Research Proposal for CERIAS 2001

Secure, Survivable, Jam Resistant Communications and Network Management

Bharat Bhargava: Principal Investigator (CS Department)
Michael Zoltowski: Co-Principal Investigator (ECE Department)
Purdue University, West Lafayette, IN 47907, USA
E-mail: bb@cs.purdue.edu, mikedz@ecn.purdue.edu

We intend to explore possibilities for external funding of the project. We have read the policies for CERIAS-funded projects and agree to abide by them. We plan to seek funding from National Science Foundation, Army Research Lab, ARPA and GE. We plan to submit proposals in Fall 2001. We have already submitted one proposal to the Collaborative Alliance Program of Army Research Laboratory in April 2001.
1 Introduction

Large heterogenous networks are difficult to manage and control in a secure manner. Some segments of the network can have wired infrastructure while others communicate using wireless channels. Interactions among these segments gives rise to interesting research questions in managing resources of the whole network efficiently. Figure 1 depicts an abstract view of a large heterogeneous network, which provides different services/applications and is vulnerable to different kinds of threats. This proposal focuses on security, survivability, and management issues being necessary in large heterogenous networks. A unique feature of this effort is to integrate the work in networking in CS with communication and signal processing in ECE.

The main thrust of the proposed research is to significantly improve the wired/wireless network management to safely and securely deliver a variety of traffic with wide range of quality of service requirements. We will focus on dynamic adjustments of network topology and communication mechanisms. This can be realized through the adaptation of the physical and link layer parameters. The second aspect of the proposed research is everything on-move nature of the wireless nodes. This introduces new threats and vulnerabilities. The spatially divergent, broadcast emanation of radio frequency waveforms that assess mobility can expose the system through interception and exploitation by an intelligent adversary via spoofing and other measures. The control messages that are needed to accommodate dynamic traffic and topology of tactical users are susceptible. In addition, distributed attacks are likely when both users and adversaries are on the move, posing extreme challenges for detection and mitigation. Secure jam resistant communications are crucial in order to achieve the military as well as communication industry needs of rapidly deploying large wireless network over wide areas. We will inspect different jam resistant protocols [19] and methods to decrease the vulnerability of wireless channels to intelligent jamming.

Existing solutions for network management use centralized mechanisms in static fashion. They react slowly or sometimes do not react to dynamic changes in the network. Moreover, centralized approaches suffer from scalability problems. Simple Network Management Protocol (SNMP) is a widely-used network management protocol on TCP/IP-based networks. A recent enhancements to SNMP added security features resulting in SNMPv3 [24]. Authentication and privacy services for SNMP are supported through the Users Security Model (USM) [24]. Specifically, USM is designed to support security against: masquerade, disclosure and modification of the information attacks. SNMPv3 supports view-based access control, which determines whether access to an object is allowed by a remote entity or not. SNMPv3 does not support security against denial of service and traffic analysis attacks. Denial of service attack on the Internet has become a pressing problem. For instance, in Feb. 2000 several major web sites (yahoo.com, amazon.com, cnn.com and others) were victims for this kind of attacks. The denial of service is an explicit attempt by an attacker to prevent legitimate users from using the network resources [18].

We propose a novel and flexible network management scheme. Th decentralize control scheme divides the network into several co-operated administration domains. This helps with flexibility on control and scalability. Each domain will have a controller to enforce several security policies e.g. load monitor and packet filtering to defeat the denial of service attacks. The controlling mechanisms are adaptable to the type, duration, timing, and severity of attack as well as their impact on router traffic.
2 Statement of the Problem and its Importance

Heterogeneous network management is a difficult problem. Existing network management schemes suffer from the following deficiencies, which give rise to proposed problems and research tasks. Our research is based on scientific experiments that test our architectural proposal and its security capabilities. The results from this research will contribute to ISPs such as AOL, e-commerce companies such as Amazon.com, network facility management in large organizations. They contribute to research in quality of service management, network security (tracking DoS attacks), network provisioning, queries of network status information, jam resistant communication, etc.

- **Scalability and Adaptability Problems:** For scalability, we need a decentralized network management scheme which may degrade the performance of the whole network and makes it prone to security attacks. Existing management scheme suffers from lack of adaptability. The research problem is the design of a dynamic adaptable scheme to account for network dynamics e.g., change in link status, load on different segments of the network, and nodes failure/recovery in addition to type, duration, timing, severity of security attacks. The challenge is to devise schemes that fully support self-reorganization and automation of the management process. Experiments A and B are designed to study these problems through implementations and simulations.

- **Security Shortcomings:** Existing network management protocols do not support protection from denial of service and flow analysis attacks. These attacks greatly threaten the decentralized network. By flooding the network with useless traffic or sending noise signals to antennas, traffic jams and loss of communication can occur.

The research problem is to devise management protocol that protect all administrative control messages and prevents various kinds of attacks and causes of interruption in regular traffic. The scheme and control should be secure even in the presence of heterogeneity in