furthermore, being able to measure the completion time of each step of the business process and estimating the probability that the completion time violates the given constraint, disruptions that perturb the system can be detected or predicted.

Benefits of parametric model-checking to assess the resilience of mammalian circadian rhythm

Morgan Magnin (A joint work with Alexander Andreychenko and Katsumi Inoue)

Abstract. Understanding the mechanisms involved in oscillatory biological regulation is a fundamental issue to analyze living systems. Time delays play a major role in the sustainability and control of oscillations, as shown for example in phenomena related to the mammalian circadian clock, a system well-known for its reactivity and adaptability with regard to various but major changes. In this talk, we formalize these properties in terms of resilience through modal logics (TCTL) and show the benefits of parametric model-checking to analyze the dynamics of a simplified model of circadian clock.

Discussion. Boolean networks can demonstrate resilience. This means that even simple discrete mechanism is capable of constructing a resilient system.

Understanding human behaviors through plan recognition

Taisuke Sato

Abstract. Understanding human behaviors in cyberspace is a big problem. We present a novel plan recognition method applicable to incomplete observations of human behaviors.

Discussion. The talk is related to Sven Dietrich's theme on learning from the attacker. The formulation here is a simple Bayesian inference. The big question, however, is who defines the possible attack space.

False rumor diffusion analysis based on the SIR-extended information diffusion model

Satoshi Kurihara

Abstract. Twitter is a famous social networking service and has received attention recently. Twitter user have increased rapidly, and many users exchange information. When the 2011 Tohoku earthquake and tsunami happened, people were able to obtain information from social networking service. Though Twitter played the important role, one of the problems of Twitter, a false rumor diffusion, was pointed out. In this research, we focus on a false rumor diffusion. We propose an information diffusion model based on SIR model, classify the way of diffusion in four categories, and reappear the real diffusion by using this new model.

Discussion. Two models for false rumor information diffusion for SNS were proposed, namely, the SIR- and multiagent-based approaches. While the SIR model, which is a famous model of the diffusion of infectious diseases, as applied to information dissemination over the net could produce single-burst diffusion, the multiagent-based model could produce multi-burst diffusions. This is because the SIR-based model does not take into account the multiplex path of communication among users in the network.

Perception-based resilience: Theories and models of human perception for resilience thinking

Rungsiman Nararatwong and Roberto Legaspi (A joint work with Hitoshi Okada and Hiroshi Maruyama)

Abstract. Perception-based resilience is the ability of a system to be resilient to stakeholder perceptions during crisis. We introduce this concept as a framework, together with our related theories and models, which particularly focus on the dynamics of user perceptions in social media. In a two-fold elucidation, we shall explain (a) our mental state model that explains individual perception changes when exposed to negative attributions to the system and (b) how theories of social identity may help understand and manage the crisis appropriately by leveraging public perceptions.

Discussion. Perception-based resilience bridges the gap between the actual and perceived (by the beneficiaries) state of the system. One interesting point that was raised is that we may lose focus if we take on the "perception first" approach. This means that we may compromise the genuine design and full recovery of the system if only to satisfy people's perception of how the system should be. Although this can be debated on a philosophical level, the issue remains important.

On the evolution of beliefs in social networks

Nicolas Schwind (A joint work with Katsumi Inoue, Gauvain Bourgne, Sbastien Konieczny, Pierre Marquis)

Abstract. In brand crisis management, negative content regarding a brand could disseminate rapidly over social media and generate negative perceptions. In such a case, identifying how information is propagated within a social network and which are the influential agents (the opinion leaders) is a hot research topic. In this work, we introduce a framework to model the evolution of beliefs in social networks, called Belief Revision Games (BRGs). BRGs are zero-player games where at each step every agent revises her own beliefs by taking account for the beliefs of her acquaintances. We provide a general definition for such games where each agent has her own revision policy. We point out a set of appealing properties for BRGs and investigate the extent to which these properties are satisfied by some merging-based policies under consideration. BRGs are useful to model the evolution of beliefs in a group of agents in social networks, and to study several interesting notions such as influence, manipulation, and gossip.

