Adaptive Information Infrastructures for the e-Society

Mihaela Ulieru

Electrical and Computer Engineering Department
The University of Calgary
2500 University Dr. NW
Calgary, Alberta, T1N 1N4 Canada
ulieru@ucalgary.ca
http://www.enel.ucalgary.ca/People/Ulieru/

Abstract. Positioned at the confluence between human/machine and hardware/software integration and backed by a solid proof of concept realized through several scenarios encompassing e-Securities, e-Health, and e-Logistics for global manufacturing and emergency response management, this work exploits latest advances in information and networking technologies to set a systematic framework for the design of the information infrastructures (coined as AIIs - Adaptive Information Infrastructures) destined to fuel tomorrow's e-Society. Designed following the natural laws of evolution, which merge self-organization and natural selection [38], these socially embedded information infrastructures can adapt to fulfill various needs as their environment demands. Computational intelligence techniques endow the AIIs with learning and discovery capabilities, emulating social and biological behavior. AIIs are destined to become an integral part of our life by supporting, rather than disturbing, a framework that facilitates strategic partnerships while providing greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions.

Keywords. distributed artificial intelligence, information infrastructures, emergency response management, e-Health, Cybersecurities, emergence, self-organization, evolution

1 Rationale

Today's electronic information technologies are linking our world, enabling partnerships otherwise impossible in all areas of our life. From e-Commerce and e-Business to e-Learning and e-Health the economic strategies as well as the routine professional practices have been irreversibly contaminated with the spice of electronic connectivity. Supported by this technological leverage, new paradigms have emerged with models that are dynamic, autonomous, self-organizing and proactive, generically coined as 'intelligent'. In particular Multi-Agent Systems (MAS) have changed the software world, and with it the world of information technologies. With the reasoning encapsulated in *societies of software agents*, having a life of their own in Cyberspace, the Internet becomes a *dynamic environment* through which agents move from place to place to deliver their services and eventually to compose them with the ones of

other agents, just like people cooperate, by exchanging services and/or putting together their competencies in a larger, more complex service.

With this the dawn of the e-Economy is already upon us and as direct consequence the e-Society emerges as a parallel world of information, where people 'cloned' as agents are 'living' in a virtual universe, emulating our games in all aspects of life, be they economic, financial, business, school or health related, or even just-for-fun, in computer games. Paradigm shifts abound in our world, shaping our lives more and more dramatically. Building on the power of distributed intelligence on the web they swing the driving forces of our economy from competition to cooperation, from individualism to strategic partnering, from power-from-information to authority-from-wisdom, from fear to trust (and, sometimes, vice versa). To secure our future we need to act quickly to take these developments in a safe direction that guarantees the hidden dangers of these technologies are superceded by its positive effects meant to improve our lives. All the right questions spanning ethical and societal concerns have to be posed before our lives immerse into such e-systems to ensure a safe environment is created.

In today's dramatic context there is an acute need for such new techniques capable to deal with critical aspects such as emergency response management, network, information and national security enhancement, population health and quality of life improvement, etc. In spite of the tremendous progress made by researchers to enable the electronic communication space (be it networked or wireless) to become a Dynamic Service Environment[1] (DSE) supporting all aspects of life, from business and commerce to education and health, society is stagnant, still using the old ways while these tremendous IT advances are not applied. Elderly and remotely located people without possibility of transportation still live in isolation. New threats test us continuously calling for new ways to cope with emergency and crisis situations and for tools that are more dynamic, anticipative and adaptive in real-time. To build more immunity for our world in coping with unexpected disasters (be they natural, such as earthquakes, floods, hurricanes or man-made ones such as oil spills in the ocean, terrorist attacks, etc.) and more recently health emergencies posed by highly contagious diseases (bird flu, SARS, mad cow, etc.) it is of the essence to unleash the power of IT. In such crisis situations there is a high need to react quickly in a reasonable, efficient way to restore the effects of the crisis.

To meet this need we propose a systematic approach to the design and implementation of such dynamic environments supporting coalition formation, which we refer to as *adaptive information infrastructures* (AII). AIIs could glue together the best organizations capable to cooperate in the timely solving of a crisis, and support the coordination of activities across such an extended cooperative organization, getting clarity to emerge from the fog of information and help make the best decisions out of the crisis chaos.

[1] www.agentcities.org (The Global Agentcities Task Force has the mandate to bring together forces from all continents in a common effort to develop the dynamic infrastructures of tomorrow's 'alive'-Web.)

2 State of the art in the design of adaptive information infrastructures

Future information systems will use ambient intelligence to create collaborative ecosystems of stationary and mobile devices, such as mobile phones, PDAs, personal mobile gateways, portable players and personal storage devices [1]. These ecosystems will form an environment that supports complex interactions between distributed systems. Multi-agent technology is an excellent candidate for realizing such an environment, but requires the development of methods and technologies for its control, maintenance and evolution. Organization is crucial to this dynamic environment because groups of agents need to communicate with each other and self-organize to meet their objectives.

As information systems become more complex, it is increasingly difficult to manage them using traditional approaches based on centralized and pre-defined control mechanisms. The dynamic configuration of loosely combined artifacts and services puts new requirements on middleware and frameworks, which need to be more adaptive and responsive in real time. One example of a new architectural approach is open resource coalition as a shared infrastructure that automates configuration decisions given a specification of the user's task [2]. They use (like most approaches [3], [4]) analytical models to make near-optimal configuration decisions.

As open-resource coalitions, shared infrastructures are:

- *pervasive/ambient*, available everywhere as an integral part of the environment;
- *intelligent*, in the sense that people will react and respond to AIIs as they would to a human being;
- *adaptive*, with their behavior changing in response to actions in the environment; and
- *anticipatory*, meaning they can anticipate an attack without conscious mediation.

