Scalable Light-Weight Peer-to-Peer Risk Communication Framework for Critical Infrastructures Management

Titus Okathe, Khalil El-Khatib, Stephen Marsh and Shahram S. Heydari
Faculty of Business and IT
University of Ontario Institute of Technology
Oshawa, Canada
{Titus.okathe, Khalil.el-khatib,Stephen.marsh, shahram.heydari}@uoit.ca

Tim Storer
University of Glasgow
School of Computing Science
Glasgow, Scotland
timothy.storer@glasgow.ac.uk

***Abstract*—Critical infrastructures are growing in scale and complexity and are becoming increasingly interdependent on one-another. This paper argues that existing centralized methods in monitoring and management are unlikely to be sustainable as this trend continues. To address this challenge, this paper presents a complementary model of critical infrastructure monitoring, management and inter-infrastructure communication. The model leverages the advantages of a distributed peer-to-peer method of communication amongst artifacts within infrastructures to provide a scalable, flexible and light-weight means of communication, interaction, and awareness.**

Keywords- critical infrastructures; communication model; interdependence

I. Introduction

Situational awareness has always proven to be extremely important for the management and operation of any system, and especially in the case of critical infrastructures (CI) [1,2,3,4]. To build this situational awareness, operators of CIs collect data from their own systems as well as from other system operators. However, the growing independencies between CIs means that their interactions can be characterized as that of a system-of-systems in which no one entity has overall control or even a global view of the entire system [5]. As a consequence, each infrastructure owner is dependent on peer infrastructures to provide information about the status of facilities or services on which it is dependent for successful operation. These other operators can be from within the same sector, as in the case of the Union for the Co-ordination of Transmission of Electricity (UCTE) or from a different sector, as is the case with the EDXL [6].

Whilst existing frameworks for information exchange can assist with providing situational awareness for CI operators, there are still some problems that can hinder the task of building a more comprehensive picture of situations faced by operators. These include:

1. Data exchange between CI operator is always based on existing collaboration, and does not allow for spontaneous exchange;
2. Data exchange is always carried out at the infrastructure level (between command and control centers), and invariably does not allow individual nodes from one infrastructure to talk to a nodes in different infrastructure;
3. Data exchange still involves a human in the loop, usually the CI operator, to scan through the collected data, who, based on their understanding of the effect of the information on other infrastructures, decides whether or not to pass on the information to other operators;
4. Lack of a simple, common language to express risk or status information[7].

Critical infrastructures are increasing in scale, complexity and interdependence, magnifying these challenges. As a consequence, there is a need to develop flexible, scalable and autonomic mechanisms for exchanging information at appropriate levels of detail in a timely manner across infrastructures. In this paper we propose a risk/status communication framework that abstracts the detailed descriptions of pertinent risks as a *statement of infrastructure artifact comfort.* We explain how this model provides a light-weight means for effectively communicating risks at an appropriate level of abstraction across heterogeneous, legacy infrastructures.

The rest of this paper is organized as follows: Section 2 reviews existing work on inter-infrastructure communication and coordination. Section 3 presents the proposed peer-to-peer model and outlines different models of inter-infrastructure communication that can be adopted for different circumstances. Section 4 evaluates the proposed model and Section 5 draws conclusions and presents the next steps in the research.

II. Background

There is an extensive literature on the modeling, monitoring and management of critical infrastructures [8], protection tools, as well as mechanisms for facilitating effective information exchange [9]. Fundamentally, the purpose of exchanging information among critical infrastructures is to improve their reliability and safety. In light of this there has been research in the area of how to quantify risk; how to represent risk across infrastructures; and the development of suitable information architecture to support these mechanisms amongst heterogeneous systems.

Hu *et al.* [10] and Algirdas *et al.* [11] propose a framework for describing risk by looking at the concepts of dependability and security. The proposed framework combines the attributes of dependability and security and they include: availability, reliability, safety, integrity, maintainability, confidentiality, authenticity, and non-repudiation.

