

# SIMP: A Simple Infrastructure Management Protocol for Infrastructure Monitoring and Management

Guofei Jiang, *Member, IEEE* and George Cybenko, *Fellow, IEEE*

*Abstract - The infrastructure networks of greatest importance to national security and stability include telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government and emergency services. After the September 11, 2001 WTC attack, more sensors and surveillance systems are being deployed to monitor these critical infrastructures. While these efforts are essential for the security of individual infrastructures, there has been little concern about how to share these heterogeneous sensor data in real time among our very large, highly interdependent, complex and dynamic infrastructure networks. Inspired by the popularity of the SNMP in network management, in this paper, we derive and propose a Simple Infrastructure Management Protocol (SIMP) for Critical Infrastructure Monitoring and Management.*

**Index terms - Infrastructure Assurance, Information Sharing, Management Protocol, Distributed System, Monitoring and Management**

## I. INTRODUCTION

According to the PDD63 report of the President's Commission on Critical Infrastructure Protection [1], the infrastructure networks of greatest importance to national security and stability include telecommunications, electrical power systems, gas and oil, banking and finance, transportation, water supply systems, government and emergency services. To effectively protect these critical infrastructures, it will be necessary to have a system in place that can monitor and manage in real time these very large, highly interconnected, complex and dynamic networks. To this end, we propose an Infrastructure Web system to provide such a distributed architecture and framework, as well as the underlying paradigms and information sharing mechanisms by which a problem of this scale and scope can be addressed.

With regard to the nature of the physical infrastructure networks, the ideal Infrastructure Web system for infrastructure monitoring and management should have the following characteristics:

1. It should be decentralized, asynchronous, and redundant;
2. It should be searchable, component-based and self-organizing;
3. It should allow new services to be built easily on top of existing services;
4. It should have an open and extensible framework capable of integrating heterogeneous infrastructure elements;
5. It should have simple interfaces to link infrastructure elements.

After the September 11, 2001 WTC attack, we notice that more sensors and surveillance information systems are being deployed to monitor our critical infrastructures. While these efforts are essential for the security of individual infrastructure elements, there has been little concern about how to share these heterogeneous sensor data in real time among our infrastructure networks. Since critical failures can cascade across various infrastructure networks in a very short time, without real-time information sharing among infrastructure elements, no interdependent infrastructures can be truly safe and no emergency responses can be really efficient. We believe that the research on these issues is of critical importance and social awareness must follow. Otherwise our industry and government may have to invest huge extra resources and efforts to improve the interoperability among these infrastructure protection systems after they have been built.

Inspired by the popularity of SNMP (Simple Network Management Protocol) in network management, in this paper, we derive and propose a Simple Infrastructure Management Protocol for infrastructure monitoring and management. However,

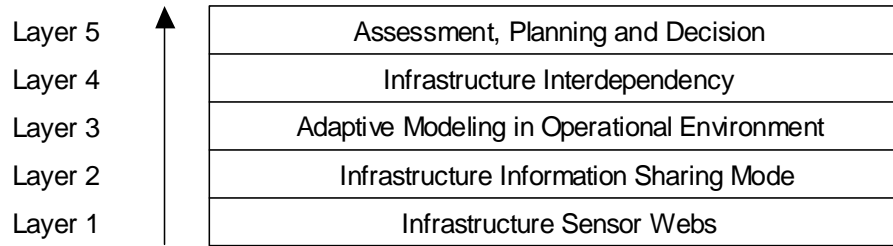


Figure 1: Infrastructure Web Research Work

we don't intend to draft a detailed protocol in this paper, which needs huge extensive work and has to be developed by some organizations like IETF (The Internet Engineering Task Force). Instead, the purpose of this paper is to spark the community to discuss and develop such a protocol for infrastructure assurance.

## II. INFRASTRUCTURE WEB PROJECT

The goal of our Infrastructure Web project is to develop the fundamental architecture and technology that is needed to build a distributed infrastructure monitoring and management networks, i.e. an infrastructure monitoring and management grid. With this grid, infrastructure elements can subscribe and pull real-time information from their dependent infrastructures to monitor their systems; state and local government can gather real-time data from this grid for threat assessments, decision-making and emergency responses.