Given their characteristics, AIIs call for a complex approach to their design. Recently, models from biology, the physical world, chemistry and social systems have inspired scholars to seek ways to more efficiently manage complex information ecosystems [5]. However, even the most sophisticated approaches [6] do not consider the ecosystem's interaction with other systems, which would induce evolution through selection.

To influence the development of this technology in a human-friendly way our approach builds on the natural laws/patterns of self-organization according to which adaptive / intelligent systems emerged in the process of universes' evolution [7].

3 Approach

Our approach [8] addresses this by enabling information infrastructures for various applications. For example, for global production integration [9], we developed a methodology for dynamic resource management and allocation across distributed (manufacturing) organizations [10], [11]. The approach integrates multi-agent technology with the *holonic* paradigm proposed by A. Koestler in his attempt to create a model for self-organization in biological systems [12]. A holonic organization is cre-

ated (see Fig. 1, [13]) as a nested hierarchy, referred to as *holarchy*, of collaborative entities (e.g. resources, people, departments, sections or enterprises) linked through an information infrastructure that defines several levels of resolution [14]. Each entity is a *holon* and is modeled by a software agent [9] with *holonic* properties—that is, the software agent may be composed of other agents behaving in a similar way, but performing different functions at lower levels of resolution.

The flow of information and matter across a holonic organization defines several levels of granularity (Fig. 1) across which we integrate the mechanism of emergence to enable the dynamic creation, refinement and optimization of flexible ad-hoc AIIs as coordination backbones for the distributed organization, capable to bring together the best resources available (within reach) depending on the needs of the particular crisis to be addressed.

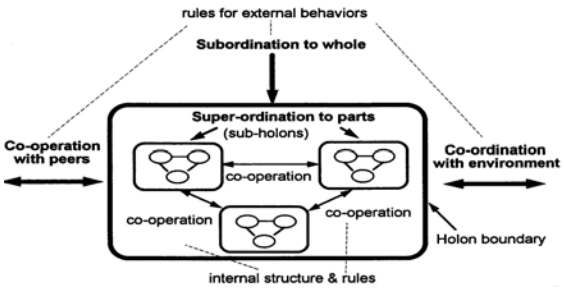


Fig. 1. Holonic Enterprise Model (from [13])

Emergence involves self-organization of the systems and natural selection through interaction with other systems. We integrate emergence into the holonic paradigm [15] to create, refine and optimize AIIs. Self-organization is achieved by minimizing the entropy measuring the fuzzy information spread across the multi-agent system [10]. This will cluster the resources (agents), ensuring interaction between the system's parts to reach its objectives timely, efficiently and effectively. Evolution is enabled by interaction with external systems (agents); for example, via a genetic search in cyberspace that mimics mating with most fit partners in natural evolution [16] or by means of dynamic discovery services [17].

Embedding and intelligence are essential in our vision. Besides the physical embedding facilitated by miniaturizing and by reducing technology costs, as socially embedded information infrastructure AIIs are destined to become an integral part of our life by supporting, rather than disturbing, a framework that facilitates strategic partnerships among 'cyber-highway enabled' participants while providing greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions. Intelligence can range from context-awareness, to more personalized and adaptive systems. In this vision, people will be immersed in such intelligent and intuitive infrastructures embedded in everyday objects in an environment recognizing and responding to the presence and needs of individuals in a seamless way.

4 Our Previous Results in the implementation of AIIs

4.1 AIIs for global manufacturing

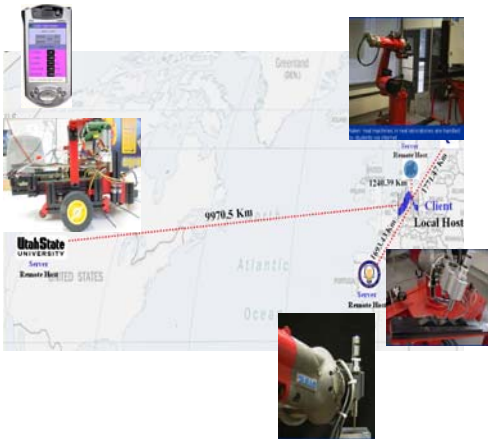


Fig. 2. Global Manufacturing Holarchy

Our work with the Holonic Manufacturing Systems (HMS) consortium demonstrated that this methodology is very useful for global supply chain management systems that integrate collaborative workflow techniques [18]. Within this context AIIs can be viewed as information ecosystems composed of collaborative but autonomous holons Fig. 2 working e.g. to create a new product by merging several specialized companies and coordinating their efforts, Fig. 3 (from [18]).

The interaction between distributed enterprises, with their suppliers and customers is modeled at the multi-enterprise level. The enterprise level hosts co-operation between entities belonging to one organization, the sales offices and the production sites. The distributed manufacturing control within a production site or shop floor is handled by the shop floor level. Here the entities are distributed work areas working together and in co-operation, in order to fulfill all orders allocated to them. The basic level (the Cell) models the interactions between equipments and humans. In [18] we focused on a supply chain scenario from the phone manufacturing industry.

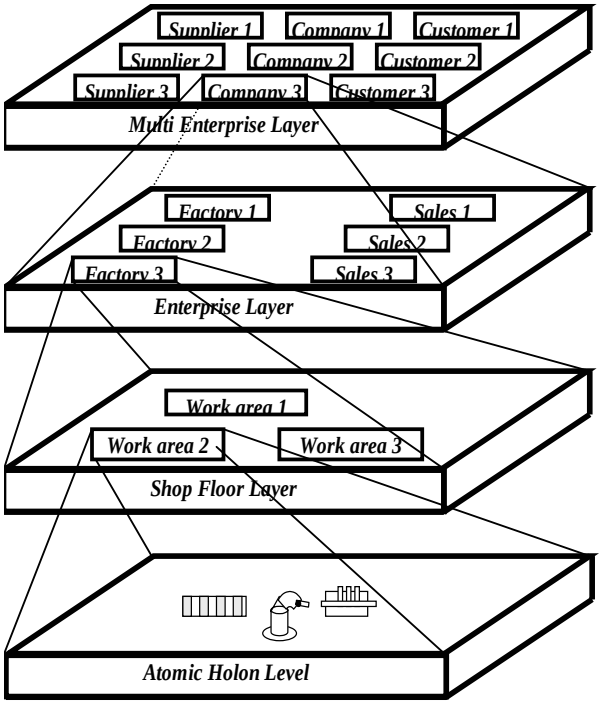


Fig. 3. Layers in Holonic Manufacturing

This approach can easily be expanded to any goods distribution networks (e.g. the Wal-Mart supply chain).

