NSF-IUSSTF Workshop on Distributed Infrastructure for Security Monitoring and Intelligence Extraction

Indian Institute of Science, Bangalore

9-13 January 2010

Dr. Timothy Finin
Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Baltimore MD 21250 USA
finin@umbc.edu

Dr. Bhavani Thuraisingham
Department of Computer Science
University of Texas at Dallas
Richardson, Texas 75080 USA
Bhavani.thuraisingham@utdallas.edu

Dr. Veni Madhavan
Computer Science and Automation
Indian Institute of Science
Bangalore 560 012, India
cevm@csa.iisc.ernet.in

Dr. Indranil Sengupta
School of Information Technology
Indian Institute of Technology
Kharagpur 721302 India
isg@iitkgp.ac.in

Executive Summary

We describe the results of a workshop on *Distributed Infrastructure for Security Monitoring and Intelligence Extraction* that was held 9-13 January 2010 at the Indian Institute of Science, Bangalore with partial support from the US National Science foundation (NSF) and the Indo-US Science and Technology Forum (IUSSTF). The workshop was attended by 31 researchers from both Indian and the United States institutions and included representatives from universities, industry and government. The focus of the workshop was research and technology development for real-time security surveillance and intelligence for critical physical and cyber infrastructure and their associated computing and communication components. Three goals were pursued: to explore the research problems and approaches underlying physical and cyber infrastructure security, to develop a research roadmap for medium and long term research on infrastructure security, and to help establish and strengthen collaborations between the US and Indian researchers. The ultimate results are expected to be of direct benefit to both the United States and India for better management of public safety and security in the face of natural disasters and terrorist events.

Examples of events that motivate this research can be found in the news nearly every month, including terrorist attacks on public places, natural disasters affecting large areas and cascading failures in complex infrastructure systems. Understanding such evolving large scale events is essential to taking remedial measures.

Our dependency on increasingly complex and automated infrastructures will only grow and the cyber and physical components are becoming deeply intertwined. Both components are vulnerable to damage from terrorism, state-sponsored attacks and natural disasters. It is a world-wide problem that can span national borders, especially as the world's economic and social systems become more integrated. An important consideration is to increase security while minimizing loss of information sharing and preserving privacy.

The high level vision of the group is to address the scientific and engineering challenges underlying the design, development, analysis and deployment of secured infrastructure systems. This will require exploring the limits of systems ranging from largely autonomous systems to synergistic man-machine systems. We recommend creating an international collaborative research program between India and the US that will include researchers from academia, industry and government. The program will frame the problem with one or more grand challenge problems and also encourage the exchange of young researchers and students between the two countries.

Creating a joint Indo-US research program in this area has unique challenges but offers great opportunities and potential. The workshop participants developed some strategies, plans and recommendations for specific actions, some of which have already been put into motion.

We recommend that appropriate funding agencies, e.g., NSF in the US and DST in India, establish a program to support international collaboration focused on cyber and physical infrastructure security that will support research, education and engagement of government, industrial and academic stakeholders. Specific targets can include developing and sharing testbeds for simulation; experimentation, data collection and analysis; access to and testing on real-world data sets; and activities to sustain collaborative effort including meetings, workshops, and exchanges.

Introduction

As the world has become more developed, industrialized and globalized, its reliance on critical physical and cyber infrastructure has increased. This infrastructure includes many systems such as electrical power generation and distribution, roads, bridges and tunnels that make up our ground transportation system, airports and air traffic control supporting airline transportation, communication networks, both wired and wireless, systems for storing and distributing water and food supplies, medical and healthcare delivery systems, and financial, banking and commercial transaction assets.

These systems are vulnerable to disruption and damage due to natural disasters such as earthquakes or hurricanes, social crises like wars and riots, and terrorism that deliberately targets infrastructure to injure, disrupt and frighten citizens. Our economy, public safety, and national security rely on our ability to monitor and protect these systems and to quickly remediate and repair any damage that might be done to them.

In January 2010 we held a workshop on *Distributed Infrastructure for Security Monitoring and Intelligence Extraction* at the Indian Institute of Science, Bangalore. Support from the US National Science foundation and the Indo-US Science and Technology Forum helped to fund the participants travel and other expenses. The workshop brought together 16 researchers from Indian universities and companies and 15 researchers from US universities, companies and government organizations. The focus of the workshop was research and technology development for real-time security surveillance and intelligence for critical infrastructure and their associated computing and communication components.

The choice of Bangalore was motivated by the presence of many institutions of higher education and research labs in and around Bangalore and a chance to co-locate the event with two meetings -- the 16th IEEE International Symposium on High-Performance Computer Architecture and the 15th ACM SIGPLAN Annual Symposium on Principles and Practice of Parallel Programming. We were able to share the group rates at several Bangalore hotels with these meetings as well as holding a joint social event. Our workshop was held at facilities provided by the Indian Institute of Science, Bangalore.

Workshop goals

The workshop was guided by three broad goals: to explore the research problems and approaches underlying physical and cyber infrastructure security, to develop a research roadmap identifying medium and long term research issue for infrastructure security, and to help establish and strengthen collaborations between the US and Indian researchers in this area. The ultimate results will be of direct benefit to both the United States and India. The expected results include techniques for better management of public safety and security against threats such as natural disasters and terrorist events.