Discussion. The contribution is a formalization of the BRG with a set of appealing properties, namely, preservation (consistency, agreement, and unanimity), responsiveness, and convergence to stable beliefs. This idea have several applications, such as determining the conditions in which gossip can propagate, determining which agents are opinion leaders, and how robust are BRGs when it comes to manipulation, among others.

Limiting perturbations in dynamic DCOP: Model with quality guarantee

Maxime Clement

Abstract. Distributed Constraint Optimization Problems (DCOP) is a framework to model many artificial intelligence and multi-agent coordination problems. In many real world problems, new solutions must be found whenever changes occur. However, a transition to a new solution induces an additional cost in real situations. We propose the Limited Perturbation Problem (LPP) where the goal is to find the best possible solution while limiting perturbations in a Dynamic DCOP.

Discussion. Multidimensionality of the objective function is always the case in non-trivial situations. Computation time is an issue, and this is related to Ribeiro's talk.

Measuring a concept that has gone mustang

Patricia Longstaff

Abstract. The basic concept of "resilience" has escaped from various disciplinary stables and is living in an interdisciplinary "wilderness". Should we tame it again? Will this inhibit its ability to adapt and evolve to new conditions? A partial "taming" is suggested to allow resilience to be measured and used in a variety of research and policy debates.

Discussion. This presentation represented the pure "social" side of the equation. Due to the escape from the comfortable silos, resilience researchers now need to pay extra efforts to communicate with others. She stressed the importance on humility and tolerance. It raised some debate among the participants, but at the same time it also suggests that humility and tolerance would be one of the viable strategies in case of a large shock, such as a disaster. Also it was pointed out that the tension between efficiency and resilience is seen in many systems.

A couple of questions was raised by the discussant:

(a) *Resistance or resilience?* Resistance is acceptable if an attack can be prevented. However, if there is no systematic method by which an unforeseen attack can be predicted, then the system has to have resilience.
(b) *Resilience of what?* Using the analogy of assets encased in a brick wall, we should ask whether we desire the resilience of the walls or the assets. In other words, what do we want to measure?

Pertinent to the resilience of cyberphysical systems, breaking the resilience of attackers would involve reducing the ability to adapt by increasing tight coupling (reduce individual options) and lowering diversity of resources and info. The other end, i.e., to increase the resilience of the "good guys", would involve loosening the coupling without practical drift and increasing the diversity of resources and options for the function.

Part III – Summary of Theme-based Group Discussions

Following the presentations of all the participants, we were divided into four smaller groups and had discussions on specific themes. They are: (1) Cyber Currency, (2) Cyber Security, (3) Business Processes, and (4) Internet of Things. We were tasked to explore new ideas for making the cyber security aspect of each theme more resilient.

Cyber Currency

This team discussed resilience of cyber currency systems. One example of such cyber currency is Bitcon and was extensively discussed in Part I of this meeting, but this team tries to capture general ideas about how to make future cyber currency more resilient. Threats to cyber currency was categorized into two layers – for individual transactions and for the social level.

For protecting individual transactions, two general strategies are identified: *Blockchain* that makes hard to counterfeit transactions, and *Distributed System* that eliminates a single point of failure. These countermeasures are mainly technical.

As for the society level, the situation is more complicated. First, any cyber-currency has to have some means to converting from/to existing currencies (i.e., *liquidity*). Cyber currency without liquidity will most likely disappear as a monetary instrument. This involves interplay with the very complex global financial systems, economic situations, government regulations, and culture (e.g., some culture puts more trust on cash). Second, cyber currency tends to have higher volatility. Bitcoin's exchange rate experienced a multiple order of magnitude fluctuations in a short period of time. If the value of a cyber currency suddenly drops, it means a serious threat to the existence of the cyber currency. Third, any cyber currency is dependent on a certain set of cryptographic technologies, which may eventually be compromised. Fourth, it is still unclear who gets benefits from cyber currency. If the benefits are evenly distributed to the stakeholders, it is likely to be used longer. If there are hidden beneficiaries of the cyber currency, it could be fragile.