4.2 Challenges in implementing AIIs for global manufacturing

The main challenges to be faced here pertain to the vertical integration between levels, where different ontologies have to communicate.

- The main barriers at the real-time control level result from the difficulty of implementing MAS concepts in a stochastic environment where hard real-time constraints must be met to achieve safe system operation.
- Need for optimal clustering (i.e. always group the best partners) – requires on-line reconfiguration of the collaborative cluster to respond to changes in market demands as well as to the needs for maintaining optimal configuration.
- Need to balance the autonomy of each individual partner with the cooperative demands of the collaborative cluster – through negotiation that can range from simple bidding (proposal and counter-proposal) to complex argumentation and persuasion strategies. An example of the latest: the cluster sets a deadline and requirements to coordinate among the partners while partners need to argue their position and integrate the deadline with their other priorities). The cluster sets the 'rules of the game' through component protocols. Preferences can be captured via a utility function such that clustering best partners can be achieved via cost minimization.
- Need for safety. To achieve a safe system, typically two general concepts are used. First, safety channels (i.e., fault monitoring and recovery code) are separated from non-safety channels (i.e., control code). This decomposition technique is typically referred to as the "firewall concept". Second, redundancy is applied in the system in the form of homogeneous redundancy where clones or exact replicas of code are used (only to protect against random failures), or in the form of diverse redundancy where different means are used to perform the same function (this protects against random and systematic failures).
- Need to manage timing and precedence relationships while executing the distributed functions and tasks.
- Need for the system to be capable of arranging for compiling of the code into low-level application code and distributing of this application code to appropriate resources for execution.
- Need to enable the user to develop an application using basic and composite function blocks and application prototypes (templates) from a library.
- Need for monitoring and fault recovery. The purpose of monitoring is to ensure that the control system performs as intended, or in other words, that no latent faults occur. When monitoring for faults, the control system should watch for failures (events occurring at specific times), and errors (inherent characteristics of the system). The types of responsibilities that our control system will have in this area are: diagnosis of program execution, monitoring for exceptions that are thrown by function block code during execution, and monitoring the system state for inconsistencies (e.g., deadline control).

4.3 AIIs for Emergency Response Management

More recently, we successfully took the holonic concept out of the factory environment by designing a holonic framework suitable for emergency response applications [19]. For this testbed the actors are either a policeman with a PDA, a firefighter with a cell phone or even a helicopter sending real-time information about the traffic jams to our planner holon. For example, it can indicate an optimal or improved route for emergency vehicles to follow or even more, it will be able to instruct the policemen to clear a road so the firefighters will be able to arrive to the building faster. In case of a bigger disaster our system will be able to contact the hospitals in the zone and start distributing the patients according to bed availability. The emergency AII is depicted in Fig. 4 with three nested levels:

Inter-Enterprise Level: This is the level on which the emergency AII is formed. Each collaborative partner is modeled as an agent that encapsulates those abstractions relevant to the particular cooperation. The "Emergency Mediator" handles the communication process between them. This will require the development of ontologies that will handle the different kind of information exchange and also will allow the system to be expanded.

Intra-Enterprise Level: Before an enterprise/organization can undertake responsibility for some subtask, it has to find out about its own internal resources to ensure that it can deliver on time according to the coordination requirements of the ad-hoc created collaborative cluster.

Atomic Autonomous Systems or Machine Level: The lowest level is the atomic autonomous systems or device/resource level, concerned with the control and coordination of distributed resources performing the work.

Planning and dynamic scheduling of resources on all levels of the emergency holarchy enable functional reconfiguration and flexibility via (re)selecting functional units, (re)assigning their locations, and (re)defining their interconnections (e.g., rerouting around a fire crew, changing the functions of a multi-functional defense unit, reallocating hospital beds to cope with the victims of the crisis, etc.).

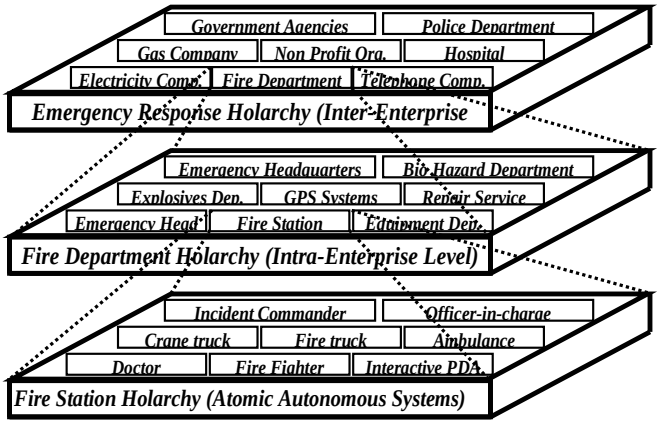


Fig. 4. Emergency Response Holarchy (AII)

As emergent dynamic information infrastructures that are autonomous and proactive, AIIs can ensure ubiquitous (optimal) resource discovery and allocation while at the same time self-organizing their resources to optimally accomplish the desired objectives. This is achieved through dynamic virtual clustering mechanisms acting on each resource within the enterprise, cloned as an agent that abstracts those functional characteristics relevant to the specific task assigned by the collaborative conglomerate to each unit. Once a crisis arises an AII emerges clustering available resources (modeled as software agents) to deal with the situation optimally.