Infrastructure security

This workshop addresses infrastructure security, an issue of high national priority in both the United States and India. Its major objective is to initiate research and cooperation mechanisms among US and Indian scientists to monitor, prevent, and recover from natural and inflicted disasters by exploiting advanced technologies such as smart sensors, wireless networks, mobile agents, data and text mining, and profile-based learning

in an integrated, collaborative and distributed manner. The research will focus on a framework consisting of real-time data gathering and fusion from a variety of sources to make online intelligent decisions while the events being monitored are unfolding and thereby provide actionable intelligence in real-time to lessen the loss of property and lives.

The uniqueness of this workshop topic lies in the synergistic combination of the proposed research in real-time data collection and information processing and intelligent situation awareness (e.g., threat detection) in an environment where the data is being generated by not only the known and preconfigured sensors but also by ad hoc sources such as mobile phones (with and without cameras). An important component here is intelligent situation awareness that requires new learning, data mining, dimensionality-reduction, social networking, and knowledge discovery techniques. The development of one or more prototype systems, both in the US and in India, and their inter-linking will go a long way in proving the technologies and synergistic learning from several different contexts.

The infrastructure security topic involves challenges in a variety of areas including distributed systems, wireless and mobile networks, sensors networks, data mining, machine learning, real-time feature extraction, information extraction from text, social networking, real-time fusion of data from heterogeneous and uncoordinated devices, real-time storage and processing of massive amounts of data, incremental intelligence revision as more information becomes available, handling data robustness, reliability and availability in fluid environments where the data sources themselves are dynamic and possibly under attack.

The purpose of the workshop had been to bring together experts from academia, industry and government to explore the various facets of the challenges involved and put together a comprehensive plan to tackle them. It was expected that the workshop will generate the core of an inter-disciplinary research proposal involving strong collaboration between US and Indian researchers to carry out the research. The workshop will also flesh out plans for prototype development and explore the partnerships necessary to get them off the ground. It is expected that the resulting proposal will be further refined following the workshop and submitted for co-funding by relevant agencies in both India and the United States. An important component of the workshop will be to lay out plans for exchange visits by researchers and students in the respective countries, the joint supervision of Ph.D. students, and development of educational material to excite and encourage students and young researchers to get them involved with this effort.

There is a growing need to establish and foster inter-disciplinary research of both theoretical and practical nature to cope with the rapid proliferation of both threats and challenges. Mechanisms for sharing "data" for analysis and the "techniques, algorithms and computational implementations" are important. The groups from the two countries have many complementary talents and infrastructures to handle the various issues. This workshop will provide a timely and crucial opportunity to develop plans to exploit these complementary strengths and produce a roadmap toward common goals.

Participants and organizers

The workshop was organized by four senior academic researchers, two from the US and two from India. The US organizers are Professor Tim Finin from the University of Maryland, Baltimore County and Professor Bhavani Thuraisingham from the University of Texas, Dallas. The India organizers were Professor Veni

Madhavan of the Indian Institute of Science, Bangalore and Professor Indranil Sengupta of the Indian Institute of Technology, Kharagpur. A complete list of participants and their affiliations is given in Appendix 2.

Meeting agenda

We met for five days from 9:00 am to 5:00 pm except for the last day, when we stopped after lunch. We began on the first day by discussing the workshop objectives, goals and "non-goals" and continued with a series of talks by the participants focused on the topics of applications and sensing issues. On the morning of the second day we continued with participant talks in the morning on three areas: Reasoning, understanding and control. In the afternoon, we held our first breakout sessions, and held three breakout sessions on sensors, reasoning, and architecture. On day three we had more individual presentations in the morning and coalesced our breakouts into two groups, one focused on completely automated systems for monitoring and responding to infrastructure attacks and problems and the other exploring systems with a "human in the loop". On the fourth day we had the final set of individual presentations in the morning followed by breakouts on automated and interactive systems and concluding with reports from the breakout leads. We spent the morning of the last day discussing our results and interacting with Dr. Arabinda Mitra, the director of the Indo-US Science and Technology Forum. A list of the individual presentations and a detailed agenda is provided in Appendices.

Breakout sessions

Our general schedule was to have individual presentations in the mornings and breakout sessions in the afternoon, with final, short reports from the breakout groups at the end of the day. Our initial set of breakout sessions reflected one way to organize the problem as comprising three general issues: sensing, reasoning and architecture. The first focused on developing sensors to collect important low-level data from and about the infrastructure systems being monitored. The second dealt with designing systems that reason with the sensor output to detect, interpret and diagnose problems. The final breakout topic explored architectural issues involving the fundamental distributed nature of the problem.

In the initial breakouts it became clear that it was difficult to talk about any of the three areas in isolation since sensing, reasoning and architectural design were necessarily intertwined. For the second and third sets of breakouts, we refractored the groups based on our consensus that we would need two kinds of infrastructure protection systems: ones were largely autonomous and operated with minimal human intervention and collaboration and ones designed to have people "in the loop" in many capacities.

Sensors

The sensor group (led by Ehab Al-Shaer) defined a general sensor as an agent that assists in the capture of information that could include hardware devices, software components, or human networks (e.g., via social media data). The capabilities of such sensors could vary, depending on their type, sophistication and domain. General capabilities include data capture, sampling, filtering, aggregation, event detection, and tracking. They identified four categories of sensors that were relevant to monitoring and protecting our physical and cyber infrastructures:

- Physical sensors cover application-specific infrastructure sensors for specific systems, including transportation, electrical, oil, gas, water, and others.
- Behavioral sensors include those that observe human behavior (e.g., cameras, motion, interactions, etc.), social network systems (e.g., popular public Internet systems like twitter and blogs) and sensors that detecting the "intangible" in human behavior, such as observing phase changes in crowds and infer intent or sincerity from behavioral signals.
- Physical sensors that focus on chemical, biological and radiological signals are needed to detect and monitor potential weapons and unfolding attacks.
- Sensors for data networks monitor the scalability, availability, and reliability of the networks that underlie our cyber-infrastructure.

