



Secure-CITI: A Secure Critical Information Technology Infrastructure for Disaster Management

Ahmed Amer, Jose Carlos Brustoloni, Panos Chrysanthis,
Milos Hauskrecht, Alexandros Labrinidis, Rami Melhem,
Daniel Mossé, Kirk Pruhs
Computer Science Dept

Louise Comfort
Graduate School of Public and International Affairs

University of Pittsburgh

Motivation

- ✦ Several scenarios for emergencies and disasters
- ✦ I, the computer scientist, will NOT claim expertise
- ✦ Pick your preferred scenario with multiple emergencies, where there is a lack of resources
 - Personnel, physical resources, computing resources, etc
- ✦ How to manage this situation?

Requirements of S-CITI

- ❗ Real-Time operation: temporal requirements, monitoring in real-time, responses cannot be delayed too much, information cannot be stale
- ❗ Reliability and Self-Healing: system should be robust to failures and other unexpected events (nature of disasters!)
- ❗ Efficiency and Scalability: size is predicted to be astronomical (millions of sensors, lots of data traffic) cliché: *need the right data at the right time for the right people*
- ❗ On-Demand Authentication: different levels of authentication depending on situation and server loads

Three-phase Approach

- ✦ Pre-emergency: deploy, monitor, evaluate emergencies
- ✦ During emergency: collect data about event (from sensors and personnel) coordinate and control, respond with deployment of personnel and resources
- ✦ Post-emergency: assessment and evaluation, feedback to pre-emergency phase
- ✦ There will be a *Virtual Coordination and Control (VCC) Center, to capture the data and situations and coordinate the response.*
- ✦ *In this model, different jurisdictions may share data*

Virtual Coordination and Control

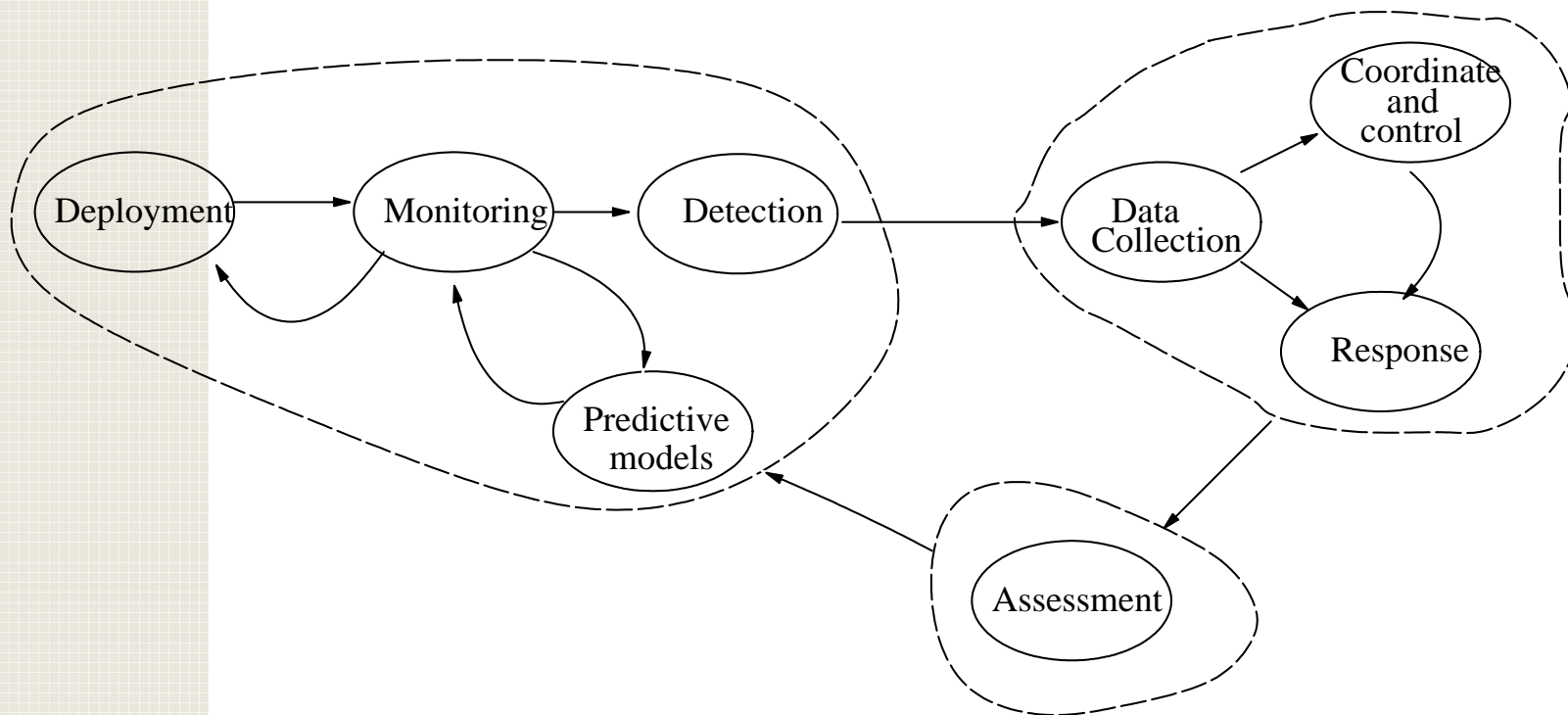
- ✦ Initially, we envision a single “situation room” where all parties come together and share the information collected appropriately:

Coordination and Control

- Privacy concerns (e.g., utilities may filter data)
 - Safety concerns (FBI/CIA/NSA may veto data sharing)
 - Data leakage problems (unauthorized data gathering)
- ✦ Later, we envision a distributed VIRTUAL C&C
 - No need for physical co-location
 - Several channels of communication with guaranteed bandwidth and Quality of Service
 - Ability to remote manage resources in all subsystems

Three-phase Framework

- ❗ System does data gathering, and perhaps suggestions to Emergency Managers (EMs)
- ❗ System does NOT act by itself, unless there is no one at helm





Communication Protocols

✦ Data routing and dissemination

- Heterogeneous nodes with respect to different resources
- Ad-hoc routing may cost too much: study scenarios first
- Adapt dynamically and autonomously to faults in nodes and routes

✦ Response in overloaded networks

- Single network is more convenient but will have more load
- Transmission of video will overtax the network

✦ Response in partitioned networks

- EM structure helps the S-CITI to fix lack of communication with nodes
- Develop protocols to work in disconnected situations (leader, what to do when, etc)

Integrated Reward-based Resource Management

- ✖ Resources of main concern are power, bandwidth, computation power, storage
- ✖ Most sets of applications will overwhelm nodes
 - Choose best set of applications to run (best = most value to system).
Examples:
 - a picture is worth a 1,000 words (on sale!)
 - coarse-grain picture at 100Kb “better than” fine-grain at 10MB
 - Value can be defined by EMs via “good” user interface
- ✖ Disaster scenarios will overwhelm network
 - Consider the “best” route the one with least congestion or the one with least probability to create a partition
 - Compress data before sending (less bandwidth, less energy)
- ✖ Fault Tolerance must be taken into account
- ✖ Security of data access is crucial



Automation and Predictive Management

- ✦ Hide complexities from EMs, e.g., where to place a certain disk-block of data? Solution: use *self-adjusting caching algorithms*
- ✦ Automation is coordinated by EMs when needed (security), and guided by EMs when possible (assigned values to tasks)
- ✦ Automated and predictive resource management at the S-CITI level, not at the decision-making level
- ✦ Integrate this with the resource management schemes mentioned above
- ✦ On-demand authentication: different personnel will be given appropriate-level challenge-response drills depending on the level of emergency or the type of service



Dynamic Data Management Protocols

- ✦ Data-driven disaster response: data type and urgency will lead the path to data management
- ✦ Dynamic *data mart creation*:
 - depending on needs of EMs, data will be retrieved, pre-fetched, and stored to increase efficiency while retaining autonomy and consistency
 - Important data must be replicated for robustness
- ✦ Dissemination of data must be:
 - Efficient and timely for control and coordination
 - Secure to avoid unauthorized access and tempering
 - Appropriate for audience (field personnel, media, families, ...)
 - Characterized after the emergency to feed the learning modules
- ✦ Streaming data management: need to process high data volume in real-time to avoid nodes to become overwhelmed or data to be dropped



Intelligent Monitoring and Diagnostics

- 🔦 Monitoring is crucial, but data intensive
 - Correlation of data from different sources is important. E.g., if all electric meters show no usage, **and** so do gas meters...
 - Such monitoring is knowledge intensive (knowledge of the CITI and of the system being monitored itself)
 - Monitoring should handle uncertainty: there **will not be** perfect knowledge base (specially in current conditions). Therefore, adapting to allow uncertainty and noisy input is very important
 - Monitoring at different data rates, depending on diagnostics
- 🔦 Diagnostics should be learned from situations and feedback from EMs

Deployment plans

- 🚀 Start small: laboratory in computer science dept
- 🚀 Make it bigger: one whole floor of the dept
- 🚀 Make it bigger: campus or building inside University, reporting to University police and maintenance depts
- 🚀 Make it bigger: THE WORLD!!!!

Conclusions

- ✖ S-CITI is, to say the least, ambitious
- ✖ IT can provide a lot of information to the EMs, who are the people that actually coordinate response
- ✖ Need to be S, ie, secure, otherwise cannot be used widely
- ✖ It is C, ie, critical, since once it is in place it will be depended upon

- ✖ EMs, utility companies, everyone must collaborate. There is no free lunch!!