4.4 Challenges in Implementing AIIs for Emergency Logistics

- To find an optimal cluster is NP-hard. By exploiting heuristics/experiences we aim to overcome the limitations of existing approaches, especially regarding the timely response constraint required by emergency.
- In emergency logistics, where the scope of possible organizations/tasks/skills is not restricted and/or predefined, it is difficult to express and code enough real world semantics to permit a goal-driven and effective communication between levels. Another crucial issue: to incorporate solid trust and reputation mechanisms in agents (e.g. institutionalized power).
- In such dynamic, intrusive environments organizations need to be protected by strong security mechanisms, exceeding today's web-service deployment standards. We will continue work with the FIPA 'Securities' Technical Committee on this issue. A possible solution is *the electronic institution* - a normative framework which emulates regulatory mechanisms in real life social institutions. Such institutions define and police norms that guide individual agents collaborating through AIIs. These norms set acceptable actions that each agent can perform in connection to the role(s) it plays and clearly specifies access restrictions on data according to these roles.

5 New Applications of AIIs

5.1 Scalable Secure Web Based Services for e-Health

We propose a holonic framework suitable for e-health applications. In [20] we defined the concept of medical holarchy as an open evolutionary health system that is highly self-organized and self-adaptive. The collaborative medical entities (patients, physicians, medical devices, etc.) that work together to provide a needed medical service for the benefit of the patient, Fig. 5 – form a medical holarchy. The levels of a medical AII are (Fig. 6):

- ***Inter-Enterprise***: Hospitals, Pharmacies, Medical Clinics/Laboratories
- ***Intra-Enterprise***: Sections/Units/ Departments of each medical enterprise
- ***Resource Level***: Machines for medical tests, medical monitoring devices, information processing resources

In this system of collaborative medical entities new devices and services (Fig. 5) can integrate themselves, offer their functionality to others and share data on a secure level. The complex interaction of diagnosis, treatment and monitoring is made possible through task planners and schedulers that are distributed, automatic and self-configuring.

Fig. 5. Medical AII

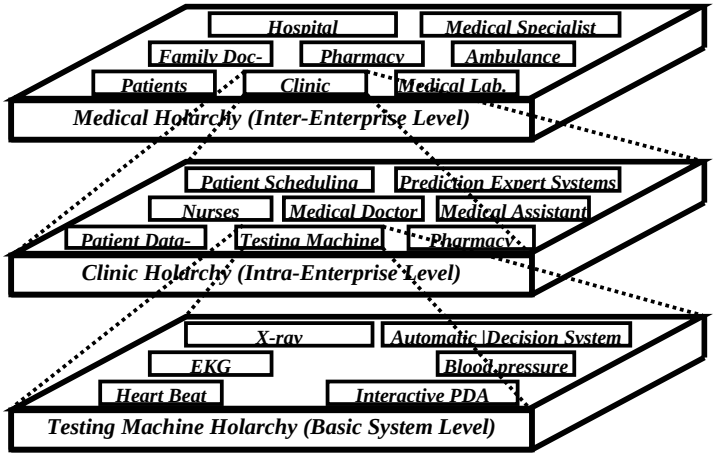


Fig. 6. Medical Holarchy (AII)

A major issue in e-Health technology adoption is reconciliation of the various standards of care across the continents. As well the security and privacy of electronic medical records is of major significance and has proven to be the major brake that slowed down the adoption of e-Health by major clinics around the world but especially in the North Americas. Therefore our goal is to develop a reusable framework for secure high-performance web-services in e-health. As a testbed for the secure AII to be developed we will use it to connect a network of medical experts that will collaborate via the AII to develop standards of care for glaucoma [24]. To enable the collaboration of highly specialized glaucoma surgeons located across the country we have developed a telehealth approach [21] that involves a consensus analyzer synthesizing expert opinions into standards of care [22].

Recently we successfully applied this concept to improve glaucoma monitoring [23] with a security layer. This has encouraged us to expand the holonic concept to other e-Health areas that require the dynamic creation of organizational structures and workflow coordination, such as rescuing people after an accident or disaster. This is a

time critical operation that requires quick diagnosis, identification of the closest available hospital and knowledge of traffic conditions.

During an AII-enabled rescue operation, novel e-Health technologies can be used, e.g. using biometric technologies [36] for patient authentication by a wireless fingerprint sensor that accesses their profile from a remote database. Depending on indicators such as blood pressure and the health history of the patient, a first diagnosis is compiled using automated decision support systems [25]. Electronic logistics support provides information about the next available and suitable hospital, initiate staff assembly and emergency room preparation, and provide on-the-fly patient check-in.

5.2 Challenges in Implementing e-Health AIIs

The main challenges to be addressed in the implementation of medical holarchies are:

- Need for development, dissemination and utilization of common communication standards, vocabularies and ontologies. Unfortunately there is not much work in this direction and we will intensify our influence in creation of appropriate e-Health ontologies by working with the standard bodies focused on e-Health. The EU's CEN/TC 251 aim is to achieve compatibility and interoperability between independent systems, to support clinical and administrative procedures, technical methods to support interoperable systems as well as requirements regarding safety, security and quality. The US standardization bodies, the American Society for Testing and Materials' Committee on Healthcare Informatics (ASTM E31) [26] and Health Level Seven [27] are involved in similar work. ASTM E31 is developing standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of information while HL7 is mainly concerned with protocol specifications for application level communications among health data acquisition, processing, and handling systems. Existing ontologies are being developed to meet different needs, each with its own representation of the world, suitable to the purpose it has been developed for. There is as yet no common ontology. Of those that are being developed, OpenGALEN [28] provides a common terminology that is currently of limited scope, while UMLS [29] lacks a strong organizational structure, and SNOMED [30] provides only diagnosis nomenclature and codification.
- Besides the social acceptance of medical holarchies, professional acceptance – that is by the medical doctors is a major issue. We hope that our scenarios will increase the confidence of medical personnel in such technologies by proving their usefulness. Health care professionals are quite reluctant to accept and use new technologies. In the first place, they usually have a very busy schedule, so they lack the time to be aware of the latest advances in technologies and how they could be used to reduce their workload. They refuse to use new tools if they are not integrated smoothly into their daily workflow. They also often mention the lack of time and personnel to convert all the required medical data into an electronic format, so that it can be easily accessed and managed[2]. Some doctors also mention the "hype"

[2] Medical records are usually hand written and distributed in different departments of a medical centre.

built around Artificial Intelligence and, especially, expert systems, twenty years ago, which did not live up to their expectations, and they may reasonably argue that the "intelligent autonomous agent" paradigm, so fashionable today, may also fail to deliver real world results.