The complete Infrastructure Web project consists of five layers research work illustrated in Figure 1. For every infrastructure element, a local Sensor Web (a system server) collects, integrates and fuses the real-time data from the distributed and heterogeneous sensors in that infrastructure. The advances in wireless communication such as Bluetooth technology allow low cost, low power and compact sensors to be interconnected easily. On the second layer, information-sharing mechanisms such as SIMP are developed to exchange the sensors data in real time between various infrastructure elements. On the third layer, infrastructure modeling is essential for threat assessments, emergency planning and responses. With the real-time data from the grid, we believe that online adaptive modeling based on daily operational environment is more feasible and useful though some researchers [2][3][4] are modeling infrastructures theoretically. At first, the highly interconnected infrastructures are hard to be modeled theoretically. How strongly one infrastructure depends on another is a case-by-case issue. A Los Angeles model is not going to work well in Boston

since each city has a different infrastructure layout, different infrastructure interconnections and different operational modes. Secondly, the infrastructure model changes over time, even for the same infrastructure. Once the online models of infrastructure elements are available, on the forth layer, the infrastructure interdependencies and network influence models are investigated to prepare any cascading failures. In the end, with these models and real-time data, advanced threat assessment, decision-making and emergency response systems can be developed to protect our critical infrastructure networks.

In September 2000, we designed a prototype of Infrastructure Web as shown in Figure 2. We moved the commercial off-the-shelf (COTS) component technology into the infrastructure assurance field. The Infrastructure Web system consists of four main components: Infrastructure server, Directory service, Sensor web and Query server. An infrastructure server is the information system associated with an infrastructure element, which implements the necessary logic for predicting, detecting and reacting the threats to that infrastructure. Sun Microsystem's JINI lookup service is used as directory services for registration and search of infrastructure elements. The Sensor Web collects real-time data from various sensors inputs and pushes these data to its associated infrastructure server. Query server offers real-time information search for emergency responses. See more details about this prototype in [5] [6].

With this prototype, it's not difficult to implement the necessary functionality for infrastructure assurance. All the infrastructure servers have peer-to-peer relationship and the complex data and event exchanges are implemented on a case-by-case basis. The infrastructure server pulls real-time data from the Sensor Web. Complicated services can be built on the existing services. However, there is no technical standard proposed for the architecture of infrastructure servers and their interfaces with other elements. The success of Infrastructure Web relies on the active participation of infrastructure elements. An

