Secure Broadband Mobile Networking IRaD

The FCC has requested an experimental plan to show how the license in the 700 MHz band will be used. The following internal research and development plan (IRaD) will be executed once all of the necessary FCC filings have been approved. As can be seen in the report, the use of a channel in the 700 MHz band is part of a larger research effort to characterize wireless communication systems for the public safety community. Detailed test plans have yet to be developed, but will include RF propagation drive tests, uplink/downlink throughput tests, and network latency. The field tests will complement tests conducted in our technical evaluation lab and demonstrate how this equipment will operate once deployed. Combining the results of controlled lab and in-field tests will offer a more comprehensive picture of the expected equipment performance than either set of tests separately.

1) Executive Summary

Secure Broadband Mobile Networking IRaD

Principal Investigator: Tim Gallagher
Information Superiority Operating Unit
Communications Systems Division
October 7, 2005

1.1 Abstract

The Secure Mobile Broadband Networking IRaD is intended to develop and apply best practices for the design and evaluation of secure wireless networks for Northrop Grumman's government customers. The IRaD consists of three main elements:

- Technical Evaluation Laboratory
- Modeling and Simulation
- Theoretical Analysis

These three pieces unite to form a cohesive capability for the evaluation of wireless technologies.

2.0 Description of Project

2.1 Statement of Problem

It is well documented that public safety agencies have a need for secure mobile broadband wireless networks to more effectively and efficiently fulfill their missions. The problem, however, is that this segment of the public interest has historically had limited resources with which to acquire this capability. Even with the infusion of federal homeland security money, these entities have attempted to retain a fiscally responsible approach to their acquisition. It is no wonder then that our experience with recent proposal efforts has shown that these customers expect firm-fixed-price contracts and in all but a select few cases, the technology selection has a strong bearing on awards. Stated succinctly, the three underlying issues to be addressed by this IRaD are:

- Technology selection
- Accurate costing
- Security in wireless networks

2.2 Proposed Solution

The IRaD will enhance, unite, and where appropriate, develop capabilities for in-house hardware evaluation, modeling and simulation, and theoretical analysis of broadband, wireless communication systems. The project will:

- Stand-up a robust hardware technical evaluation laboratory.
- Establish and apply more sophisticated testing and evaluation methodologies and processes.
- Tailor and apply existing RF and network modeling tools to more accurately model end-to-end networks.
- Gain a deeper understanding of the technologies relevant to our customers.
- Develop a suite of security options for these different wireless networks.

2.3 Description of Proposed Technology and Challenges

Initial efforts of the proposed IRaD will be centered on the development of core competencies in technical evaluation, modeling and simulation, and theoretical analysis. These efforts will quickly support the investigation of the technologies targeted as essential for Northrop Grumman to maintain and advance our position as a leader in public safety wireless systems. Identified technologies include the recent appearance of hardware specifically designed to operate in the new public safety frequency band (4.9 GHz), WiFi, and 700 MHz. These efforts will also provide a platform for in-house testing and evaluation of different

wireless security options; thus developing our security expertise to span white paper through implementation.

3.0 Statement of Work

Task 1: Stand-up technical evaluation lab.

> *Objective*: Equip Technical Evaluation Laboratory facility with appropriate hardware and software to fully evaluate identified wireless technologies.
>
> *Approach*: Identify the appropriate equipment. Establish methodologies and processes for evaluation. Apply those practices to the evaluation of critical wireless technologies.
>
> *Result*: Hardware laboratory capable of evaluating wireless technologies utilizing a standard process. This platform will also be suitable for testing and integrating identified public safety applications.

Task 2: Test and evaluate 700 MHz and 4.9 GHz solutions

> *Objective*: Understand the operation and performance of newly available 4.9 GHz and 700 MHz equipment.
>
> *Approach*: Systems will be deployed in these bands and their characteristics (RF, network, security) will be assessed.
>
> *Result*: The outcome will be a thorough understanding of the capabilities of 4.9 GHz and 700 MHz public safety equipment. Our early testing of this technology will allow us to make informed proposals regarding appropriate use and cost.

Task 3: Develop and test security architecture for mobile wireless networks.

> *Objective*: Determination of appropriate security measures and equipment for mobile wireless networks.
>
> *Approach*: Develop and document different secure wireless architectures for 700 MHz and 4.9 GHz. Evaluate vendor hardware and software in the Technical Evaluation Laboratory.

Result: Suite of security options for wireless mobile networks and the experience to propose the appropriate choices for the intended systems.

Task 4: Test and evaluate Tropos WiFi mesh network deployment

Objective: Understand, in an actual deployment, the performance of an 802.11b/g mesh network for public safety.

Approach: Teams will be deployed to gather the appropriate RF and network data necessary to properly assess the performance of the network.

Result: The outcome will be RF propagation models and network traffic statistics that will enable us to better transplant and estimate the performance of these types of systems in other environments.

4.0 IRaD Objectives

This IRaD addresses the requirement that to properly assess a technology's appropriateness for a given application a deep understanding of those technologies is required. Combining under one umbrella the capability to test and evaluate hardware solutions (both in-lab and in-field), simulate their performance in different environments and under different conditions, and understand the fundamental advantages and disadvantages of the technologies, provides the framework for this understanding. The result will be intelligent and informed evaluations of broadband wireless communication systems for the public safety community.