We will address these challenges when developing the medical AIIs as a primary response to the needs and requirements of today's healthcare system, especially to the need for ubiquitous access to healthcare services and ease of workflow management throughout the medical system.

5.3 Holonic Cybersecurity System

Information infrastructures are critical to the functioning of society; however, they are vulnerable because of threats and complex interdependencies [31]. New research in this field needs to account for these security issues, which are crucial to future information systems and services. In this context, AIIs provide new dimensions to security:

- *Reliability* of critical infrastructure with survival capabilities, such as power and water distribution.
- *Resilience* based on an anticipative environment that enables operation under continuous threats and attacks.

The issue of Cybersecurity is very difficult to tackle, given that nobody owns the Internet and there is no single 'command post' to control its security. The status quo regarding intrusion detection raises many challenges:

- Post attack information accumulates through many different organizations; therefore ID tools are unable to interact, making correlation of results difficult.
- Incident responses are local. There is no unified mechanism for analyzing such informational alerts and determine their implications/risk factor.

This places on the 'wish list' for security systems the following demands:

- 'On-the-fly' system configuration, requested by the continuous network changes
- Timely detection of *all kinds* of attacks
- Prevention (and counter-attack) in *any network place*
- Universal installation and maintenance

Most approaches to cybersecurity focus mainly on system protection against known attacks [32], leaving it vulnerable to the myriad of creative intrusion-hackers that produce new viruses daily. Given that today's content inspection techniques use a set of known signatures leaves the question 'How can we deal with unknown attacks?' still open.

Few approaches are taking an anticipative view, by emulating the way biological organisms protect themselves [33], [34]. AIIs are networks with moving objects and subjects 'cloned' as intangible agents in cyberspace. This vision of security cannot be defined top-down. In this ever-changing environment, security policies must evolve and adapt to suit the circumstances. Some of the requirements for the design of Cybersecurity mechanisms meant to protect our information are:

- Coordination in analysis, alerts, incidents management, counteract and response;
- Scalable, continuous running, fault tolerant, self-monitoring mechanisms;
- Ability to detect new kind of attacks;
- Ability to anticipate attacks;

To cope with these needs, we propose a holonic cybersecurity model that emulates biological behavior by inducing immunity into the network or system under attack. Much like Noria et.al. realize network immunity in [37], our system is organized as a holarchy distributed throughout the network, Fig. 7. The AII will anticipate attacks by activating specialized agents seeking the presence of intruders into the network,

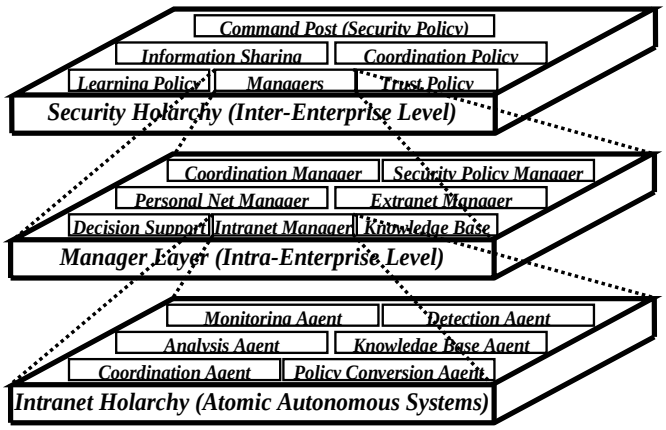


Fig. 7. Cybersecurity Holarchy

similar to how antibodies fight viruses in biological systems.

At the highest level, the "Command Post" embeds the generic security policy for an organization, which takes care of the following tasks:

- Crisis Management
- Coordinating with other organizations/government agencies
- Lower level systems management
- Shared information with trusted organizations
- Specifies which sets of network parameters should be analyzed by each entity in the holarchy

In case of an unexpected attack, every command post in the security holarchy is alerted, triggering fighter agents that specialize in eliminating attackers.

At the middle (inter-enterprise) level, 'managers' control specified agents to analyze and correlate data collected by them, whereas at the lowest level, local agents monitor specified activities. Their main functions are:

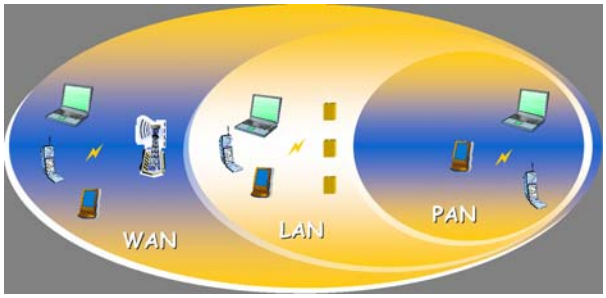
- Understand network topology
- Analyze information given by Agents

- Make decisions depending on network topology and information given by other managers and their agents
- Coordinate the 'atomic' agents (e.g. scheduling their operations)
- Manage the 'atomic agents' knowledge base updates and mediate information exchange with the 'command post' (Fig. 7).