The group identified two "grand challenge" ideas: (1) detecting anomalies in human behavior relevant to terrorism or other threats (both a sensing and reasoning challenge) and (2) leveraging and exploiting millions of cell phones in support of disaster recovery to help locating missing people, measuring population density, determining evacuation routes, and gather sensor information. The breakout identified three research catalysts: (1) broad data sets, e.g., biometric sensor data tested on both western and Indian physiology, (2) physical sensors and sensor networks tested in broad range of conditions in India and US under different geography, climate, infrastructure, population density, and languages and (3) common research test beds, platforms and formats.

Reasoning

The reasoning group (led by Sharad Mehrotra) discussed higher level reasoning, interpretation and datamining over more abstract representation using ontologies and shared data models. A wide range of techniques and approaches are involved, from signal processing of relatively low level sensor output, to statistical data mining and machine learning, and finally to high level theorem proving, abduction and argumentation.

Three "grand challenge" problems were discussed. The first was whether it is possible to develop a general purpose reasoning system that can create situational representation from multimodal information, contextual data, domain semantics, etc. Such a system would involve active information fusion, detecting relevant entities and events (and ontologies for describing them), representations for modeling and using provenance data and uncertainty, handling inconsistencies and contradictions, and operating in real-time dynamic environments. The second was the development of an end-to-end model for infrastructure trust and security. Key issues are how to model the human aspects of the system, the cyber aspects and their interdependencies. A final challenge is how to build reasoning systems that cooperate and collaborate with people acting as humans-in-the loop. A key insight was that the infrastructure is the composition of technology, people and process.

Architectures

The architecture group (led by Anupam Joshi) focused on software and networking architectures in support of families of applications, including appropriate security and policy enforcement. It identified a collection of research challenges, both small and grand. One set of challenges surround policy-based management systems, where issues include dealing with configuration changes and the timely verification of policies through

online calculations. A traditional ACL might work, but the state space may "explode" if there are too many undefined variables. A related issue is the automatic discovery, maintenance and adaptation of policies, obviating the need for complex policy engineering and management systems. A second challenge is storage survivability. Securing storage over time is needed to guaranty the survivability of critical data. A third challenge is the modeling of large scale scenarios involving multiple or cascading failures. Such situations can involve problems of configuration management and consistency with multiple ISPs and multiple parties. In such scenarios we do not have good visibility and must operate with partial information. Furthermore, there are deep information sharing issues involving privacy and the desire to protect proprietary information.

Autonomic systems

This group (led by Anupam Joshi) considered systems that were completely autonomic or mostly autonomous with a few, well defined and limited points of human interaction and direction. Such systems are appropriate and in many cases required when the complexity and speed of monitoring, diagnosing and reacting to situations is beyond human capabilities.

The group identified and discussed several application scenarios. These included a fire or other disaster in a confined space, requiring rapid sensing and response, flood prediction, both early warning and response, the protection of train transportation system and cyber-physical infrastructure protection, e.g. a smart grid network. A number of advantages and disadvantages were explored including the following.

One advantage of autonomous systems is that privacy is less of an issue when people are not in the loop. A concern is real time robust reasoning with bounded error is much harder in completely autonomous system. One approach that offers promise is to use data mining over historical information to build a more adaptive system that could both plan for and react to new and unexpected scenarios. A great deal of time was devoted to exploring the question of what can and cannot be done in a fully automated fashion, an issue that remains unresolved.

Synergistic man-machine systems

The final breakout group (led by Ponnurangam Kumaraguru) discussed systems that are designed with one or more humans "in the loop". A goal is to design, develop, and deploy synergistic man-machine secured infrastructure systems that can exploit the advantages of both people and machines for sensing, reasoning, and control. Various research challenges for all three areas were identified. Models for shared and collaborative man-machine sensing and reasoning are not well developed. For control, there are real dangers of human information overload and the need for time to make appropriate decisions.

Outcomes and recommendations

The workshops addressed infrastructure security, an issue of high national priority in both the United States and India. The major objective is to monitor, prevent, and recover from natural and inflicted disasters by exploiting advanced technologies such as smart sensors, wireless networks, mobile agents, data and text mining, and profile-based learning in an integrated, collaborative and distributed manner. The workshop focused on the exploration of frameworks consisting of real-time data gathering and fusion from a variety of sources to make online intelligent decisions while the events being monitored are unfolding and thereby provide ac-

tionable intelligence in real-time to lessen the loss of property and lives. The workshops also discussed concepts and ideas relevant to other important topics, including *smart grid* technology for energy savings and *protecting privacy* in a world of increased automatic monitoring of cyber-physical systems.

The workshop participants reached a consensus on a number of ideas and recommendations for future activities to improve our ability to monitoring our important physical and cyber infrastructure systems to protect them from natural or man-made damage. We hope that these will lead to significant research funding opportunities in both countries that will support collaborative research between groups from the two countries. This research has the potential to have far reaching consequences on our ability to manage the new security threats in both cyberspace and the physical world. We describe the key insights we gained from the workshop, plans and recommendations for future actions, and specific recommendations for funding agencies in the US and India.

Insights gained

The participants accomplished some specific outcomes in preparing for the workshop, during the week-long meetings and in subsequent discussions by email. Taken together these represent a movement toward consensus on ways to frame some of the key underlying issues and specific plans on future collaboration. We list some of the insights we gained, both technical and strategic, during the deliberations and subsequent interactions.