MICIE [12] has the objectives of (1) design of CI modeling techniques which can help in the modeling of the effects of undesired events occurring in a given CI on the Quality of Service (QoS) of its services as well as those of interdependent CIs, (2) design and implementation of an infrastructure for secure cross CI information sharing and mediation, and (3) design and implementation of a MICIE on-line risk prediction tool that encompasses the CI modeling. MICIE also uses a Service Quality Descriptor (SQD) data structure to exchange information between interdependent CI's [13].

Several research groups have investigated techniques for modeling infrastructure interdependencies, highlighting the challenge of presenting dependencies in a uniform manner. Beccuti *et al.* [14] described the CRUTIAL project which employs a Petri-net like approach to modeling systemic effects of individual dependency failures in multiple critical infrastructures. Klein [15] and Klein *et al.* [16] describe the Integrated Risk Reduction of Information-based Infrastructure Systems (IRRIIS) project, which integrates models from a variety of heterogeneous infrastructures in order to analyze their interdependencies. Several other techniques have also been applied to understanding dpendencies in critical infrastructures, such as systems-of-systems modeling [17] and agent based simulations [18].

Several research efforts are underway to facilitate effective and timely information exchange between CIs. The Critical Infrastructure Warning Information Network (CIWIN)[19] is part of the effort by the European Union (EU) to build a secure network for the exchange of critical infrastructure alerts and warnings among EU member states. CIWIN "…offers an efficient and rapid alternative to often time-consuming methods of searching for information, i.e. create a type of "one-stop-system" to obtain all relevant information on Critical infrastructures in the EU"[15]. Additionally, CIWIN "offers the possibility to Member States to communicate directly and upload information that they deem relevant". However, there have been concerns as to the relevance of such a platform given that many of the member states already have Rapid Alert Systems (RAS) of their own which can already perform the functions proposed by the CIWIN [20].

Separately, in [21], Flentge *et al.* present a language for exchanging information across CIs called the "Risk Management Language" (RML). RML is developed around the idea of analyzing CIs using the Implementation-Service-Effect Metamodel (ISE)[22]. RML is an XML based and is therefore extensible. It divides the messages exchange by CIs into three (3) groups:

– Information messages: used to provide information to the service consumer about the possibility of service degradations, as well as any time span and their location.
– Negotiation messages: used by the service provider and the service consumer to exchange and negotiate terms of service delivery.
– Administrative messages: used to control the message exchange.

RML has been tested within the context of the IRRIIS project [23]. Other techniques have also been proposed for extending this work to the autonomic management of interactions between and within infrastructures. Gustavsson and Ståhl described the work on applying self-healing techniques to critical infrastructures in the INTEGRAL project [24]. Hall-May *et al.* [25] and Krrüger *et al.* [26] have separately advocated the use of a service oriented architecture approach to integrating infrastructure management systems.

III. PROPOSED MODEL

This paper proposes a novel approach to critical infrastructure monitoring, management and inter-communication. The proposed model leverages a decentralized agent based, peer-to-peer architecture in which individual artifacts in different critical infrastructures are able to interact directly with others via a variety of communication models. This contrasts with conventional models of critical infrastructure inter-management, in which each entire infrastructure is treated as an agent, service or other computational entity and where communication only occurs between centralized control centers.

In our proposed model, an infrastructure is represented as a collection of agents, with each agent representing some artifact in an infrastructure. For example, consider a fictional modern city comprising many infrastructures such as:

- An electrical power supply infrastructure consisting of electricity consumers, generating facilities, sub-stations, pylons and cabling.
- The water supply consisting of pipes, reservoirs, filtration plants, pumps and water consumers.
- The road network, comprising road lanes, intersections, traffic signals and vehicles.
- The telecommunications network, comprising switches, servers, end-user communication devices, wireless and mobile network base stations and cabling.
- An underground railway network consisting of train sets, rail links and stations.

All of these infrastructures are interdependent on the state of each other. A water pump, for example may depend on power supplied by the electricity infrastructure. On the other hand, a nuclear power station may depend on a ready supply of water to act as a coolant.