Manager agents interact with the 'atomic' agents by:
- sending goals, derived from security policies;
- delegating specific functions of monitoring/detection and specifying the various domains to monitor;
- gathering particular information, such as: the suspicion level of a particular user, the list of events generated by a user, etc.;
- gathering relevant reports or analyses, and alarms.

The basic agents have the 'mission' to determine an initial attack by analyzing low-level network events ('local sniffers'). For this they carry on the following functions:
- Real-time monitoring of network packets;
- Full IP de-fragmentation and upper protocol data reassembly;
- Provide immediate information analysis in original environment, at that very instant and catching additional local data that might be required;
- Delay / block network traffic/ isolate segment suspected of 'attack'
- Content inspection for security behavior violations
- Delete, modify suspicious/malicious content

Given that the holonic model (Fig. 7) is mirrored by the organization of wireless networks (Fig. 8), the proposed holonic cybersecurity system encompasses both networked and wireless environments.



(WAN – wide area network; LAN – large area network; PAN – personal area network)

Fig. 8. Wireless holarchy

The holonic approach enables also a topology-oriented approach in which critical points of action are identified where agents 'migrate' as needed. This enables in addition to the automatic detection of an attack, also attack localization as close as possible to its source. Agents must be able to isolate a specific network's segments. Managers coordinate the activity of basic agents by moving the basic agents across differ-

ent network points in order to investigate what is the really "relevant" information and how to extract quality from quantity.
The requirements for deploying and exchange of information are:

- It should be faster than suspicious code. This demands predefined quality of service (QoS) priorities (dedicated 'traffic line' for emergency services)
- The secure 'tunnel' between Managers, Agents and 'Command Post'/Mediator (Fig. 7) has to be 'always ready'
- Self-deploying: ability to send mobile agent(s) in response to attack escalation

From an information gathering perspective, the task is huge, and characterized by the following challenges:

- Huge data repository: millions of data streams go through dominant Internet node points;
- Variable parameters due to network dynamics;
- Hundreds of parameters (data dimensions);
- 'On-the-fly' analysis opens a performance issue;
- Training time for large data sets may be high

This calls for advanced data mining capabilities, which can be incorporated into the distributed intelligence of the holonic system, by the managers and local agents, as follows.

Managers can deal with:

- Network Topology
- Collection of run-time abnormal information from the basic agents
- Collection of run-time information gathered from government and non-government trusted organizations
- Implement the "Command Post" directives

The basic agents can deal with:

- Protocols packet headers
- Selective data content analysis – application data streams
- Network segments and hosts profiles

Computational intelligence techniques endow the cybersecurity AII with learning and discovery capabilities. Neural networks can be used to learn:

- to detect anomaly (abnormal low-level network events; abnormal data stream content; abnormal behavior of hosts and network segments)
- to distinguish malicious traffic from normal traffic
- to update activity profiles of hosts and network segments
- to detect multi step attack scenarios
- to detect new classes of incidents

Fuzzy logic can encapsulate the strategy into linguistic rules. Examples of rules for the 'atomic' agents are:

IF (The number of total packets observed in the data collection interval for a particular day/hour for the specific host == MEDIUM)
AND (The numbers of TCP connection attempts in this data collection interval for

a specific host == HIGH)
THEN "SYN_Flood" == MEDIUM-HIGH

IF (The numbers of TCP connection attempts in this data collection interval for a specific host == HIGH)
AND (The number of successfully established TCP connections in a time interval for a specific host == LOW)
THEN "SYN_Flood" == HIGH

IF (The numbers of TCP connection attempts in this data collection interval for a specific host == HIGH)
AND (The number of incoming packets from a sole source == MEDIUM-HIGH)
THEN "SYN_Flood" == HIGH

Examples of rules for managers:

IF (The number of agents reporting about the MEDIUM SYN-Flood attack == LOW-MEDIUM)
AND (These agents resided according to the "sheaf" topology == MEDIUM)
THEN "SYN_Flood" == HIGH

IF (The number of agents reporting about HIGH SYN-Flood attack == LOW)
AND (HOPs number between these agents ==LOW)
AND (HOPs number between reporting agent and possible attacked host ==LOW)
THEN i "SYN_Flood" == HIGH

As opposed to today's intrusion detection systems, the proposed model encompasses a broader vision of Cybersecurity, which can be expanded to a national or even global Cybersecurity system. (In this vision, at the top holarchic level an 'organization' can be a country or even the planet.) Although all system's entities use intelligent decision making techniques which ensure automatic response to intrusion such capabilities will enable to mainly 'buy time' in taking low-level (non-critical) decisions. Human intervention is still required to make critical decisions and takes place through interactions between the security officer and s*ecurity policy manager agent/ extranet manager agent*. It ensures the reception of specifications and requests from the security officer such as which security policies to apply. It enables the delivery of security reports and alarms when an attack is detected. The security officer can also ask for additional information (e.g. asking for the current security state of the network or the list of suspicious users).

5.4 Security-related challenges

- Can a trusted access capability be built into security protected environments, enabling emergency help (medical, fire brigade and police) to intervene when life-critical help is at stake?
- How can we decide on the appropriate policies, strategies, architectures and allocation of resources in the absence of an assumed rationale for threat?

- Across an open, large community, how can knowledge be securely exchanged over time, as the community evolves and data and trust change?
- How can we manage the security associated with spontaneous cooperation without imposed or predefined fixed roles and rules?
- Can the ideal of running secure applications on an insecure network be reached? Can we include liability in the design rationale?

5.5 Generic Challenges in AII research and development

Some of the difficult questions posed by this research are:

- Can pathological emergent behavior of the total system, arising from the interactions between people, agents, objects, and their various policies, be avoided?
- How do we translate the interaction of agents in different contexts and environments into machine understandable language?
- How do we express and code sufficient real world semantics when the scope of interaction between agents is too broad or not predefined [35]?