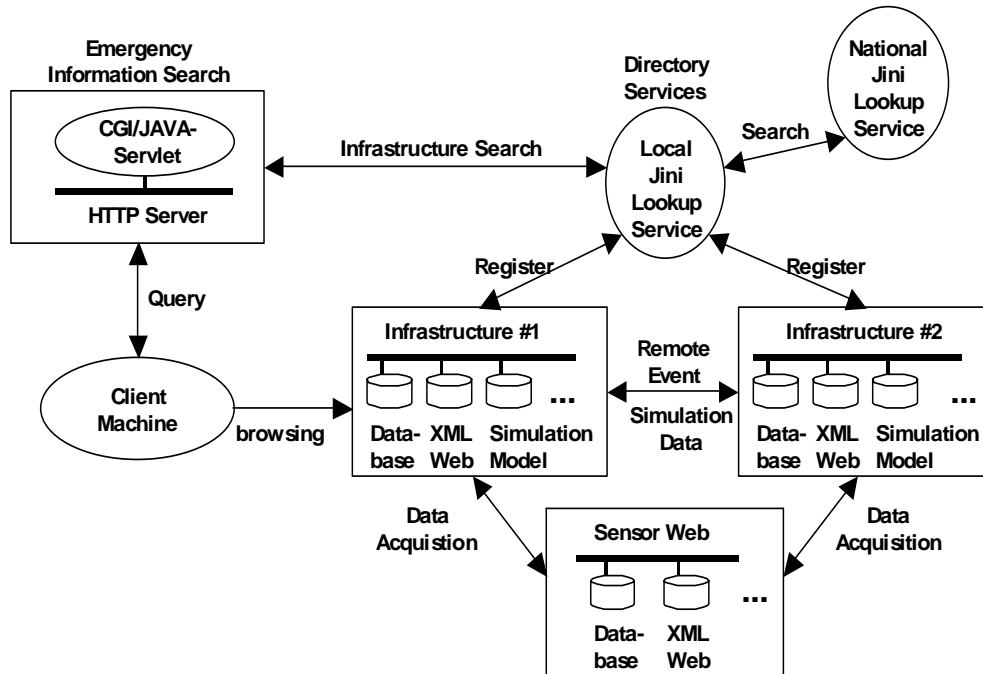


Figure 2: A Prototype of Infrastructure Web

infrastructure server is simply a node in this infrastructure management and monitoring networks. Without a concurred standard for these nodes and their interfaces, Infrastructure Web can hardly survive, grow and scale.

### III. SNMP AND SIMP

With regard to the problem raised in our design, we have to standardize the architecture of infrastructure servers and simplify the interfaces between them. Simple Network Management Protocol (SNMP) is widely used in monitoring and management of network devices such as routers, switches, computers, printers and ups. It suggested itself because of the similarities between device networks and infrastructure networks from network management view. Both infrastructure elements and network devices are distributed network nodes that need to be monitored and managed. Two networks have many similar features while they monitor objects in different domains. Device networks monitor objects such as routing status and network traffic. Instead, infrastructure networks monitor objects such as electricity power voltage in power grid and gas pressure in gas pipe network.

The popularity of SNMP in network management is derived from its simplicity. In fact it only has four

operations – two to retrieve management data from devices, one to set configuration data for devices, and one for a device to send an asynchronous notification. The complexity is really in the management data that SNMP accesses. SNMP mainly consists of three parts: SNMP protocol, Structure of Management Information (SMI) and Management Information Base (MIB). SNMP protocol defines SNMP operations, message format and message exchange between an application and a SNMP agent. SMI specifies a set of rules for naming and defining managed objects. MIB is a structured collection of all the managed objects maintained by a device [7]. By periodically querying the data from the remote SNMP agents, various SNMP applications can be designed to satisfy users' demands.

Based on the similarities between device network management and infrastructure network management, we derive a Simple Infrastructure Management Protocol (SIMP) for monitoring and management of critical infrastructure networks. SIMP keeps the three parts framework of SNMP to maintain the simplicity: SIMP protocol, SIMP Structure of Management Information (SMI) and SIMP Management Information Base (MIB). In the following subsections, we discuss how these parts can be migrated to the Infrastructure Web system for distributed infrastructure assurance.