While dividing the problem into the stages of sensing, reasoning and control initially made sense to everyone, we concluded that effective research projects necessarily involve all three. We should develop frameworks that can effectively interleave and integrate sensing, reasoning and acting to monitor and protect cyber-physical infrastructure. The interactions between the components can support one another. For example, reasoning about initial data from sensors might propose a hypothesis about the underlying situation that could call for additional, active sensing for confirmation. Similarly, a system might decide to perform an action in order to obtain additional data needed to better understand the state of affairs. While architectures that combine these components in a sophisticated way are not new, they are seldom used in large-scale, practical applications.

We concluded that there are two important use cases that call for different approaches: mostly autonomic systems that require little or no human intervention and synergistic human-machine systems that involve significant interactions at multiple levels. It is possible, of course, to look at these as the endpoints of a continuum and to find the most appropriate place on it for a given application. However, we need a better understanding of the two use cases and the techniques they require for design, implementation and use in practical systems.

As our automated and semi-automated systems become more complex, they are prone to fail in unexpected ways. People are able to notice and respond to these system failures just as they can react to their own. Our automated systems, however, are typically oblivious to their shortcomings. We need to endow out systems with a degree of self-awareness about their performance and develop heuristics to allow them to better adapt when it is declining.

An important factor that came across during the workshop was the unanimous recognition of the importance of infrastructure security and the extreme inadequacy of current preparations, as well as the leading role the research community has to play in generating and leading the technical vision to enhance the infrastructure security. Also recognized was the need to expand the workforce with expertise in infrastructure security. Noteworthy is the fact that the participants were bound by a common interest with national boundaries becoming transparent from the very onset of their interactions. Yet there are differences in cultural, political and legal frameworks as well as the differences in available infrastructure that require practical implementations and techniques to adapt to different environments.

Actions and recommendations for the research community

The workshop participants developed some strategies, plans and recommendations for specific actions, some of which have already been put into motion.

Strategically, we believe that a joint Indo-US program offers both benefits and challenges. A key benefit is that it will bring to the surface issues that arise from the global nature of infrastructure security. The significant differences in culture, language, governmental organization and the level of development between India and the US are a good approximation for any that might be faced in the future. Mounting a joint research program will require addressing specific challenges beyond the technical ones, such as the difficulties introduced by distance and the need to coordinate multiple government-sponsored programs.

We recommend that one or more relevant "grand challenge" problems be selected that can motivate and focus research activities. These problems can be used to make the abstract problem of physical infrastructure protection concrete and to help define both a short term and long-term research agenda.

One problem inherent in securing many physical infrastructure systems is that they are composed of many, diverse legacy sub-systems and components. To take electrical power systems in the U.S. as an example, many of these systems are as much as fifty years old. Instrumenting, communicating with and controlling a network of such systems is a challenge. Finding approaches to increasing the interoperability of systems from different technology generations should be addressed.

Closely coupled with this is the development of several concrete use cases that can be used to illustrate the problems and stimulate thinking. We recommend that the research community start by developing use cases for both the "mostly autonomous" and "human in the loop" scenarios.

We identified some immediate potential collaboration opportunities among the group participants, which we list in Appendix 4. We have already begun to explore several of these, as documented in Appendix 5.

We discussed opportunities for exchanging research students between institutions in India and the US. There are some programs that can support students from the US in visiting and studying and working in Indian research laboratories. Similarly, some programs exist in which advanced Indian research students can join a US academic lab for the final year or two of their PhD research. Several of the participants from both countries are exploring these opportunities for their students.

Sajal Das, Krishna Kant and Nan Zhang are editing a handbook with the working title of *"Securing Cyber-Physical Infrastructures: Foundations and Challenges"* that will include chapters from many of the workshop participants. The intended audience of this handbook includes researchers and graduate students working on the broader areas of security in networking (wired, wireless, sensors, etc), grid, clouds and high performance distributed computing, as well as practitioners in the relevant application areas such as smart grids, emergency management. The handbook can also serve as a text for advanced courses and seminars.

We recommend that we begin immediately with several small, organically identified Indo-US collaborations. Several opportunities involving the participants have already been proposed. This can be supported by extending the community of interested researchers, maintaining a common website with a mailing list.

One group of participants led by Dr. Ram Dantu has already assembled a team and is actively working on the human-in-the-loop challenge. It hopes to create a platform soon for sharing, and discussions. They also are planning on organizing a workshop, editing a special issue of a relevant journal and a possibly collaborating on a proposal for research funding. Towards the above objectives, Dr. Dantu gave a presentation on these efforts at the Analysis of Mobile Phone Networks (NetMob[1]) workshop held in May 2010 as part of NetSci 2010 -- The International School and Conference on Network Science.

Ehab Al-Shaer and Krishna Kant are organizing SAFECONFIG 2010[2], the second ACM Workshop on Assurable and Usable Security Configuration. This will be held in Chicago on 4 October 2010 in conjunction with the 17th ACM conference on Computer and Communication Security.

We are planning a follow-on workshop to be held in the United States perhaps late in 2010 that will further explore these topics. This will allow us to engage some researchers unable to attend the meeting in Bangalore.

Recommendations for funding agencies

Creating a joint Indo-US research program in this area has unique challenges but offers great opportunities and potential. There are clearly common concerns yet each country has a unique environment. Problems of terrorism and natural disasters do not respect national boundaries and are increasingly global in their effect. A joint program will allow researchers to address the global problems, test scalability and operate in different and perhaps extreme environments. Managing the heterogeneous types of data in the two countries and different data protection regimes will require flexible and robust approaches. The two countries have different cultures, norms and attitudes but also have different areas of strengths. Just as the problem does not respect national boundaries, the solutions cannot be confined by them either. We suggest some actions that might be taken by funding agencies both in the US (e.g., by NSF) and in India (e.g., by DST).

