PROPOSAL TITLE: Secure Shadow Networking for Scientific Research Collaboration

Primary Investigator(s)

Bharat Bhargava
Professor
bb@cs.purdue.edu

Department of Computer Sciences, Purdue University

Network Management
Security
Measurement & Analysis
Simulation & Modeling
Mobility
Ad hoc nets
Wireless

Abstract

Security and quality of service in mobile/wireless ad hoc networks will contribute to scientific research collaboration. We investigate the development of a suite of protocols and algorithms that enable researchers to securely collaborate over mobile ad hoc networks as well as the wired backbone. A series of experiments in key management, malicious intruder identification, and detection of denial of service attacks will be conducted. A close collaboration with Purdue ITaP on shadow network will provide realistic parameters and measurements for network management.

Proposed Research

Purdue (ITaP) is working with Cisco to build a campus-wide shadow network for supporting education and research (e.g. Living Laboratory). The Purdue Shadow Network will be enhanced by our research on wireless ad hoc networks, security, congestion control, and measurements/experiments. We investigate the development of a suite of protocols and algorithms that lead to a secure collaboration environment integrating mobile ad hoc networks and the wired backbone.

Collaboration requires secure information sharing and communication among a large number of academic, governmental, and military sites. In wireless/mobile ad hoc networks, the limited power, weak computation capability of mobile nodes, and restricted bandwidth of the open media impede the establishment of a secure collaborative environment. The research challenges are: (1) How to design an efficient key management scheme to support authentication, data integrity control, and information confidentiality? (2) How to motivate the collaboration among mobile nodes which try to maximize their own benefit? (3) How to identify and isolate malicious attackers?

The research tasks to address these problems are outlined as follows:

(1) Authentication and key management

Authentication relies on the key management service. Security mechanisms available to enforce data integrity and non-repudiation use cryptography, which requires exchange of secret keys

and/or public keys between the message sender and receiver. Broadcasting a group key with TESLA protocol [1] in an ad hoc network has to disclose the key in every packet. This consumes too much power. Applying TESLA for key commitment and setup in broadcast authentication in distributed networks is difficult [2].

We plan to develop an enhanced TESLA protocol considering the trade-off between energy and delay. The self-adaptive protocol will have a number of key discloses, so it will guarantee the key distribution reliability under different wireless channel scenarios (error rates, jamming attacks, etc.). Key management schemes that are effective in trusted collaboration environment will result from this research.

(2) Collaboration mechanism design

The second task is to design mechanisms that prevent mobile nodes from misbehaving and motivate them to collaborate. Instead of assuming that participating mobile nodes will act as instructed, we consider the environment in which all participants are rational and actions are strictly determined by their self-interests. Each mobile node is associated with a utility function that presents its preference over the possible outcomes. The utility function could be communication delay, bandwidth requirements, and quality of service parameters such as delay jitter and packet loss ratio. This research will develop protocols and algorithms that lead the network system to a rational and optimal operating point where the utility of individual nodes is maximized only when the goal of collaboration is achieved. We plan to apply the research from the game theory [3] (especially results on non-cooperative games) and results from the distributed algorithmic mechanism design [4]. Proposed mechanisms will be tested in a prototype, and experimental studies will provide guidelines to determine parameters for utility functions.

(3) Intruder identification

The third task is to identify and isolate the mobile nodes that do not operate in a rational manner. Discriminating the malicious nodes from the rational nodes will save the resources and improve system performance. The proposed mechanism will extend the existing algorithms of intrusion detection in ad hoc networks [5][6]. It will inspire the nodes to collect and share connection and communication histories which will be used as evidence to prove service violation. A forensic search engine in mobile nodes will quickly extract the required information for local intruder identification. An algorithm will be designed to achieve consistent opinions on the identities of the selfish or malicious nodes. Because of the accuracy problem of current Intrusion Detection Systems, the proposed mechanism will be tolerant to false positive and false negative mistakes. An architecture design of the proposed work can be found at [7]. The intruder identification mechanism will be evaluated through simulation. The four criteria include accuracy, communication and computation overhead, effectiveness, and robustness.

Research Impact:

A modernized campus backbone at Purdue provides 100 Mbps+ switched connection capability from the desktop with gigabit connectivity from buildings to the backbone. The Purdue Shadow Network is a redundant network that provides physical network connectivity between labs and buildings throughout the West Lafayette campus for research and experimentation. This research will contribute towards Purdue Shadow Network and the Living Laboratory. The wireless and ad hoc network emphases will supplement the wired network. The proposed research will span security, QoS, pervasive computing, and experiments for scientific collaboration. This will result in a prototype, measurements, analysis, and will provide guidelines for network management.

PhD students will complete their theses on secure networking and will be trained for industry. Current effort uses ns2 simulation but this collaboration with ITaP will allow students to experiment in a realistic network environment.

The research results obtained from the Purdue Shadow Network can provide measurements and data for Cisco. A workshop will be organized with the Cisco researchers and engineers for potential enhancements and evaluation of Cisco solutions for pervasive computing and shadow networking. The knowledge transfer on security will help Cisco to compete in the rapid growth and emergent technology of business environments.

Images Not Specified.

Time Frame for Funding and Research Completion

Funding begins on January 1st, 2004.

Research milestones are as follows:

April 30th, 2004. Development of authentication and key management schemes, and design of collaboration mechanism.

August 31st, 2004. Design of intruder identification protocol and development of prototype for collaboration.

December 31st, 2004. Integration of wired backbone shadow network and ad hoc network. Evaluation and final report.