There are many challenges in realizing AIIs. Highly interdisciplinary research (e.g., industrial engineering and control systems, distributed artificial intelligence and logic programming, information systems and communication technologies) is required to develop and implement dynamic services for a networked economy. We hope that the proposed research will succeed in tackling these complex developments with appropriate solutions emerging.

6 Conclusions

This research aims to create a theoretical foundation for the design of adaptive information infrastructures (AIIs) enabling and sustaining tomorrow's e-Society, as well as envision various areas of application for such AIIs, that would improve human life. The recent theoretical results obtained by us in modeling the property of emergence in self-organizing systems were refined and expanded with other recent results to create a model of *emergence in Cyberspace*, by this setting a foundation for the development and emergence of AIIs mirroring biological behavior.

The principal merit of the proposed holonic AII architecture is that it provides an environment that can react appropriately to highly unpredictable situations. By using natural models of emergence, much in the same manner as DNA is controlled in genetic engineering, we will be able to control the emergence of AIIs as crises arise. AIIs will address the emergency quickly, efficiently and most appropriately. Once a goal is set (where a certain need has to be fulfilled), the AII self-organizes to accomplish this goal optimally.

AIIs are applicable to a wide range of problems requiring timely configuration and coordination of distributed resources needed to address emergency situations, such as: *disaster emergency logistics* (evacuation planning, scheduling of emergency relief crews, food and water distribution, hospital bed planning); *national defense and security* (emergence of military AIIs as infrastructure for coordination of military opera-

tions in case of an unexpected attack);Cybersecurities (network and information securities); *ubiquitous ad-hoc healthcare* (emergence of medical AIIs grouping the most suitable medical entities able to cooperate and organize their interaction to respond adequately to patient's need; medical emergency logistics with patient information retrieval and heterogeneous transaction workflow management throughout the medical organization); *fault-tolerant flexible production* (emergent planning and scheduling of reconfigurable manufacturing production; customer-centric supply chain and workflow management; fault tracking and error reporting across the manufacturing organization).

Our future work will focus on the design of a reference model that enables the quick deployment of AIIs for emergency applications. We will investigate new areas of application, such as: how the AII approach can be used to provide advance warning of an impending health epidemic (e.g. bird flu, SARS) based on simultaneous agent monitoring of multiple hospital emergency room activity and how could a similar approach help prevent communication network outages by agent monitoring of network traffic on various routers. We will expand our previous results on global production integration, to other manufacturing areas, such as continuous monitoring of various processes and pipelines to predict changes in delivery schedules or unanticipated maintenance of equipment. We will continue to lead the development of international standards in AIIs design within international standards bodies such as the Foundation for Intelligent Physical Agents (FIPA), and the Intelligent Manufacturing Systems Consortium (IMS).

References

[1] Proceedings of the 'Ambient Intelligence: First European Symposium', EUSAI 2003, Veldhoven, the Netherlands, November 2003, E. H. L. Aarts (Editor), Springer-Verlag New York, Incorporated, ISBN 3-540-20418-0 / 3540204180.

[2] Vahe Poladian, Joao Pedro Sousa, David Garlan, and Mary Shaw, Dynamic configuration of resource-aware services, Proceedings of ICSE 2004, May 23-28, 2004, Edimburgh.

[3] M. Pechoucek, V. Marik, J. Barta, Knowledge Based Approach to Operations-Other-Than-War Coalition Formation, IEEE Tr on Intelligent Systems, Special Issue on Coalition Operations, 2002.

[4] Track on Coalition Formation, Proceedings of AAMAS 2003, July 16-18, 2003, Melbourne, Australia.

[5] Proceedings of International Workshop on Engineering Self-Organizing Applications, AAMAS 2003, July 15, Melbourne, Australia.

[6] Sven Brueckner, H. Van Dyke Parunak: Resource-aware exploration of the emergent dynamics of simulated systems, Proceedings of AAMAS 2003: 781-788.

[7] Stuart Kaufmann, *Investigations*, Oxford University Press, ISBN 0-19-512104-X

[8] Mihaela Ulieru, "Emergence of Holonic Enterprises from Multi-Agent Systems: A Fuzzy-Evolutionary Approach", Invited Chapter in *Soft Computing Agents: A New Perspective on Dynamic Information Systems*, (V. Loia – Editor), IOS Press -Frontiers in AI and Applications Series 2002, ISBN 1 58603 292 5, pp. 187-215.

[9] Mihaela Ulieru, "Modeling Holarchies as Multi-Agent Systems to Enable Global Collaboration", Proceedings of the IEEE Computer Society Press – 13th International Conference and Workshop on Database and Expert Systems Applications (DEXA 2002), September 2-6, 2002, Aix-en-Provence, France, pp. 603-608, ISBN 0-7695-1668-8, Order # PRO1668.