Building international collaborative research projects is difficult without a dedicated source of funds available to support them. We recommend that the NSF CISE division and perhaps other funding agencies establish

---

[1] http://www.inma.ucl.ac.be/~blondel/netmob/

[2] http://hci.sis.uncc.edu/safeconfig/

programs specifically to support international collaboration involving research, education and engagement around the topic of cyber and physical infrastructure security. The programs can be structured collaborative efforts between research groups in the US and other countries but might identify India as an example where some activities have already begun.

Ideally such programs might be tightly coordinated or at least share a set of overarching goals and common organizational infrastructure for communication and meetings. However, the establishment of appropriate programs should not wait for such coordination – it can evolve once the programs have begun to form.

We recommend that an Indian agency, such as the Department of Science and Technology, also consider establishing a source of funds dedicated to supporting collaborative research efforts in this area.

We believe that the research community will benefit greatly from the development and availability of common research testbeds and datasets. While some isolated examples do exist, it will be especially important for a joint Indo-US program to have testbeds and data that represent both environments. We recommend that funding agencies identify this as an early goal in programs seeking funding.

We also recommend that funding be made available for activities that can sustain and strengthen the collaborations by funding meetings, workshops, scholarly and exchanges.

These initial steps should be followed by large-scale research projects to address key areas, including the following:

- Collection and fusing of information from multiple heterogeneous sources, ranging from low-level signals generated by devices to text and images extracted from social media systems;
- Developing sound technical approaches to integrate systems and components whose design and technology spans many decades of standards and sophistication;
- Extracting and correlating events and developing a global understanding, annotated with information on certainty and data provenance;
- Designing "situation awareness" systems with intuitive human interfaces and visualizations that allow people to quickly and reliably monitor, query and access information about a potential, current or emerging crisis;
- Developing new privacy and security techniques for cloud computing environments that will be used to store and process the massive amounts of information required for infrastructure security;
- Formulating effective options for remedial actions, characterizing their cost, probability of success, and possible side-effects, and making recommendations or decisions based on an appropriate utility model;
- Identifying areas where new standards for instrumentation, measurement and communication can lower the cost and raise the reliability of engineering new systems and adapting old ones; and
- Developing and applying methodologies to evaluate the performance and effectiveness of relevant techniques and systems for monitoring and protecting physical and cyber infrastructure systems.

The programs should leverage expertise and unique contexts (social or otherwise) both in the US and India. We hope that this will initiate a long-term, collaborative effort to uncover and address key research problems in this space.

Acknowledgments

We thank the National Science foundation and the Indo-US Science and Technology Forum for their generous support for the workshop. The Indian Institute of Science, Bangalore graciously hosted the workshop, providing good meeting facilities and lunches. This report is the result of the effort of and contributions from all of the participants.

References

This is a partial collection of references that were mentioned during the workshop, mostly to relevant work done by participants.

R. Radvanovsky and A. McDougall, Critical infrastructure: homeland security and emergency preparedness, (second edition), CRC Press, 2010.

H.M.N.D. Bandara, A. P. Jayasumana and I. Ray, Key Pre-distribution Based Secure Backbone Design for Wireless Sensor Networks, Proceedings of the Third IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseApp), Montreal, Canada, Oct. 2008.

S. Mathew and S. Upadhyaya, Attack Scenario Recognition through Heterogeneous Event Stream Analysis, Proceedings of IEEE MILCOM 2009, Boston, MA, October 2009.

Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, BHIDS: A New Cluster Based Algorithm for Black Hole IDS; Wiley Journal of Security and Communication Networks; to appear, 2010.

P. Sil, R. Chaki and N. Chaki, HIDS: Honesty-rate based collaborative Intrusion Detection System for Mobile Ad-Hoc Networks, Seventh IEEE International Conference on Computer Information Systems and Industrial Management Applications, Ostrava, The Czech Republic, June 2008.

L. Porta, T. H. Illangasekare, P. Loden, Q. Han and A. P. Jayasumana, "Continuous Plume Monitoring Using Wireless Sensors: Proof of Concept in Intermediate Scale Tank," Journal of Environmental Engineering, Volume 135, Issue 9, pp. 831-838, September 2009.

P. Lee, A. P. Jayasumana, S. Doshi and V. Chandrasekar, "Data Fusion Latency in Internet-based Sensor Networks – An Analysis," Proceedings of the 33rd Annual IEEE Conference on Local Computer Networks, Zürich, Switzerland, Oct. 2009.

Q. Han, A. P. Jayasumana, T. Illangasekare and T. Sakaki, "A Wireless Sensor Network Based Closed-Loop System for Subsurface Contaminant Plume Monitoring," Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium, Miami, FL, April, 2008.

Paul Sroufe, Santi Phithakkitnukoon, Ram Dantu and Joao Cangussu, "Email Shape Analysis", CDCN 2010, 11th International Conference on Distributed Computing & Networking, January 3-6, 2010, Kolkata, India.

Prakash Kolan, Ram Dantu, and Joao Cangussu, "Nuisance Level of a Voice Call", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP), Number 1, Volume 5, Article 6, October, 2008.

Huiqui Zhang, and Ram Dantu, "Socioscope: Social Relationship and Behavior Analysis in Mobile Social Networks", Workshop on Analysis of Mobile Social Networks (NETMOB, part of Network Science conference), May, 2010.