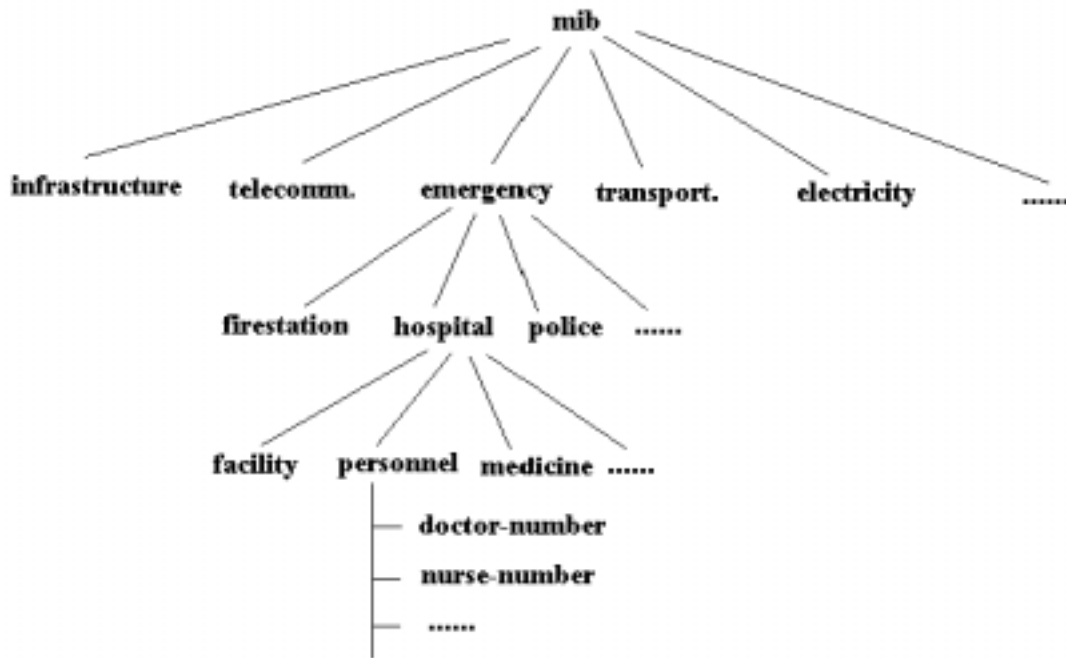


Figure 3: An example of SIMP MIB hierarchy

#### A. SIMP Protocol

Every infrastructure element has a generic SIMP agent hosted on its Infrastructure server. The agent pulls real-time data from the infrastructure element and responds queries to SIMP applications. Usually SIMP applications in this grid are various infrastructure monitoring and management systems. SIMP can keep SNMP's basic operations for simplicity: Get, Get-Next, Set and Trap. Get operation is used by SIMP applications to retrieve real-time data from distributed agents; Set operation is used by infrastructure element itself to configure its own agent; Trap mechanism is used by agents to actively notify the SIMP applications of specific events, which were subscribed by these applications for emergency alerts.

SIMP and SNMP should have big differences in message format and message exchange protocol. A SIMP agent is hosted on an infrastructure server instead of a network device. Since the server usually has much more computing power than the network device, SIMP can use XML (Extensible Markup language) to describe data and advanced application protocols such as SOAP (Simple Object Access Protocol) for message exchange. These standard new technologies can dramatically reduce the complexity of SIMP systems.

#### B. Structure of Management Information

Structure of Management Information (SMI) specifies a set of rules for naming and defining managed objects, which is a sort of toolkit for creating a MIB. All managed objects are arranged in a hierarchical tree structure. The definition of a managed object consists five or more attributes: Object Name, Syntax, Access, Status and Description [7]. Since SIMP is designed to manage objects in thoroughly different domains, SIMP needs new SMI to define names for these new objects and their tree structures. However, SIMP can extend object attributes in SNMP to define its managed objects though more attributes are required to describe the more complex infrastructure objects. While the infrastructure networks need their elements to publish some data for public security, these elements may have to keep some sensitive data private, i.e. some management objects are mandatory to be implemented by every element while some objects may be optional. Meanwhile some management objects may only be accessible to specific users. Access controls to these objects have to be concerned.

#### C. Management Information Base

Management Information Base (MIB) is a structured collection of all the managed objects maintained by a