Another issue that was raised during the plenary discussion was the boundary question. A cyber currency is not a self-contained system. Resilience of a cyber currency is not attainable without resilience of the other parts of the society. Thus, the "boundary leakage" issue that we discussed during the Part II of this meeting also applies here.

Cyber Security

This team tries to identify major threats to cyber security in our future society and their countermeasures.

Considering the upcoming technology adaption in our society, the team identified the following five areas as major threats: Drones, Power Plants, DDoS (Distributed Denial-of-Service), Doping, and Communications. Drones are new technology, and their implications to cyber security have not investigated well. However, it is clear that if an attacker can take the full control of drones that are designed and operated for legitimate purposes (e.g., disaster surveillance),

potential damage inflicted would be large. Other civil infrastructures such as power plants also have similar vulnerability.

Countermeasures were mainly discussed on the people (or societal) side – the team identified people education, drills, and emergency plans are major countermeasures. Also following the ideas presented in the Part II of this workshop, they discussed how to focus on the people aspect of the attackers, including surveillance and counterattacks. One final comment made by the team was that if it is hard to attain a desired level of resiliency, stopping using the cyber system and reverting to manual operations is one option.

Business

How to make business processes more resilient when facing cyber security threats was the topic of this team. The team first set the assumption that the overall cost of business operations is their utility function and then discussed potential strategies to make business processes more resilient.

When a "shock" is induced to a business process (by a cyber attack in this case), the team identified three layers of adaptation processes. The first layer is the control loop – that is, Wiener-sytle feedback mechanism needs to be built into the business process design. This mechanism should be able to absorb relatively frequent but small disturbances. The second layer is the dynamic changes of business processes. One example would be switching a supplier when the supplier is unable to deliver necessary parts due to a cyber attack. This layer can be facilitated by an appropriate provisioning of technology, such as the ones discussed by Rony Flatscher and Richard Zahoransky. Then there are situations that requires the top level management decisions to deal with, and that requires decision support systems.

In order to make business processes resilient, the team stressed the importance of maintaining the resilience at all layers.

Internet of Things (IoT)

This team is tasked to focus on Internet of Things, but the discussions strayed to more general resilience. The ideas discussed are listed below.

- Strategies to achieve resilience would include agility, improvisation (old goal with new path), innovation, isolation, a holistic assessment that may involve introducing controlled shocks (e.g., penetration tests, white hackers, "chaos monkeys", "beehive trucks"), layered resilience/ panarchy/ "boundary leaks", and presence of trusted sources.

- Factors that hinder resilience (and promote vulnerability) include rigidity, tight coupling, slow recovery, frequenting shocks, and increasing correlations.

- The difference between efficiency and resilience may lie in the temporal aspect. If intervention or recovery can or should be attained in the short term, then the system should be efficient and optimal in its response. However, if the system would need to sustain itself for the long term (say, until 100 years), then it has to be resilient.

- Efficiency is an "enemy" of resilience (Longstaff) and convenience may impose risks.
- Resilience thinking should take into account culture.
- Question raised: Is singularity a solution for resilience? Singularity refers to the profound and extremely rapid technological and scientific advances that can drastically transform (previously unknown novel associations and functions) life as we know it.
- Question raised: Can disobedience to rigid rules yield resilience?

Conclusion – Take-Aways and Next Steps

The organizers concluded the workshop with the short plenary discussion on the over-all systems resilience themes. We found that the following aspects of resilience had been repeatedly discussed during the workshop:

1. *Known vs Unknown.* Some researchers focus more on "known unknowns" such as natural disasters (they have been seen in the history albeit infrequently), but there was always the question of whether we should consider the "unknown unknowns". However, considering the "unknown unknowns" poses at least two big challenges, namely:

   - There are noncomputable aspects [4][5]. Predictions will be inaccurate and uncertain since statistical extrapolations are based on a handful of analogous past experiences or mechanistic models that mislead to dire situations [4]. What exists is the dearth of historical data for robust predictive analyses [5]. For example, Engineering Resilience and mathematical models have been mainly focusing on "known unknowns" because the probability distribution of "unknown unknowns" cannot be specified by definition. We believe that responding to "unknown unknowns" requires understanding the limitations of mathematical models and integrating mathematical and social thinkings.
   - While the problem poses significant complexity, our approaches and models persistently demonstrate linear, fragmented, and incomplete knowledge. The problem is highly complex, indeed chaotic, that involves nonlinear behaviors that span across multiple and simultaneous temporal and spatial scales, and plausibly with large interrelations and interdependencies among variables. Such behaviors can cause one situation, albeit a small perturbation, to become critical and trigger other events in a cascading fashion such that the different situations within the cascade also move towards criticality.

   There are excellent suggestions in the literature on how to overcome these problems. For example, Carpenter et al. suggest [4] that our tendency to deny the noncomputable aspects can be countered by considering a wide variety of sources of knowledge and stimulate a diversity of models. Another is McCracken who proposes [5] a framework on how socio-technical systems can come together on cyberspace to obtain and integrate data from various sources for robust predictive models. The solutions to these problems, however, remain to be partial.

2. *Efficiency vs. Resilience.* We realized that many of our discussions were reduced to the question of whether we want more efficiency or more resilience. Longstaff stated the importance of having some agreement to this, e.g., since this issue challenges some major assumptions in business and public policy thinking, she raised the excellent question of how to get this trade-off into business and policy debates.

3. *Bounce Back vs. Bounce Forward.* Engineering resilience is often considered to be an ability to bounce back, i.e., the system goes back to the

original state after a perturbation. In the social context such as organizations and cities, a painful shock also presents an opportunity to innovate. This aspect of resilience is termed as "bouncing forward". It may also be the case that, independently, the two are insufficient as best recovery path and the assessment of backward-forward trajectories offers an optimal strategy [6].

The idea of resilience as bouncing forward has been presented in various domains, e.g., human development [7][8], engineering [9], and social science [9-11], among others. There seems to be a general agreement on the importance of this concept. However, most would operationalize rather than formalize this concept due to the difficulties associated with formalizing. Hence, how to formalize the concept is an open research problem.

4. *Boundary Leaks.* Even when a system is permanently damaged, if we enlarge our scope to the enclosing system that includes the damaged system as its subsystem, we may be able to achieve resilience of the larger system. Different forms of this "boundary leak" idea appeared in multiple different contexts in the workshop. This suggests that we may have to be flexible in terms of the system boundary, and should always be ready for the fallback plan, that is, to save the larger system in case the subsystem cannot be saved. It was also suggested that these resilience plans have to be prepared at all the levels of potential system boundaries.

5. *Metrics.* Metrics of resilience have been always the issue, which is closely related to the debate on the exact definition of resilience. It was pointed out that because resilience is context dependent (as presented by Maruyama at the beginning of this workshop), metrics should also be context dependent. This makes sense, and requires further investigation.

   It is also the case, however, that Longstaff raised pertinent issues on resilience metrics being context-dependent. First, are there variables that are context independent, i.e., general across different contexts (in the same way that diversity, redundancy, and adaptability are general resilience strategies) and therefore should be at least considered in each context? Second, is it possible to measure these? Lastly, what is their relationship to each other if any, e.g., does one move another by a predictable amount or in a predictable direction?

   It was pointed out that one important aspect of resilience metric is the distinction between the performance metric, i.e., what was the performance of the system given a particular timeline, and the competency metric, i.e., how the system is prepared for future events. The performance metric can be captured in situations where the system performance is clearly defined, such as in Bruenau's resilience triangle. The competency metric is measured in aspects like adaptability and tight coupling. The ROIS team is working on formalizing the relationship between the performance metric and the competency metric.

The purpose of this workshop is to bridge the gap between the social and mathematical. Although majority of the participants were more on the mathematical side, we had significant amount of "social" discussions. Most important

is that we captured the following three points as ideas for making systems more resilient:

1. *Empowering Operators* If an unknown-unknown event happens, improvisation is necessary. Improvisation requires an out-of-box thinking and sometimes involves breaking rules. If the system operators are afraid of making mistakes, they are likely sticking to the rules and may miss the opportunity to improvise. How to empower the system operators by providing appropriate tools (as in Flatscher's presentation) and resources and to encourage them to improvise would be an important area of social resilience research.