Prakash Kolan, Ram Dantu and Joao Cangussu, "Network Risk Management using Attacker Profiling", Journal of Security and Communication Networks (SCN), Volume 2, Issue 1, January/February 2009, pages: 83--96, John Wiley and Sons.

Huiqui Zhang, Ram Dantu,and Joao Cangussu, "Quantifying Reciprocity in Social Networks", Social Mobile Web workshop, held in conjunction with the 2009 IEEE International Conference on Social Computing (SocialCom 2009), vol. 4, pp. 1031-1035, 29th - 31st August 2009, Vancouver, Canada.

Enkh-Amgalan Baatarjav, Ram Dantu, Yan Tang, and Joao Cangussu, "BBN-Based Privacy Management Sytem for Facebook", Proceedings of the 7th IEEE Intelligence and Security Informatics (ISI'2009), Richardson, Texas, June 8-11, pages 194--196, 2009.

Ram Dantu, Joao Cangussu, and Sudeep Patwardhan, "Fast Worm Containment using Feedback Control", IEEE Transactions on Dependable and Secure Computing (TDSC). Number 4, Volume 2, pages 119-136, April-June 2007.

Prakash Kolan, and Ram Dantu, "Socio-Technical Defense Against Voice Spamming," ACM Transactions on Autonomous and Adaptive Systems (TAAS), Vol. 2, No. 1, pp. 1-42, March 2007.

Appendix 1: Participants

Participants from India

Veni Madhavan, Indian Institute of Science, Bangalore, cevm@csa.iisc.ernet.in
Research areas: cryptography, formal methods

Indranil Sengupta, Indian Institute of Technology, Kharagpur, isg@iitkgp.ac.in
Research areas: Cryptography and network security

Joydeb Chattopadhyay, Advanced System Laboratory, kajjoy@yahoo.com
Research areas: real-time embedded systems, sensing

Raja Datta, Indian Institute of Technology Kharagpur, rajadatta@ece.iitkgp.ernet.in
Research areas: wireless ad-hoc networks, computer networking, distributed systems

Nabendu Chaki, University of Calcutta, nabendu@ieee.org
Research areas: wireless and mobile networks, distributed systems

Anupam Joshi, IBM Research -India and UMBC, anupamk.joshi@gmail.com
Research areas: intelligent networked systems, mobile computing, semantic web, social media

Ratnajit Bhattacharya, Indian Institute of Technology Guwahati, ratnajit@iitg.ernet.in
Research areas: wireless communication, communication engineering

S. K. Ghosh, Indian Institute of Technology, Kharagpur, skg@iitkgp.ac.in
Research areas: Network Security, Spatial Database

C. Pandu Rangan, IIT Madras, prangan55@yahoo.com
Research areas: cryptography, secure multi-party computation

K. Gopinath, Indian Institute of Science, Bangalore, gopi@csa.iisc.ernet.in
Research areas: Systems Security

Ponnurangam Kumaraguru, IIIT Delhi, pk@iiit.ac.in
Research areas: security attacks, trust behavior, cross-cultural privacy issues

Dhiraj Sanghi, LNM Institute of Information Technology, Jaipur and IIT Kanpur, dheeraj@lnmiit.ac.in
Research areas: Computer Networks, Protocols, TCP/IP, IPv6, Network Security, Telecom Regulation

Phalguni Gupta, Indian Institute of Technology, Kharagpur, pg@cse.iitk.ac.in
Research areas: Biometrics

N. Balakrishnan, Associate Director of IISc, balki@aero.iisc.ernet.in

Gulshan Rai, Ministry of Communication and Information Technology, grai@eis.ernet.in

Shivkumar Kalyanaraman, IBM Research – India, shivkumar-k@in.ibm.com

Arabinda Mitra, Indo-US Science & Technology Forum, amitra@indousstf.org

Participants from the US

Ehab Al-Shaer, University of North Carolina, Charlotte, ealshaer@uncc.edu
Research areas: formal methods, network scanning, botnet characterization, security metrics

Elisa Bertino, Purdue University, bertino@cerias.purdue.edu
Research areas: security, data mining, policy

Ram Dantu, University of North Texas, rdantu@unt.edu
Research areas: wireless networks, network security, VOIP security

Sajal Das, UT/Arlington, das@cse.uta.edu
Research areas: wireless and sensor networks

Tim Finin, UMBC, finin@cs.umbc.edu
Research areas: semantic web, information extraction, intelligent agents

Atsushi Inoue, Eastern Washington University, atsushi.inoue@ewu.edu
Research areas: distributed network security, knowledge management

Anura Jayasumana, Colorado State University, anura.jayasumana@colostate.edu
Research areas: sensor networks, network protocols, performance modeling

Krishna Kant, Intel Research, krishna.kant@intel.com
Research areas: security and networking

David Kotz, Dartmouth College, david.kotz@dartmouth.edu
Research areas: wireless networks, wireless security, sensor-network security

Sharad Mehrotra, UC Irvine, sharad@ics.uci.edu
Research areas: situation awareness, security, sensor networks, visualization

Nageshwar Rao, Oak Ridge National Lab, raons@ornl.gov
Research areas: information fusion, visualization, sensor networks, distributed computing and networking

Bhavani Thuraisingham, UT/Dallas, Bhavani.Thuraisingham@utdallas.edu
Research areas: security, knowledge management

Shambhu Upadhyaya , SUNY at Buffalo, shambhu@cse.buffalo.edu
Research areas: information assurance, computer security, fault diagnosis, fault tolerant computing

Xindong Wu, University of Vermont/Burlington, xwu@cs.uvm.edu
Research areas: IT Security, data mining

Nan Zhang, George Washington University, nzhang10@gwu.edu
Research areas: information security and privacy, databases and data mining, and distributed systems

Appendix 2: Presentations

Thirty-four individual presentations were made which are listed below. The presentation slides and material for these are available on the Infrasec website (http://infrasec.umbc.edu/).