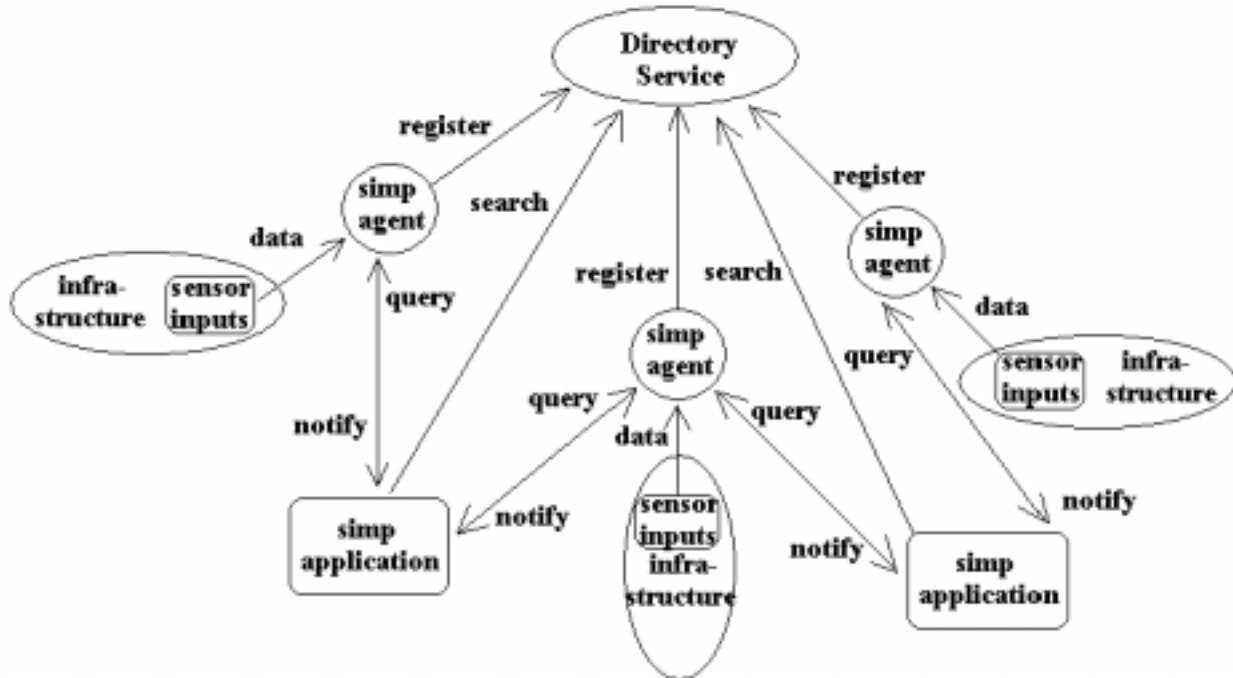


Figure 4: SIMP framework in Infrastructure Web

device. The managed objects are structured in the form of a hierarchical tree. In fact SNMP applications use the tree structure to describe, locate and query the managed objects. As mentioned above, SIMP has to define new MIBs for infrastructure networks. Every category of infrastructures listed in the PDD63 report should have a specific MIB while generic attributes of infrastructure elements can be described in a general MIB. All the managed objects listed in a specific MIB have to be carefully defined and structured by experts from that specific field since they know better about what should be the critical management objects for certain infrastructures. Some professional committees should be organized to define both the SMI and the MIBs. An example of SIMP MIB hierarchy is shown in Figure 3.

#### IV. SIMP IN INFRASTRUCTURE WEB

The SIMP framework in Infrastructure Web mainly consists of four components: SIMP applications, SIMP agents, Directory service and Sensor inputs. SIMP standardizes the information flows in the grid and the management objects of infrastructure elements, and then simplifies the interfaces between these components. We believe that this simplicity and standardization of SIMP is essential for the success to build such an infrastructure monitoring and management network. The SIMP framework in Infrastructure Web is illustrated in Figure 4.

##### A. SIMP Agents

A SIMP agent is hosted on the associated infrastructure server and serves as an interface or a proxy for the individual infrastructure element. It's also the gate between infrastructure networks and the individual infrastructure element. It receives various sensor inputs from its associated infrastructure element and organizes the data based on the standard MIB structure. When applications send queries to the SIMP agent, it responds with the real-time data extracted from its data structure. Like SNMP agents, SIMP agent software should include some basic components for message handling, security and authentication, access controls etc.

With COTS technology such as XML and SOAP, generic SIMP agent software can be designed for all categories of infrastructures. Various infrastructure MIBs can be designed as modules with XML DTD or Schema [8]. SIMP agents can load certain modules based on the system configurations and parse them to specify the management objects. The sensor inputs are fused and mapped to the MIB variables for associated objects, which are saved in an XML-enabled database. Once an agent receives a query, it searches the queried objects in the database and responds the values of those objects. Meanwhile SIMP agents can use XML tagged data to standardize the message exchange with all sensors. Some projects such as DARPA Agent Markup Language (DAML)

[9] have proposed some standard ontology for sensors. In fact sensor data output process is more like a bulk SIMP set operation to update the data in the SIMP agent. SIMP agent can also define a general implementation for trap mechanism, which applications use to subscribe the notification of specific events from agents.

