Agnes Hui Chan

College of Computer Science
Northeastern University
Boston, MA 02115 office:(617) 373-2390
Email: ahchan@ccs.neu.edu Fax: (617) 373-5121
URL: www.ccs.neu.edu/home/ahchan home:(781) 259-9691

Education

Ph.D. in Mathematics (Advisor: D.K. Ray-Chaudhuri) *August 1975*
Ohio State University, Columbus, Ohio
MA in Mathematics August 1972
Ohio State University, Columbus, Ohio
AB magna cum laude in Mathematics *June 1970*
Smith College, Northampton, MA

Software Built

http://www.ccs.neu.edu/home/ahchan/wsl/authkeyprotocol/index.html :
Library of Symmetric Key Based Encryption Algorithms for Palm OS
Library of hash functions for Palm OS
Multiple Precision Integer Arithmetic Library for Palm OS (MPLib)
Server Specific Mutually Authenticated and Key Exchange Protocol between Palm OS and Linux

Biographical Statement

Professor Chan has served as the Associate Dean and the Graduate Director of the College of Computer Science at Northeastern University for the past eight years. Her research interest is in the area of cryptography and communication security, concentrating in the area of pseudo random sequences and electronic cash. She is currently investigating fast, efficient cryptographic algorithms for low power mobile devices. In particular, she is considering authentication protocols and key revocation problems. Professor Chan's education and research background spans over three different disciplines – mathematics, electrical engineering and computer science. These cross discipline experiences have helped her in identifying both the theoretical and the implementation issues in building a secure communication system.

At the same time, she has taught a variety of courses ranging from freshman C++ to Ph.D. level courses in Cryptography and Theory of Computation. She has served as Program Chair of Information Security Conference, 2002 and was on the Program Committee of International Symposium of Information Theory and Application. She was on the Technical Editorial Board of Cryptologia and served as an elected member of the Board of Governors of the IEEE Information Theory Society between 1995 and 1997. She was an invited speaker in the first Tapia Conference, the Workshop on Cryptography, Sequences and Coding held at the Institute of Mathematical Application, and at the NATO Workshop on Sequences and Correlation. She was an invited participant in the NSF Workshop on Cryptography and Coding and is the organizer of a panel discussion on Electronic Commerce in the IEEE Conference on Computer Networks. She is active in promoting interest in science and engineering among women, in particular, she was an invited participant in the NSA Symposium on Women in Mathematics and participated in the CRA Distributed Mentor Project for woman undergraduates.

Survivable Ad Hoc Wireless Networks

Agnes H. Chan
College of Computer Science
Northeastern University

Advances in terrestrial fiber and satellite communications technology have significantly increased the use of wireless mobile devices both for telephony and data communications. The continued success of a heterogeneous global network requires that wireless service providers address issues of fundamental concern to their clients such as quality of service, reliability, privacy, throughput and affordability. At the same time, due to geographical inaccessibility and/or lack of support from local legislatures, infrastructure networks cannot provide universal coverage. This is especially true in disaster situations where existing infrastructure may be damaged. In order to provide communication capability in such situations, the deployment of ad hoc wireless networks becomes a necessity.

While much work has been done on fault-tolerant wired networks, ad hoc wireless networks present new and different constraints that are not commonly observed in wired networks. These constraints can be described as follows:

1. The communication medium is highly susceptible to both passive and active cryptographic attacks, such as eavesdropping and message modification and/or insertion.
2. The communication environment is subject to significant changes, such as weather, terrain, external interference from other users as well as from hostile enemies.
3. Mobile devices are often low-powered, both computationally and with respect to power supply.
4. The network topology tends to be constantly changing with little or no pre-deployed infrastructure or fixed based stations.
5. There is limited bandwidth compared to dedicated wire-line network.
6. Significant variations are found in link quality and connectivity.
7. The life/death status of mobile devices that may serve as “relays” or “routers” cannot be depended on.

It is expected that the dependency on ad-hoc wireless networks will continue to grow in the future. However, a simple migration of current technologies developed for wire-line survivable networks to ad hoc wireless environment will not suffice. Researchers in this area face many challenges, ranging from the design of algorithms and protocols, to their implementation and integration into systems, and finally to their analysis with respect to both performance and vulnerability. Here we list two major challenges in ad-hoc wireless networks.

(1) Dynamically configure ad-hoc network to maintain connectivity.

Currently almost all network algorithms deal with situations where all mobile units have unlimited power and are assumed to be connected. In reality, unlimited power is not a realistic assumption. What can be assumed is that a *few* devices may be able to exert higher power than average when needed. Power control must be considered in order to best utilize these few "designated" devices to maintain network connectivity. The following identifies important problems that need to be addressed in this area

(a) *How should power control be managed in the conservation of energy for future use*? As mobile units are relied on as both users and routers, it is important that they stay alive to maintain connectivity of the ad-hoc network. The challenge lies in not optimizing conservation locally at each mobile unit, but optimizing power availability globally to maintain connectivity.

(b) *What strategy should be used to choose "designated devices"?* Since the few designated devices are effectively acting as decision-makers, they are prime targets for malicious attacks. The criteria for choosing these "leaders" must be thought through carefully and once chosen, these leaders must be protected with appropriate security measures and their availability must be guaranteed.

(c) *Design efficient algorithms to configure the network topology dynamically in order to ensure connectivity*. Since the topology of an ad-hoc network is constantly changing, routing decisions cannot be made based on global topology.

(d) *Design efficient network protocols with respect to power control.* Efficient network protocols with respect to power conservation need to be proposed, implemented, and studied.

(2) Securing Ad-Hoc Networks from Malicious Attacks.

Unlike wire-line networks where each local loop is dedicated to a single user, a wireless link is shared among users. Anyone who has access to the link can eavesdrop and can retransmit a message as a fraudulent call. In addition, due to the ad-hoc nature of device locations it is even more difficult to ensure the authenticity of a device. At the same time, security protocols and algorithms have to be simple and efficient due to the limited computing power available in mobile terminals. Some of the problems associated with security in ad-hoc networks include the following:

(a) *Authentication protocols between low-power devices*. Since relays and routers are wireless, mobile devices, they are vulnerable to being compromised. Thus authentication is a minimal requirement for ensuring security.

(b) *Key Revocation*. In a communication network where data are transmitted in encrypted form, session keys are usually set up between the communicating parties and identities of the parties have to be authenticated. Most of the currently used technologies depend on the use of certificates, which may be expired or revoked over time. It is important that a revocation list of such certificates is maintained and secured. On the other hand, the maintenance of integrity of such a revoked list usually exceeds the capability of a low power device. It is therefore important to find efficient means of revoking certificates for low power devices in a wireless ad-hoc network.

(c) *Prevention of Denial of Service Attack.* The connectivity of an ad-hoc network depends on the availability of its mobile units. The challenge for this problem is to identify the different possible modes of denial of service attacks in order to design appropriate countermeasures.

(d) *Election Algorithm for Trusted Authority*. In an ad-hoc network where the topology and participants are dynamically changing, it is difficult to rely on one single "pre-determined" trusted authority (TA) or leader (L). On the other hand, many protocols require the presence of a TA or a L to distribute keys or to set up "standards". Efficient, distributed algorithms are needed to come to a general consensus on decision-making processes.

(e) *Integration of Security to Systems.* While provably secure, efficient algorithms and protocols are being proposed, our experiences have shown that when these protocols are integrated into real systems, security loopholes are often created. These loopholes can be due to implementation oversight as well as user errors. In either case, it is a challenge to researchers to come up with a survivable ad hoc network that is resilient to both malicious and unintentional attacks.