

# Secure Wireless Command and Maintenance Environment

**Bharat Bhargava**  
**Department of Computer Sciences**  
**Purdue University**  
**bb@cs.purdue.edu**

**Michael Zoltowski**  
**Department of Electrical and Computer Engineering**  
**Purdue University**  
**mikedz@ecn.purdue.edu**

## 1 Introduction

A Command and Maintenance Environment (CME) that optimizes the instruction and maintenance process by integrating data, information, and logistics across the bases, battle ships, and battle groups will support all strategies for reducing the maintenance and manning burden throughout the fleet. As an important part of the Smart Ship Science and Technology Program of Navy [1], wireless/mobile networks have been deployed on battle ships to provide increased responsiveness, visibility, and accessibility of information to the commander and crew. But there are security risks that threaten the safety and efficiency of the system (e.g. jamming the channel, sending false routes, or conducting illegal data accesses). These threats can come from all layers of the wireless networks. They must be mitigated before these networks can be installed on a broader scale.

## 2 Research Tasks

This project plans to integrate communication (smart antennae), routing (trusted routing discovery in ad hoc networks), authentication and key management, and intrusion detection. Research on Quality of Service (QoS) assurance, Deny-of-Service (DoS) attacks, and vulnerability/threat analysis in wireless/mobile ad hoc systems and sensor networks will lead to the establishment of a secure wireless CME. The principal tasks to secure the environment and our proposed solutions are briefly described:

- **Communication**

The idea of smart antenna has been presented in [16]. Omni directional antenna transmits information uniformly in all directions. Neighboring devices cannot be broadcasting at the same time because it will cause congestion. The transmissions enable adversaries to eavesdrop the communication, analyze the pattern of the traffic, and locate the sender. One solution to the problem is the use of smart antennae. Since transmissions are directed, remote stations can be reached with lower power consumption, and eavesdropping becomes more complicated. A smart antenna consists of multiple sub-antennae and switches. Smart antennae are available in several forms: sectorized, phased-array, and adaptive array. Sectorized antennae consist of individual sector elements aimed in different directions, where only one sector at a time is energized with Radio Frequency (RF). Phased-array antennae can steer a main lobe in any direction, but are not capable of forming intentional nulls. Adaptive arrays can form not only multiple main lobes, but also steerable nulls in the direction of interferers [17]. A switch can direct the beam in a specific direction. It increases security and conserves power [18]. Some antennae on multiple devices can be communicating with devices in different directions.

Another idea is the use of jam resistant antennae [2][3]. The idea is to use two antennae on each device and use polarization in a way to receive signals from one direction. The success of the semi-blind method (cross relation method and exploitation of the training sequence) and a method based only on the training sequence has been demonstrated. The simulation shows that training-based sequence-based performs better. One can use blind or semi-blind algorithms for channel estimation as long as there are two distinct antennae available having either different polarizations or significant spatial separation for diversity sake. The ideas of channel estimation and equalization for GSM with multiple antennae will be studied.

To apply the smart antenna technology to 802.11, training signals can be carried in the request-to-send (RTS) and the clear-to-send (CTS) packets. The minimum length of the training signal and the possible modification on MAC layer for CSMA/CA will be studied. The mechanisms of anti-jamming during link set-up stage will also be examined. The suitable level of transmitting power will be evaluated based on power consumption and the probability of successful link set-up under different levels of jamming.

We plan to investigate implementing smart antennae to improve reliability. The ring protection or mesh protection [4] can be used since smart antenna makes the wireless network a virtual wired network. Multi-routes in a ring or mesh network can help a node reach the data sink through the routes away from the jamming sources. The feature that in a sensor-based network, all the nodes will finally route to the data sink will be considered for the route redundancy design. A series of experiments will be conducted to study the efficiency of the ring and mesh protections. The evaluation parameters include the reduction of the data loss due to jamming, and energy saving at the sensors.

- **Trusted routing protocol for ad hoc networks**

In a mobile/wireless ad hoc network, every node participates with other nodes to deliver packets to their destination. The safety of a communication solely depends on a proper choice of a sequence of nodes used to reach the destination [7]. We use the degree of trust [8] to estimate the risk of selecting a node. Trust information is propagated and routes are discovered according to specific requirements. Sending packets through trusted routes that only involve trustworthy nodes will decrease the probability of malicious attacks and information leakage. We formalize trust for routing by building a model that quantifies the trustworthiness of a node based on its behaviors (e.g., forwarding packets, choosing proper routes), reliability, and security. Algorithms are being developed to assess the trustworthiness of a route based on information of nodes. We plan to experimentally study the integration of security mechanisms such as authentication, encryption/decryption, and filtering to defend against malicious attacks.

- **Authentication and key management**

A cluster-based protocol and a hierarchy-based protocol have been proposed to implement fault-tolerant authentication [5]. The robustness analysis and experimental evaluation will be conducted to compare them and provide guidelines for the design of efficient key distribution protocols and the authentication methods.

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 [20] 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. 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 disclosures, 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 a trusted collaboration environment will result from this research.

We propose a group key management protocol for a sensor-based network. In this protocol, every node only holds a part of the group key. When an encryption/decryption operation is initiated, the nodes will share their partial keys and the group key will be recalculated. The partial keys will be collected in a hierarchical fashion. One of the nodes will act as a leader. With this organization, the group members can compute the group key efficiently. And the confidentiality of traffic within the group will be achieved.