### *B. Sensor Inputs*

The ability to monitor the states of distributed infrastructure elements relies on the sensor inputs. The Sensor Inputs collects information not only from physical hardware sensors and intelligent software sensors, but also from information sources like public records and human observations. After the September 11, 2001 WTC attack, we believe that more surveillance systems will be deployed to counter terrorism. Meanwhile the advances in wireless communication like Bluetooth technology allow low cost, low power and compact sensors to be internetworked easily. Since various sensor data are from heterogeneous and distributed parts of the infrastructure, a Sensor Input needs to include a wrapper software to integrate and fuse the data, map them to standard MIB variables, and pack them with XML tag for message exchange with SIMP agents. The wrapper software is like a translator who translates various “dialects” (sensor data) to “an official language” (XML tagged MIB variables). Since different infrastructures have various sensors, facilities and operation modes, the wrapper software has to be implemented by infrastructure elements on a case-by-case basis.

### *C. Directory Service*

The directory service maintains a directory of available SIMP agents. When Infrastructure Web participants build applications to manage and monitor their interested infrastructures, they can easily search the directory to find the existing SIMP agents. The directory service can just be a simple CGI web page for agents’ registration and search or an advanced system like JINI lookup service. SIMP agents register themselves on the directory service with the associated infrastructure’s attributes such as name, category, location, contact etc. The management objects of an agent are not published on the directory service since they are listed in the standard MIB of that infrastructure category. Meanwhile, since SIMP agents have strict access controls on their managed information, a SIMP application has to contact SIMP agents and subscribe the permissions to access their managed objects.

### *D. SIMP Applications*

SIMP applications pull the real-time data from their subscribed SIMP agents, then analyze, process and display these data based on their users’ needs. Except that SIMP applications have to use the standard protocol and format to communicate with SIMP agents, there is no specific other requirement for SIMP applications. SIMP participants usually have various concerns about the management and monitoring process of their infrastructures. To this end, they have to build their customized SIMP applications. For example, a SIMP application can be as simple as a JAVA applet on a web page to report real-time status of an infrastructure, or it can be as complex as a large-scale monitoring and decision system for the infrastructure networks in a big city. Once a SIMP application needs complex data processing such as data mining and hypothesis verification, the development of this application has to use some very specific expertise and domain knowledge.

However, general SIMP application software suites, like HP Openview, can be developed for infrastructure management. For example, a general infrastructure management software can be developed over the related geographical information system (GIS) to view the status of various infrastructure elements and their connections. By pulling infrastructure icons, a local infrastructure monitoring system can be built in minutes. Different icons represent different category of infrastructures. The SIMP framework standardizes the MIBs of infrastructures and the communication between applications and agents. Thus the field operators can search their concerned infrastructures from the directory service, pull the related icons to the GUI-based software platform, and input their concerned managed object’s names to build their customized monitoring systems. The software can get all other work done automatically to pull the data from agents and display them.

## V. RELATED WORK

There are a lot of government reports that address the policy and technology demanded for critical infrastructure assurance. The director of DoE’s Critical Infrastructure Protection Office, Ms. Paula Scilingi, urged to build a similar system for operational information sharing in a CNN interview (Oct. 21, 2001). To the best of our knowledge, we haven’t observed any work proposed to develop a standard protocol for infrastructure management and build an infrastructure management network.

However, there is some related work in the infrastructure assurance research and the information grid research.

Knight, McHugh and Sullivan [10] at the University of Virginia have a research group working on information survivability for critical infrastructure protection. They focus on the survivability mechanism, survivability measurement, fault tolerance and error recovery of single system model. Sandia National Laboratories also has a Critical Infrastructure Surety (CSI) group [11] working on consequence-based analysis, energy infrastructure assurance and interdependencies simulation with their supercomputer. Argonne National Laboratories has an Infrastructure Assurance Center (IAC) [12] working on dozens of research subjects relating to Infrastructure Assurance. EPRI/DoD's Complex Interactive Networks/System Initiative (CIN/SI) is a 5-year, \$30 million program. Six consortia, consisting of 28 universities, are focusing on advancing basic knowledge and developing breakthrough concepts in modeling and simulation; measurement, sensing, and visualization; control systems; and operations and management [13][14].