In the proposed model, each of the artifacts (road lane, railway station, vehicle and so on) is represented as an agent. Figure 1 illustrates an example of the architecture for three infrastructures: power supply, telecommunications and transportation. Each infrastructure is shown as a circle containing a number of artifacts represented as agents.

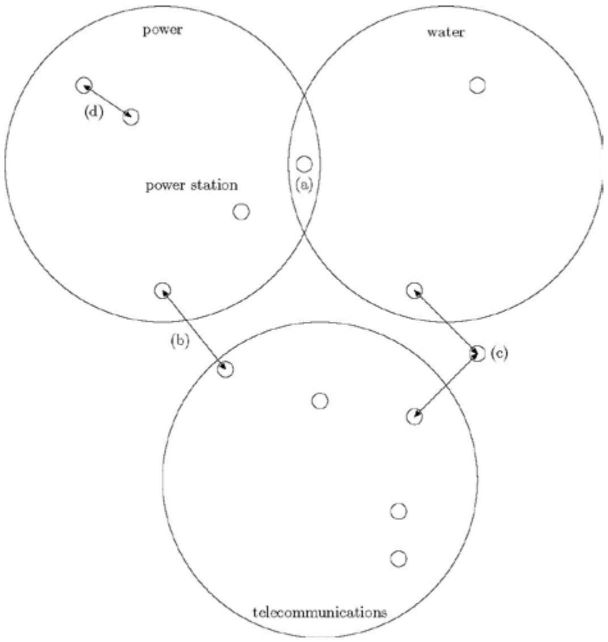

Figure 1. Peer to peer model of inter-infrastructure artifact communication.

We anticipate that agents within the same infrastructure will be able to communicate with each other directly, using a variety of specialized messages and protocols that suit the specific needs of the infrastructure. In particular, we assume that most infrastructures will continue to maintain a centralized control center that will receive status information communicated from infrastructure artifacts, as well as issue commands. However, the arrangement of communication between agents within an infrastructure is an infrastructure dependent issue and not considered further here. Each infrastructure has very different technical characteristics requiring tailored monitoring and management systems. Consequently, we presume that each infrastructure owner will adopt information and communication technologies for infrastructure monitoring, management and internal communication that suits their own needs. This allows each infrastructure owner to continue to use a heterogeneous range of legacy ICTs for infrastructure management as they see fit.

Separately, inter-infrastructure communication is enabled by permitting agents from different infrastructures to also communicate with each other. This allows the communication of information across infrastructure inter-dependencies directly between relevant infrastructure artifacts, rather than via central control centers. For example, a water pump in the water supply infrastructure can be informed of a pending shortfall in the power supply by a nearby power system artifact, giving it time to either reduce the amount of power it requires to operate (by moving to a more efficient but less capable mode, for example) or transition to a safe state for temporary shut-down.

A challenge here is the vast array of infrastructure status information that may be pertinent to a dependent infrastructure artifact. Deciding which information must be communicated and in what format so that it can be understood by a peer infrastructure. This diversity reflects the different physical systems that have to be managed in different infrastructures, and the priorities for measuring different characteristics. For example, water flow rates, reservoir levels and purity may be important characteristics for a water supply infrastructure. However, a nuclear power station may only need to be alerted if the level of water in its coolant reservoir drops below a certain critical minimal level.

As described in Section 2, several research efforts are underway to develop standardized means of communicating this information between infrastructures that may be managed using a heterogeneous range of ICTs; and Genc *et al*. describe the application of a service based publish and subscribe software architecture to the problem of information distribution[27]. However, neither of these approaches addresses the general need to provide a holistic over-view of the status of a critical infrastructure to peers in a flexible and scalable manner.