Research Cooperation with Cisco

Measurements and data in realistic network environments from Cisco are needed for experimental studies in the proposed research.

Support Requirements

Total Budget

$99,165.00

Breakdown

Duration: January 1, 2004 - December 31, 2004.

Budget breakdown is as follows:

Professor Bharat Bhargava, Primary Investigator, three months academic year salary (25% effort) $30,053

Postdoc research associate, Xiaoxin Wu, six months salary (25% effort) $ 9,501

Graduate research fellow, two half-time Ph.D. students $39,936

Fringe benefits $9,491

Graduate fee remits $7,184

Domestic travel for collaborative meetings with Cisco researchers $2,500

Report, copying, and communication $500

Matching Funds

[1] Secure Mobile Systems, funded by NSF, $279,172

[2] ITR: Scalable Edge Router for Differentiated Services Networks, funded by NSF, $363,680.

[3] Integrating Wireless Communication for Quality of Service and Security, funded by NSF, $45,000 (Postdoc support)

[4] NSF Science and Technology Center for the Trusted Collaboration (CTC), submitted to NSF. The estimated budget is $26 million for five years of center activity at Purdue.

Researchers

Graduate Students Involved

Gang Ding (Passed Qualifier Exam)
Issa Khalil (PhD student)
Weichao Wang (Passed Qualifier Exam, working on PhD thesis)
Yi Lu (Passed Qualifier and Preliminary Exam, working on PhD thesis)

Researchers

Bharat Bhargava
Professor Bhargava's research involves both theoretical and experimental studies in distributed systems and wireless networks. His research group has implemented an adaptable video conferencing system and is involved in networking research using ideas of active routers, diffserv, and mobileIP. Professor Bhargava has conducted experiments in large scale distributed systems, ad hoc networks, authentication, key management, fault-tolerance and QoS. He is conducting experiments with large scale communication networks to support emerging applications such as digital library and multi-media databases. His current interests are in secure mobile and ad hoc systems, multimedia security, and QoS as a security parameter. Professor Bhargava was the chairman of the IEEE Symposium on Reliable and Distributed Systems held at Purdue in October 1998. Professor Bhargava is on the editorial board of three international journals. In the 1988 IEEE Data Engineering Conference, he and John Riedl received the best paper award for their work on "A Model for Adaptable Systems for Transaction Processing." Professor Bhargava is a fellow of Institute of Electrical and Electronics Engineers and Institute of Electronics and Telecommunication Engineers. He has been awarded the charter Gold Core Member distinction by IEEE Computer Society for his distinguished service. He received Outstanding Instructor Awards, from the Purdue chapter of the ACM in 1996 and 1998. He has been inducted in the Book of Great Teachers at Purdue. He has received IEEE Technical Achievement award for a major impact of his decade-long contributions to foundations of adaptability in communication and distributed systems in 1999. Professor Bhargava's students have received best paper awards in international conferences and have started a Nasdaq listed company. Professor Bhargava has a research laboratory at the Department of Computer Sciences, Purdue University, called the RAID lab. He has nine Ph.D. students and three post doctorates working on QoS and security issues in differentiated services networks, security and routing in mobile and ad hoc network, peer-to-peer streaming, hacker behavior and vulnerabilities in enterprise network, and formalizing trust and evidence for user authorization in open environments. The networking equipment and software have been funded by an infrastructure

grant from NSF. Several of his students are working in Cisco. Detailed information about the laboratory and projects can be found at http://www.cs.purdue.edu/homes/bb.

Xiaoxin Wu
Dr. Xiaoxin Wu receiced his Ph. D degree from the ECE Department, UC Davis, in wireless networks. His major research interests include cellular networks, ad hoc networks, and sensor networks, with research focus on quality of service, network security, integrated networks. The title of his thesis is "Supporting Quality of Service (QoS) in Hierarchical Wireless Networks". Currently Dr. Wu is working as a postdoctoral research associate in the Department of Computer Sciences, Purdue University. He is preparing an NSF proposal "Secure Wireless Networks" to Networking Division.

Additional Information on Researchers

Cisco Account Manager
Bruce Kennedy (317-816-5200, bkennedy@cisco.com),

Cisco Champion
Graham Holmes (408-527-6556, gholmes@cisco.com) and John F. Wakerly (408-527-9183, wakerly@cisco.com)

University Administrative Contact
Bharat Bhargava
Department of Computer Sciences

Purdue University

250 N. University Street

West Lafayette, IN 47907-2066
bb@cs.purdue.edu
765-494-6013

Information for Addressing the Check (if proposal is selected for funding)

Make check payable to:
Purdue University

Send check to:
Computer Science Business Office

250 N. University Street

West Lafayette, IN 47907-2066

Any Special Wording Required in the Award Letter:

Equipment Requests

Additional Information

References to Other Research
[1] A. Perrig, R. Canetti, J. Tygar, and D. Song. Efficient authentication and signing of multicast

streams over lossy channels. In IEEE Symposium On Security and Privacy, Berkeley, 2000.

[2] D. Liu and P. Ning. Efficient distribution of key chain commitments for broadcast authentication in sensor networks. In Proceedings of Network and Distributed System Security Symposium Conference, San Diego, 2003.

[3] M.J. Osborne and A. Rubinstein. A course in game theory. The MIT Press, Cambridge, MA, 1994.

[4] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions. In International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIALM), Atlanta, 2002.

[5] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), Boston, 2000.

[6] L. Zhou and Z.J. Haas. Securing ad hoc netowkrs. IEEE Network Magazine, 13(6), December, 1999.

[7] http://raidlab.cs.purdue.edu/research/ii-adhoc.pdf.