For the information grids research, while commercial companies are making enterprise-scale component framework available on the market such as Microsoft's DCOM and Sun's EJB, several large-scale grids projects are under the way for distributed computing such as Globus [15], the Air Force's Joint Battlespace Infosphere (JBI) [16], Infosphere [17] and CoABS [18]. While these grids projects are developing the complex fundamental technology that is needed to build grids for distributed computing, the Infrastructure Web project intends to develop feasible technology to protect large-scale infrastructure networks and use them for infrastructure monitoring in real time.

## VI. CONCLUSIONS

To effectively protect critical infrastructure networks, a new approach of integrating, coordinating and managing infrastructure protection must be deployed. To this end, we proposed a distributed Infrastructure Web system to monitor and manage these infrastructure networks. Without a standard, the infrastructure elements in the networks can hardly exchange heterogeneous data in real-time to protect the highly interdependent networks, especially when some critical failures can cascade across the network in a very short time. Inspired by the popularity of SNMP in network management, this paper proposed a Simple Infrastructure Management Protocol (SIMP)

for critical infrastructure management and monitoring. We believe that the simplicity and standardization of SIMP framework is essential for the success to build a national infrastructure protection network.

## Acknowledgements

This work was supported under Award number 2000-DT-CX-K001 (S-1) from the Office of Justice Programs, National Institute of Justice, Department of Justice. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Justice.

## VII. REFERENCES

- [1] The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. See [http://www.ciao.gov/CIAO\\_Document\\_Library/paper598.htm](http://www.ciao.gov/CIAO_Document_Library/paper598.htm)
- [2] C. Chen, Z. Jiang and P. Varaiya, "Causes and Cures of Highway Congestion", IEEE Control System Magazine, vol.20, no.6, 2001.
- [3] C. DeMarco, "A Phase Transition Model for Cascading Network Failure", IEEE Control System Magazine, vol.20, no.6, 2001.
- [4] C. Asavathiratham, S. Roy, B. Lesieutre and G. Verghese, "The Influence Model", IEEE Control System Magazine, vol.20, no.6, 2001.
- [5] G. Cybenko and G. Jiang, "Developing a Distributed System for Infrastructure Protection", IEEE IT professional, vol.2, no.4, July/August, 2000.
- [6] G. Jiang, G. Cybenko and D. McGrath, "Infrastructure Web: Distributed Monitoring and Managing Critical Infrastructures", Proceedings of SPIE conference on Enabling Technologies for Law Enforcement and Security, November, Boston, 2000.
- [7] D. Zeltserman, "A Practical Guide to SNMP v3 and Network Management", Prentice Hall, 1999.
- [8] E.R. Harold, "XML Bible", IDG Books Worldwide, 1999.
- [9] DARPA Agent Markup Language Program, see <http://www.daml.org/>.
- [10] <http://www.cs.virginia.edu/~survive>

[11] <http://www.sandia.gov/CIS/>

[12] <http://iac.anl.gov/>

[13] M. Amin, "EPRI/DoD Complex Interactive Networks/Systems Initiative: Self-Healing Infrastructures", Proceedings of the 2<sup>nd</sup> DARPA-JFACC Symposium on Advances in Enterprise Control, Minneapolis, MN, July 10-11, 2000.

[14] M. Amin, "Toward Self-Healing Energy Infrastructure Systems", IEEE Computer Applications in Power, vol. 14, no. 1, January 2001.

[15] <http://www.globus.org/>

[16] <http://spock.deepthought.rl.af.mil/programs/jbi/>

[17]. <http://www.infospheres.caltech.edu/>

[18]. <http://coabs.globalinfotek.com/>