[10] Mihaela Ulieru, Dan Stefanoiu and Douglas Norrie, "Holonic Metamorphic Architectures for Manufacturing: Identifying Holonic Structures in Multi-Agent Systems by Fuzzy Modeling", Invited Chapter in *Handbook of Computational Intelligence in Design and Manufacturing* (Jun Wang & Andrew Kussiak – Editors), CRC Press 2000, ISBN No 0-8493-0592-6, pp. 3-1 – 3-36.
[11] Mihaela Ulieru and Dan Stefanoiu, "Holonic Self-Organization of Multi-Agent Systems by Fuzzy Modeling with Application to Intelligent Manufacturing", IEEE-SMC 2000, Nashville, USA, October, pp. pp. 1661-1666 – with Dan Stefanoiu – postdoctoral fellow and Douglas Norrie.
[12] Arthur Koestler, *The Ghost in the Machine*, MacMillan, 1968.
[13] Christensen, James H., Holonic Manufacturing Systems: Initial Architecture and Standards Directions, in *Proceedings of the First European conference on Holonic Manufacturing systems*, European HMS Consortium, Hanover, Germany, 1994.
[14] Mihaela Ulieru, Scott Walker and Robert Brennan, "Holonic Enterprise as a Collaborative Information Ecosystem", Workshop on "Holons: Autonomous and Cooperative Agents for the Industry", Autonomous Agents 2001, Montreal, May 29, 2001, pp. 1-13.
[15] Mihaela Ulieru, "A Fuzzy Mathematics Approach to Modeling Emergent Holonic Structures", Invited Chapter in *Geometry, Continua and Microstructures*, pp. 241-255, Academic Press, 2002 – ISBN 973-27-0880-8.
[16] Mihaela Ulieru and Silviu Ionita, "Soft Computing Techniques for the Holonic Enterprise", FLINT 2001, M. Nikravesh and B. Azvine (Eds.), New Directions in Enhancing the Power of the Internet, UC Berkeley Electronics Research Laboratory, Memorandum No. UCB/ERL M01/28, August 2001. pp 182-187.
[17] LARKS: Dynamic Matchmaking Among Heterogeneous Software Agents in Cyberspace, K. Sycara, S. Widoff, M. Klusch and J. Lu, *Autonomous Agents and Multi-Agent Systems*, Volume 5, No. 2, June 2002, Kluwer ISSN 1387-2532.
[18] Mihaela Ulieru and Mircea Cobzaru, "Building Holonic Supply Chain Management Systems: An e-Logistics Application for the Telephone Manufacturing Industry", IEEE Transactions on Industrial Electronics, December 2004 (accepted).
[19] Mihaela Ulieru and Rainer Unland, "Emergent e-Logistics Infrastructure for Timely Emergency Response Management by Collaborative Problem-Solving with Optimized Resource (Re)Allocation", invited chapter in *Engineering Self-Organising Systems - Nature-Inspired Approaches to Software Engineering*, Di Marzo Serugendo, G.; Karageorgos, A.; Rana, O.F.; Zambonelli, F. (Editors), Springer Verlag, 2004, X, 299 ISBN: 3-540-21201-9, pp. 139-156.
[20] Mihaela Ulieru, "Internet-Enabled Soft Computing Holarchies for e-Health Applications", in New Directions in Enhancing the Power of the Internet, (L.A. Zadeh and M. Nikravesh – Editors), pp. 131-166, Springer Verlag, Berlin, 2003.
[21] Mihaela Ulieru and Alexander Grabelkovsky, "Telehealth Approach to Glaucoma Progression Monitoring", *International Journal of Information Theories and Applications* 10(3), 2003, ISSN 1310-0513, pp. 326-330.
[22] Mihaela Ulieru and Marcelo Rizzi A Cooperative Approach to the Development of Expert Knowledge Bases Applied to Define Standard of Care in Glaucoma, Proceedings of CoopIS 2003, Catania, Sicily, Nov. 3-7, 2003, pp. 235-243, Springer Verlag Lecture Notes in Computer Science LNCS 2888.
[23] Mihaela Ulieru, Soft Computing Agents for e-Health, NAFIPS 2004 (North-American Fuzzy Information Processing Society) International Conference, Banff, Canada, June 27-30 (accepted).
[24] Mihaela Ulieru and Adam Geras, "Emergent Holarchies for e-Health Applications – A Case in Glaucoma Diagnosis", Proceedings of IECON 2002 – 28th Annual Conference of the IEEE Industrial Electronics Society, November 5-8, 2002, Seville, Spain, ISBN 0-

7803-7475-4, pp. 2957-2962, (proceedings on CD-Rom, IEEE Catalog Number 02CH37363.)
[25] Mihaela Ulieru, "Fuzzy Logic in Diagnosis: Possibilistic Networks" invited Chapter in Fuzzy Logic (J. Baldwin) John Wiley &Sons, 1996, ISBN 0471 962813, pp.135-177.
[26] ASTM E31 - http://www.astm.org/COMMIT/ COMMITTEE/E31.htm
[27] HL7 (Health Level 7) - http://hl7.org
[28] OpenGALEN: http://www.opengalen.org
[29] UMLS: http://www.nlm.nih.gov/research/umls
[30] SNOMED: http://www.snomed.org
[31] Tom Berson, Sun Tzu in Cyberspace: The Art of Information Warfare, Keynote Address at the Cybersecurity 2003 Conference, May 20, Foster City, CA, USA.
[32] Yuefei Xu, et. al., A Security Framework for Collaborative Distributed Systems Control at the Device Level, Proceedings of the 1st IEEE International Conference on Industrial Informatics, Banff, Canada, August 21-24, 2003 (M. Ulieru, R. Unland, A. Weaver, Editors), ISBN 0-7803-8200-5, pp. 192-199.
[33] D. L. Chao and S. Forrest, Information Immune Systems, *International Conference on Artificial Immune Systems* (ICARIS). pp. 132-140 (2002)
[34] N. Foukia, S. Fenet, S. Hassas and J. Hulaas, *"An Intrusion Response Scheme: Tracking the Alert Source using a Stigmergy Paradigm"*, in Proceedings of the 2nd International Workshop on Security of Mobile Multiagent Systems (SEMAS-2002), AAMAS 2002,, Bologna, Italy, July 16, 2002.
[35] Tim Kindberg and Armando Fox, Systems Software for Ubiquitous Computing, *IEEE on Pervasive Computing*, Jan-Mar 2002, pp. 70-81.
[36] http://www.biometrics.org
[37] Noria Foukia and Salima Hassas and Serge Fenet and Paul Albuquerque, "Combining Immune Systems and Social Insect Metaphors: A Paradigm for Distributed Intrusion Detection and Response System" in Proceedings of Mobile Agents for Telecommunication Applications, 5th International Workshop, MATA 2003, Marakech, Morocco, October 8-10, 2003
[38] Stuart Kaufmann, At Home in The Universe: The search for the laws of self organization and complexity, New York: Oxford University Press, 1995