2. *Learning on Attackers.* Predicting what shock comes next is one of the key resilience strategies. If the shock comes from an intentional attacker, understanding its capabilities and plans enables better preparations for the incoming attack. This "intelligence" can be done by social techniques such as those employed in anthropology, as well as mathematical modeling such as the plan recognition presented by Sato.

3. *Influence on Beneficiaries.* The mathematical camp usually deals with the resilience of the system itself. However, Nararatwong and Legaspi pointed out that there are cases where the system is resilient but the beneficiaries (people) do not perceive it as such, or the other way around, i.e., the system is vulnerable and yet people's perception tolerates the vulnerability. This aspect of perception-based resilience should be further investigated.

Further Recommendations

The workshop was engaging and productive. However, a significant portion of the domain has yet to be tackled and the depth of the issues raised demand further explorations and investigations. Hence, a sequel of the workshop is warranted with the following major points to consider in the preparations:

- The sequel should further focus on the synergy between the social and mathematical. This means anchoring to a particular domain and attempting to both operationalize and formalize aspects of resilience.

- Cyber-security should once again be the focus due to it being an ever growing concern. With security being breached in governments (e.g., Snowden incident) and big companies (e.g., Sony, Target, eBay, Apple, etc.), for example, there is the consistent doubt about the security of our information that can have local (including personal) and global effects when breached.

- Motivated with the issues we raised, the sequel should attempt to identify the venues where they can be optimally debated (i.e., with the intent to resolve within a definite time frame) and the pertinent people who should tackle them.

References

[1] P. Bak, How Nature Works: The Science of Self-Organised Criticality. New York, NY: Copernicus Press, 1996.

[2] M. Scheffer, S.R. Carpenter, T.M. Lenton, et al., "Anticipating critical transitions," Science 19, vol. 338, no. 6105, pp. 334–348, 2012.

[3] N. Schwind, T. Okimoto, K. Inoue, et al., "Systems Resilience: A challenge problem for dynamic constraint-based agent systems," Proc. 12th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2013), Ito, Jonker, Gini, and Shehory (Eds.), May 6–10, 2013.

[4] S.R. Carpenter, C. Folke, M. Scheffer, et al., "Resilience: Accounting for the noncomputable," Ecology and Society, vol. 14, no. 1, article 13, 2009.

[5] J. McCracken, "In the shadow of 9/11," in T.B. Fowler and M.J. Fischer (Eds.), "Rare Events: Can We Model the Unforeseen?" Sigma 10, vol. 1, pp. 30-35, 2010.

[6] A.Y. Grinberger and D. Felsenstein, "Bouncing back or bouncing forward? Simulating urban resilience and policy in the aftermath of an earthquake," Proc. Institution of Civil Engineers: Urban Design and Planning, vol. 167, no. 3, 2014.

[7] S. Crawthorn, Bounce Forward: How to Transform Crisis into Success. Wrightbooks, 2013.

[8] M. Sleijpen, F.J.J. ter Heide,T Mooren, et al., "Bouncing forward of young refugees: A perspective on resilience research directions," European Journal of Psychotraumatology, vol. 4, 2013.

[9] P.H. Longstaff, T.G. Koslowski, and W. Geoghegan, "Translating resilience: A framework to enhance communication and implementation, Proc. 5th International Symposium on Resilience Engineering, June 2015.

[10] J.B. Houston, M.L. Spialek, J. Cox, et al., "The centrality of communication and media in fostering community resilience: A framework for assessment and intervention," American Behavioral Scientist, vol. 59, no. 2, pp. 270-283, February 2015.

[11] S.B. Manyena, G. OBrien, P. O'Keefe et al., "Disaster resilience: A bounce back or bounce forward ability?," Local Environment, vol. 16, pp. 417424, 2011.