The model proposed in this paper employs a different approach, by *abstracting* the detailed status information that is specific to a particular infrastructure artifact as an overall sense of *comfort* in infrastructure artifact. The concept of computational comfort has previously been employed in the management of user-personal device interactions in order to provide a more flexible and context adaptable security environment. [28,29,30] In this previous work, a personal device (such as a smartphone or tablet) would continually evaluate its sense of comfort based on a range of factors, such as the user's actions, data accessed, connected services and networks, physical location and time. The device can then adjust its security posture as well as deter less desirable actions based on its overall sense of comfort. For example, a user accessing personal family photographs at home may enhance a device's sense of comfort (because this is a familiar activity). However, performing the same action in a public place or work environment may cause the device comfort level to drop. In this situation, the device would begin to resist (but not prevent) the users action in order to communicate the sense of discomfort as a warning that the actions may be inappropriate.

A range of factors may contribute to the sense of comfort of an agent in a critical infrastructure, depending on the nature of the underlying artifact. Some examples are:

- Flow rates on a reservoir supply pipe.
- Power fluctuations on an electrical line.
- Average vehicle speed on a road link.
- Congestion on a road link, or frequency of traffic signal changes at an intersection.

The computation of an individual infrastructure node's comfort is therefore specific to that node. However, the node (agent) can use the computed sense of comfort to communicate in an abstract manner about potential problems within the infrastructure to dependent artifacts (nodes) in other infrastructures.

The inter-infrastructure agent communication may occur according to several different models of interaction, depending on the relationship between the respective infrastructure owners and the nature of the underlying artifacts. The different models of communication are shown in Figure 1:

- A shared agent, with a presence in both of the communicating infrastructures, labeled (a) in Figure 1. A shared agent receives communications directly from agents in all of the infrastructures it resides in. This arrangement reflects a situation where two infrastructure owners have a significant amount of trust in one another. The agent's level of comfort is computed from the infrastructure specific factors of all the infrastructures it resides in.
- Direct agent to agent communication, labeled (b) in Figure 1. This represents a medium level of trust between two infrastructures. The agents are able to inform each other directly about their current level of comfort. This peering between agents represents a situation where one agent represents an artifact that is dependent on the performance of its peer.
- Communication mediated by an agreed independent third party, labeled (c) in Figure 1. This arrangement represents the lowest level of trust between two infrastructures. The agents in the peer infrastructures' communication is mediated by an agreed independent third party. This may be in order to prevent direct access between agents, for example, to permit anonymous communication of information, or to filter messages. This model is analogous to information security coordination centers that have been established in several jurisdictions for industry specific incident reporting.

The selection of the appropriate form of inter-agent communication is a design decision that will depend on the relationship between infrastructure owners and the nature of the underlying infrastructures. The use of shared agents between infrastructures allows for a closely integrated sense of comfort that allows agents in both infrastructures to respond directly to problems. However, this model assumes a willingness of infrastructure providers to 'share' control of artifacts within their infrastructures and may not be appropriate in all cases. Mediated communication can provide for information that is more limited and anonymous, but can make this information less useful (an agent may not be able to determine which peer is causing the mediator to report discomfort). The middle case provides for a compromise situation in which direct communication of comfort is permitted between certain peer artifacts in an infrastructure.

A final aspect of the proposed model is that agents in one infrastructure may also comprise a number of agents in a critical infrastructure themselves. In this situation, an aggregated agent presents an overall comfort level for the underlying infrastructure. In Figure 1, the power station agent in the power supply infrastructure could be a large complex system, comprising many supporting infrastructure artifacts. However, the overall status of the power station can be abstracted for the purpose of communication to peer artifacts in the power supply infrastructure.

IV. Evaluation of the Proposed Model

In the context of disaster management, Genc *et al*. have argued that the challenges in information distribution in critical infrastructures include **interoperability**, **timeliness**, **security**, **flexibility** and **adaptability**, due to the evolutionary nature of the set of participants [23]. Considering the proposed model against these criteria:

- **Interoperability**: the model imposes minimal new standards on the implementation of CI management systems. Each infrastructure is able to decide for itself which artifacts should be enabled to express comfort levels to peer artifacts. In addition, the computation of comfort levels for a given artifact is left to the infrastructure owner. This leverages the expertise in each infrastructure and minimizes the need for cross-infrastructure communication.
- **Timeliness**: The three models of artifact interaction described in Section 3 provide for real time (type *a* or *b*) or mediated communication (type *c*) as appropriate to the situation between two infrastructures. In addition, the communicated information is abstracted away from the details of the infrastructure, enabling infrastructure artifacts to respond rapidly to changing contextual information.
- **Security**: The different communication models proposed in Figure 1 allow an infrastructure owner to customize their interactions with peer infrastructures based on perceived security risks. Mediated communication can provide a firewall between infrastructures where there is a desire for indirect communication (for anonymity or confidentiality purposes (for example).
- **Flexibility**: The proposed model provides for considerable variation in adoption for infrastructure owners. A system architect is able to select which artifacts in an infrastructure act as agents able to express comfort, as well as selecting which agents they will communicate with in other infrastructures and in what way. In addition, the hierarchical composition of infrastructures allows an
- **Adaptability:** Depending on the situation, the model allows critical infrastructure providers to exchange information with whomever they deem important in the current situation, and without the need for lengthy relationship set-up process.

V. Conclusion and Future Work

We present a new, complementary model for the communication of infrastructure awareness within and between Critical Infrastructures. The model is lightweight, and uses the concept of *comfort*, itself a subjective measure of potential security or risk tolerance, to allow individual artifacts (nodes) within infrastructures, represented by autonomous agents, to make informed, self-aware judgments of ongoing real-time situations.

Currently, the model is abstract and has not been fully implemented, although we have implementations of infrastructure awareness and modeling using Esri's ArcGIS system. It is our intent to take this model and develop it into a working system for Critical Infrastructures, and couple it with our ongoing work in the area of Infrastructure Awareness and Augmentation.

REFERENCES

[1] Commission of the European Communities: Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final, 2006.

[2] European Commission Information Society and Media Directorate-General: Availability and Robustness of Electronic Communications Infrastructures The ARECI Study Final report, March 2007.

[3] J. Yoon, S. Dunlap, J. Butts, M. Rice, and B. Ramsey, "Evaluating the readiness of cyber first responders responsible for critical infrastructure protection," International Journal of Critical Infrastructure Protection, 13 , 2016, pp.19-27.

[4] A. Farouk "Critical Infrastructure Protection in Developing Countries," Handbook of Research on Economic, Financial, and Industrial Impacts on Infrastructure Development. IGI Global, 2017, pp.23-39.

[5] J. Boardman and B. Sauser, "System of Systems: The Meaning of," the IEEE/SMC International Conference on System of Systems Engineering, 2006, pp. 118-123.

[6] M. Raymond, S. Webb, and P.I. Aymond, "Emergency Data Exchange Language (EDXL) Distribution Element," v. 1.0 OASIS Standard EDXL-DE v1.0, 1, May 2006.

[7] Union for the Co-ordination of Transmission of Electricity (UCTE): Final Report, System Disturbance, 2006.

[8] M. Alam and K.A. Shakil, "A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment," Advances in Engineering and Technology Series, Elsevier 7, pp.147-153, 2014.

[9] J. Parajuli and K. E. Haynes. "Transportation Network Analysis in Nepal: A Step toward Critical Infrastructure Protection," 2016.

[10] J. Hu, P. Bertok and Z. Tari, "Taxonomy and Framework for Integrating Dependability and Security," Information Assurance: Dependability and Security in Networked Systems, Elsevier, 2008, pp. 149-170.

[11] A. Aizienis, J. -C Laprie, B. Randell, and C. Landdwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, 2004, pp. 11-33.

[12] S. De Porcellinis, G. Oliva, S. Panzieri, and R. Setola, "A Holistic-Reductionistic Approach for Modeling Interdependencies," Critical Infrastructure Protection III, C. Palmer and S. Shenoi (Eds.), vol. 311, 2009, pp. 215-227, Springer AICT.

[13] M. Aubigny, C. Harped, and M. Castrucci "Risk ontology and service quality descriptor shared among interdependent critical infrastructures," Critical Information Infrastructures Security, Springer, 2011, pp. 157-160.