- Sajal, Krishna, Tim, Bhavani, Veni, Indranil, Introductions and Overview

- N. Balakrishnan, Perspectives on information infrastructure monitoring and security
- Shambhu Upadhyaya, IUSSTF workshop on cyber security, cyber crime, cyber forensics
- Gulshan Rai, Perspectives on certain Government of India national initiatives
- Sajal Das, Emerging Sensing technologies (HW, SW, services, protocols)
- Xindong Wu, Ubiquitous Personalized Information Processing and Services
- David Kotz, Opportunistic sensing using personal mobile devices
- Pandu Rangan, Secure multi-party computation
- Nageshwar Rao, Infrastructure for National-Scale Testbeds for High Performance Networking
- Sharad Mehrotra, Semantics for sensor scheduling for scalable data collection
- Raja Datta, Optimized collaborative techniques for intrusion detection in wireless environment
- Anura Jayasumana, Research approaches to anomaly detection and virtualization
- Anura Jayasumana, Tutorial on distributed sensor/actuator based infrastructure for meteorology, power, healthcare, etc
- Shambhu Upadhyaya, Cyber Attack Scenario Detection and Statistical Signature Generation Through Heterogeneous Event Stream Analysis
- S.K. Ghosh, Security of Enterprise Networks
- Atsushi Inoue, Short tutorial on reasoning with uncertainty
- Ehab Al-Shaer, Reasoning about uncertainty in situation-aware synthesis
- Shivkumar Kalyanaraman, Opportunities for collaboration with IBM research India
- Bhavani Thuraisingham, Adaptive data mining for cyber and national security
- Elisa Bertino, Security policy management: concepts and issues
- Nabendu Chaki, Formal modeling of distributed applications for security management
- Veni Madhavan, Cryptographic and cognitive computations
- Indranil Sengupta, Vulnerabilies and efficient implementations of security primitives
- Nan Zhang, Privacy-preserving data collection/analytics/sharing for infrastructure
- Joydeb Chatterjee, Smart environments
- Phalguni Gupta, Protecting critical infrastructures through multimodal biometrics
- Ram Datu, A new fingerprinting technique
- Nageshwar Rao, Cyber-physical aspects of Infrastructure vulnerabilities and robustness
- Ehab Al-Shaer, Event correlation infrastructure for Large-scale distributed systems
- Anupam Joshi, Short tutorial on policies and policy driven systems for privacy and access control
- Chiranjib, Machine learning, information mining and applications in information security
- Xindong Wu, Integrated, collaborative and distributed security information collection, filtering and fusion
- Sharad Mehrotra: Semantic middleware for pervasive spaces
- Tim Finin, Tutorial on semantic interoperability and linked data

Appendix 3: Agenda

Jan 9: Opening, Applications & Sensing Issues

08:30 – 09:00 Arrival

09:00 – 09:30 Welcome, Introductions and Overview (pdf)

- Sajal, Krishna, Tim, Bhavani, Veni, Indranil

09:30 – 10:30 Perspectives on information infrastructure monitoring and security

- Prof. N. Balakrishnan, Associate Director of IISc

10:30 – 11:00 Objectives, goals and non-goals

- Sajal Das, Krishna Kant, Tim Finin, Bhavani Thuraisingham, Veni Madhavan, Indranil Sengupta

11:00 – 11:15 Coffee Break

11:15 – 12:00 Perspectives on related areas

- Shambhu Upadhyaya, IUSSTF workshop on cyber security, cyber crime, cyber forensics

12:30 – 13:00 Perspectives on certain Government of India national initiatives

- Mr. Gulshan Rai, Ministry of Communication and Information Technology

13:00 – 14:00 Lunch

14:00 – 15:30 Emerging Sensing technologies (HW, SW, services, protocols)

- Sajal Das,
- Xindong Wu: (T) Ubiquitous Personalized Information Processing & Services
- David Kotz: Opportunistic sensing using personal mobile devices

15:30 – 15:45 Coffee Break

15:45 – 17:00 Challenges in data collection, fusion & filtering (scalability, robustness, security, failure tolerance, mobility, etc.)

- Pandurangan, IIT/Madras, Secure multi-party computation
- Nageshwar Rao, (T) Infrastructure for National-Scale Testbeds for High Performance Networking
- Sharad Mehrotra, semantics for sensor scheduling for scalable data collection

17:00 – 17:15 Wrap up

- Quick discussion of the day just ended
- Thoughts for the next day

Jan 10: Reasoning, understanding & control

08:45 – 09:00 Arrival

09:00 – 09:15 Agenda 2.0 discussion

09:15 – 11:00 Presentations (20 minutes each)

- Raja Datta, Optimized collaborative techniques for intrusion detection in wireless environment
- Anura Jayasumana, Research approaches to anomaly detection and virtualization
- Anura Jayasumana, Short tutorial on distributed sensor/actuator based infrastructure for meteorology, power, healthcare, etc.
- Shambhu Upadhyaya, Cyber Attack Scenario Detection and Statistical Signature Generation Through Heterogeneous Event Stream Analysis

