2.2 Deeply Networked World/SWARMS (Smart World Airforce Repair and Maintenance System)

In the future, networking and networked devices will be broadly and deeply deployed to make possible the truly *smart world* in which intelligent agents query, collate, and manage systems. An agent model will be developed and deployed, in which agents function correctly as individuals and collaborate with each other effectively in order to make higher-level decisions than any individual agent might make. Both individually and in groups, agents will provide higher-level, composite functions responsive to societal policy constraints that may change or evolve over time. Humans will not be responsible for managing the large numbers and heterogeneity of devices in such a deeply networked world. The network will be self-organizing and self-healing. This will require the ability to measure and evaluate its behavior, and either mask or correct problems when they arise.

2.2.1 Scenario Description

In the future, the Airforce has implemented an architecture called the Smart World Airforce Repair and Maintenance System, or SWARMS, where every repair component and parts depot is "smart." SWARMS predicts when and where specific repairs will be needed and, at the level of the whole aircraft, understands flight schedules and uses this information to plan where and when work should be done. SWARMS informs the global inventory system, which in turn makes sure that by the time a plane arrives at a destination the appropriate parts are there, with enough information that the repair can be made.

In SWARMS, a part knows where it is. A depot knows how many of which kinds of parts it has and has a model of what is needed based on reports about the schedule of arriving planes. Every part, when installed in an aircraft, is also introspective. Each one knows how well it is functioning and can predict when it will need to be repaired or replaced. The composite systems not only integrate over all their parts, but also have a higher level understanding of the emergent system to support mission planning.

In this scenario, there are critical issues relating to trust, assurance, and security, including privacy, authenticity, authorization, and denial of service. The system must maintain security to prevent exploitation by the enemy. For example, SWARMS data are of great use for espionage and sabotage by the opposing force, and maintenance schedules and procedures are critical to the safety of the aircraft.

2.2.2 SWARMS Networking and Networking Research Needs

The SWARMS discussion identified key networking elements of the scenario, including:

- Smart devices that monitor their location, query function and status, and identify situations requiring attention

- ♦ Sensors and systems considered at different levels of aggregation – e.g., as individual devices or as components of larger systems
- ♦ Automated functions implemented to evaluate conditions and to control behavior
- ♦ Multiple simultaneous agents acting collectively

The SWARMS discussion identified the research needed to support these elements, including:

Trustworthiness of complex self-organized networks

The end user must know that the end-to-end system can be trusted to meet requirements. Characteristics of a complex system contributing to end user trust in the system include reliability, robustness, and security. Technical capabilities for implementing these characteristics include digital signatures, authentication, authorization, path quality,
information source, and quality of the information. The trustworthiness of a complex system is a function of the trustworthiness of its components and how they are integrated. It may change as sensors, networks, and other resources change over time. Since some network paths may be more trustworthy than others, the algorithms chosen to organize, select, and establish network paths contribute to the trustworthiness of the system. Research is needed to develop these algorithms.

Sensor data may have different "value" to an end user depending on the trust associated with the specific sensors that produced the data. Distributed sensor design characteristics, such as reliability and communications mechanisms, contribute to the end user trust in a sensor and its data. These characteristics are a consideration in the design and cost of producing the sensors. Trust will also be affected by the sensors chosen and the data paths used to obtain data from these sensors.

Adaptive distributed systems

Adaptivity may enable a greater functional range for a distributed system. In a bandwidth- and sensor-limited environment, the system can adapt the sensors chosen and the data they transmit to produce information tailored to specific levels of the decision and operational hierarchy. Several alternatives for adaptation exist:

- ♦ For simple network, the application may adapt
- ♦ For a simple smart network, the applications may adapt based on network-provided information, including initial information and operational feedback
- ♦ For a complex highly controllable network, the network may adapt based on information provided by applications
- ♦ For a complex implicitly adaptive network, the applications run and the network adapts

Adaptive networking depends on performance measurement and evaluation. Tools are needed for development, implementation, evaluation, and use of adaptation algorithms.

Scalability and self-organizing communications algorithms

We expect orders of magnitude increases in both the number of networked devices and network traffic on the future Internet. It is critical that the network scale to accommodate those increases. Research is needed to understand network behavior with these increases and to study networked systems' complexity. Research is needed to adapt relevant science from other fields such as chaos theory, economics, catastrophe theory, stochastic processes, and generalized control theory to promote breakthroughs and revolutionary solutions to scalability. Network performance measurement is critical to providing information on the functioning of the network to guide real-time network management, and to provide an understanding of network behavior to support design of the future Internet. Network performance measurement tools need to be developed, standardized, and ubiquitously deployed to provide performance data. A performance data archive is needed to provide an historical record for understanding operational network behavior, complexity, and trends and to support network simulation and design.

Currently, network scalability is implemented using hierarchical and cluster network organization. However, such organization is difficult to implement for mobile network elements, for responding to dynamic conditions, and for responding to administrative constraints. These require that self-organizing networks be able to continually change the network organization.

Research is needed to identify core networking functions and parameters, to develop algorithms that will enable highly flexible multimodal routing to support scaling and QoS, and to implement more flexible addressing schemes to accommodate emerging optical technologies. Routers need broader semantics for topology, name, attributes, and coordinates (grid location, hierarchy, etc.), and scaling for orders of magnitude expansion in numbers of networked devices and network traffic. Network simulation tools are needed to determine performance limits of a network to anticipate problems before they occur.