[14] M. Beccuti, G. Franceschinis, M. Kaâniche, and K. Kanoun, "Multi-level dependability modeling of interdependencies between the Electricity and Information Infrastructures," Int. Workshop on Critical Information Infrastructures Security (CRITIS09), volume 5508 of Springer LNCS, 2008, pp. 48-59, Frascati (Rome), Italy.

[15] R. Klein, "Information Modelling and Simulation in Large Dependent Critical Infrastructures. An Overview on the European Integrated Project IRRIIS," the 3rd International Workshop on Critical Information Infrastructures Security, CRITIS 2008, Rome, Italy, October 2008, LNCS 5508, Springer, Berlin.

[16] R. Klein, E. Rome, C. Beyel, R. Linnemann, W. Reinhardt, and A. Usov, "Information Modelling and Simulation in Large Interdependent Critical Infrastructures in IRRIIS," the 3rd International Workshop on Critical Information Infrastructures Security, CRITIS 2008, Rome, Italy, October 2008, LNCS 5508, Springer, Berlin.

[17] W. Tolone, "Making Sense of Complex Systems Through Integrated Modeling and Simulation," Advances in Information and Intelligent Systems, volume 251 of Studies in Computational Intelligence, Springer, 2009.

[18] E. Casalicchio, E. Galli, and S. Tucci, "Modeling and Simulation of Complex Interdependent Systems: A Federated Agent-Based Approach," CRITIS 2008, pp. 72-83.

[19] Commission of the European Communities, "European Commission," [Online]. Available: http://ec.europa.eu/governance/impact/commission_guidelines/docs/sec_2008_2701_ia_ciwin_en.pdf. [Accessed June 2017].

[20] Commission of the European Communities, "CIWIN," [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF. [Accessed June 2017].

[21] F. Flentge, C. Beyel and E. Rome, "Towards a standardised cross-sector information exchange on present risk factors," Critical Information Infrastructure Security, Springer, 2008, pp. 349-360.

[22] F. Flentge and U. Beyer, "The ISE metamodel for critical infrastructure," Critical Infrastructure Protection, Springer, 2007, pp. 323-326.

[23] R. Klein, "The EU FP6 Integrated Project IRRIIS on Dependent Critical Infrastructures," Critical Information Infrastructures Security, Springer, 2011, pp. 26-42.

[24] R. Gustavsson and B. Ståhl "Self-healing and Resilient Critical Infrastructures," Critical Information Infrastructure Security, Third International Workshop, CRITIS 2008, Rome, Italy.

[25] M. Hall-May and M. Surridge, "Resilient Critical Infrastructure Management Using Service Oriented Architecture," CISIS 2010, The Fourth International Conference on Complex, Intelligent and Software Intensive Systems.

[26] I.H. Krrüger, M. Meisinger, M. Menarini, and S. Pasco, "Rapid Systems of Systems Integration - Combining an Architecture-Centric Approach with Enterprise Service Bus Infrastructure." Proc. IRI'06, IEEE Systems, Man, and Cybernetics Society, Sep. 2006, pp. 51-56.

[27] Z. Genc, F. Heidari, M.A. Oey, S.van Splunter, and F.M.T. Brazier, "Agent-Based Information Infrastructure for Disaster Management." Springer Berlin Heidelberg, 2013, pp.349-355.

[28] S. Marsh, P. Briggs, K. El-Khatib, B. Esfandiari, and J.A. Stewart, "Defining and investigating device comfort." Journal of Information Processing 19, 2011, pp. 231–252.

[29] S. Marsh, S. No¨el, T. Storer, Y. Wang, P., Briggs, L. Robart, J. Stewart, B. Esfandiari, K. El-Khatib, M.V. Bicakci, M.C. Dao, M. Cohen, and D.D. Silva, "Non-standards for trust: Foreground trust and second thoughts for mobile security." Proceedings STM 2011, Springer.

[30] T. Okathe, S.S.Heydari, V. Sood, O. Cole, and El-Khatib K, "Middleware For Heterogeneous Critical Infrastructue Networks Intercommunication," International Journal on Smart Sensing and Intelligent Systems, vol. 9.3, 2016 , pp. 1261-1286.