11:00 – 11:15 Coffee Break

11:15 – 13:00 Presentations (20 minutes each)

- S.K. Ghosh, Security of Enterprise Networks
- Atsushi Inoue, Short tutorial on reasoning with uncertainty
- Ehab Al-Shaer, Reasoning about uncertainty in situation-aware synthesis
- Shivkumar Kalyanaraman, Opportunities for collaboration with IBM research India

13:00 – 13:30 Lunch

13:30 – 15:30 Breakout sessions

15:30 – 15:45 Coffee Break

15:45 – 17:00 Breakout reports and discussion

17:30 – 20:30 Address by former President of India, Dr. A. P. J. Abdul Kalam

Jan 11: Implementation issues and deep dive breakouts

08:45 – 09:00 Arrival

09:00 – 11:00 Presentations (20 minutes each)

- Bhavani Thuraisingham, Adaptive data mining for cyber and national security
- Elisa Bertino, Security policy management: concepts and issues
- Nabendu Chaki, Formal modeling of distributed applications for security management
- Veni Madhavan, Cryptographic and cognitive computations
- Indranil Sengupta, Vulnerabilities and efficient implementations of security primitives

11:00 – 11:15 Coffee Break

11:15 – 12:30 Presentations (20 minutes each)

- Nan Zhang, Privacy-preserving data collection/analytics/sharing for infrastructure
- Joydeb Chatterjee, Smart environments
- Phalguni Gupta, Protecting critical infrastructures through multimodal biometrics

12:30 – 13:15 Lunch

13:15 – 15:30 Breakout sessions

15:30 – 15:45 Coffee Break

15:45 – 16:45 Breakout sessions

16:45 – 17:15 Brief updates from breakouts

17:15 – optional IISc lab tours

19:00 – 21:00 dinner

Jan 12: Collaboration deep dives (technical, funding, logistics)

08:45 – 09:00 Arrival

09:00 – 11:00 Presentations (20 minutes each)

- Ram Dantu, A new fingerprinting technique
- Nageshwar Rao, Cyber-physical aspects of Infrastructure vulnerabilities and robustness
- Ehab El-Shaer, Event correlation infrastructure for Large-scale distributed systems
- Anupam Joshi, Short tutorial on policies and policy driven systems for privacy and access control

- Chiranjib, Machine learning, information mining & applications in information security

11:00 – 11:15 Coffee Break

11:15 – 12:30 Presentations (20 minutes each)

- Xindong Wu, Integrated, collaborative & distributed security information collection, filtering & fusion
- Sharad Mehrotra: Semantic middleware for pervasive spaces
- Tim Finin, Sort tutorial on semantic interoperability and linked data

12:30 – 13:15 Lunch

13:15 – 15:30 Breakout sessions

15:30 – 15:45 Coffee Break

15:45 – 17:00 Breakout report and integrated collaboration plan

19:30 – 22:00: Conference Banquet (ITC Windsor Manor?)

Jan 13: Straw-man proposal and committed future plans

08:45 – 09:00 Arrival and Coffee

09:00 – 11:00 Develop straw-man joint proposal with clearly defined responsibilities deadlines

11:00 – 11:30 Firm future plan commitments & closing over coffee

11:30 – EOD Social event

Appendix 4: Potential collaborations

A number of opportunities for immediate collaboration were identified. For each we list the set of institutions and the topic(s) of their possible joint research.

IIIT Delhi and SUNY at Buffalo

- Cyber crime data visualization

IIIT Delhi, Vermont, UT Dallas, GWU, University of Calcutta, IIT Kharagpur

- Adaptive data mining for cyber crime
- Inverse resource allocation

IISc, ORNL, UT Arlington and University of North Texas

- Cyber-Physical networks

University of Calcutta, UT Arlington and University of North Texas

- Shape based ISP data analysis for behavioral interpretation

University of Calcutta and CSU

- Large-scale Sensor-Actuator Systems for Monitoring and Protection

UCI, UMBC, UT Dallas, IISc and IIIT Delhi

- Large Scale video data analytics (UC test bed)
- Ontology for describing content, markup language, representation, retrieval query framework

IIIT Delhi, UT Dallas, UCI and GWU

- Human aspects of privacy

University of Calcutta and UCI

- Modeling and analysis of loosely structured data

IIT KGP UT Arlington, GWU and UNT

- Attack graphs
- Game theory models for security

Appendix5: Initial collaborations

Several events visits to discuss initial collaborative research projects projects have already been planned, including the following:

- Nabendu Chaki (U. Calcutta) visited Sajal, Nan Zhang and Krishna Kant on May 3-5, 2010 (UTA, GWU)
- Raja Datta (IIT Kharagpur) visited UTA on May 23-31 and FGW on June 1-6.
- Ehab Al-Shaer and Krishna Kant are organizing SAFECONFIG 2010[3], the second ACM Workshop on Assurable and Usable Security Configuration. This will be held in Chicago on 4 October 2010 in conjunction with the 17th ACM conference on Computer and Communication Security.
- Sajal Das, Krishna Kant and Nan Zhang are editing a handbook with the working title of *"Securing Cyber-Physical Infrastructures: Foundations and Challenges"* that will include chapters from many of the workshop participants. The book is scheduled for completion in the Spring of 2011. The intended audience of this handbook includes researchers and graduate students working on the broader areas of security in networking (wired, wireless, sensors, etc), grid, clouds and high performance distributed computing, as well as practitioners in the relevant application areas such as smart grids, emergency management. The handbook can also serve as a text for advanced courses and seminars.

[3] http://hci.sis.uncc.edu/safeconfig/