- **Intrusion detection and intruder identification**

This task is to identify and isolate the mobile nodes that attack or do harm to the connectivity of the networks. 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 [21]. 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. A project supported by Center for Education and Research in Information Assurance and Security (CERIAS) has made some progress in this research. The intruder identification mechanism will be evaluated through simulation. The four criteria include accuracy, communication and computation overhead, effectiveness, and robustness.

- **Quality of service and Deny-of-Service attacks**

Critical applications, such as disaster recovery or dealing with unexpected attacks, demand QoS. This includes packet loss rate, transmission latency, and delay jitter over shared networks. Providing different levels of QoS may attract abusers that steal bandwidth and other network resources. Such behavior makes use of known vulnerabilities in firewall filter rules to inject traffic or spoof the identities of valid users with high QoS levels. This creates a need for developing an effective defense mechanism that can automate the detection and reaction to attacks on the QoS provisioned network domain. Inspired by recent results on network tomography, we infer internal characteristics of a network domain using edge-to-edge probes, and design a distributed monitoring system to detect service violations and bandwidth theft in a network domain [9]. We employ agents on selected routers of the QoS domain to efficiently measure packet delays, loss, and throughputs. Measurements are communicated to a Service Layer Agreement (SLA) monitor (SLAM). The SLAM can analyze measurements and automatically detects potential attacks and violations of negotiated SLAs, as well as flag the need to re-provision the network by increasing capacity or limiting users. A suite of

protocols to detect DoS attacks (e.g. flooding by a malicious device, impersonation, and Byzantine gang attack) and identify the malicious nodes are presented in [6].

We plan to study the service violation in Wireless LAN. CSMA/CA allows the users to adjust their contention efforts. A QoS level can be achieved by using different back off strategies [10]. A selfish user or a service violator may ignore this rule and occupy the shared bandwidth by increasing their contention frequency, i.e., using small values of back off time. To identify the service violators, the access point (AP) has to know the traffic load in the network. We propose that AP will poll periodically, and users who have data to send will reply to this poll with a short message. The reply will be sent in a randomly picked slot during the "poll-reply" frame. Since there may be message collision, research will be conducted on the accuracy of this polling scheme on estimating the network load. To tell whether the user is malicious or is lucky, an upper bound for the throughput of an individual user in a WLAN network with different traffic load and QoS levels will be studied. A user whose throughput is above the upper bound is malicious. A user with a high throughput but below the upper bound will be urged to degrade its QoS level. Effectiveness of the violation detection will be evaluated by the accuracy of malicious judgment, network fairness, and overhead.

- **Vulnerability analysis and threat assessment and avoidance**

Wireless communication requires protocols such as IEEE 802.11 and its siblings. A shared key of size 40 or 64 bits in IEEE 802.11 and 128 bits in IEEE 802.11b is used to provide authentication and encryption of data. However, these protocols are vulnerable to a wide range of attacks and an attacker can jam all frequencies in the band being used by the wireless network. Vulnerabilities include decrypting traffic and injection of new traffic from unauthorized mobile nodes. Security problems and flaws in IEEE 802.11 based networks are discussed in [19].

Vulnerability analysis of wireless networks will consider the design, implementation, and maintenance of systems. A taxonomy and a formal model for characteristics of vulnerabilities will be developed. Formal descriptions of the impact of vulnerabilities and quantitative vulnerability impact evaluation methods will be studied.

Threat avoidance is important at the design and implementation stages of a computer system. An insufficient degree of threat avoidance makes a system vulnerable to attacks. Research to provide practical procedures, methods, algorithms, and tools should utilize the ideas of exploiting unpredictability and non-determinism, and the existing fault avoidance models from the reliability area [11]. Threat tolerance needs better algorithms and tools for both design-time and run-time decisions (i.e. after the system is deployed). We plan to develop new techniques and approaches analogous to the ones used for fault tolerance. Initial results of our work are presented in [12].

### **3 Applications for Navy**

The results of the proposed project will have significant impacts on the current projects in Navy. Some examples are as follows.

- **Automatic Maintenance Environment and Total Ship Monitoring**

In January, 2003, the USS Howard, a guided-missile destroyer has been outfitted with specialized wireless gateways based on IEEE 802.11b wireless LAN standard [13]. At the same time, hundreds of sensors have been deployed on the hull, mechanical, and

electrical devices to collect real time data from them. The security and efficiency of these devices are under test before they can be installed in a broader scale. The proposed research on anti-jam and security enhancements on 802.11b will guarantee the data confidentiality and communication efficiency in battle fields under electrical attacks. The secure data sink and integration algorithms for sensor networks will help the command system to respond faster to the sudden events even when a large amount of data from engines, pipes, and weapon controllers is being transferred.

- **Mobile Hospital of MASH**

In the Iraqi Freedom operations in 2003, the Navy has employed mobile hospitals to help agencies meet missions [14]. They have been supporting about 1000 doctors, nurses, and field corpsmen in MASH handling from 50 to 500 patients in 24 to 48 hour cycles. With the help of the research results from quality assurance and secure data access control, the doctors will be able to get the real time information technology support that is similar to a fixed hospital site. At the same time, the confidentiality of the patient information is guaranteed because only the trusted users will be granted the access.

- **Wireless security in Navy Intranet Project**

Wireless security is an important topic in the Navy's \$6.9 billion intranet project [15]. With the deployment of wireless routers and access points, there will not be a strict line of "firewall". Applying smart antenna and hierarchical key management schemes to the wireless routers can decrease the information breaches caused by eavesdropping. The intrusion prevention and detection methods must be deployed to stop the people hacking into the wireless system.

#### **4 Related research in progress**

The research laboratories led by Prof. Bhargava and Prof. Zoltowski are conducting theory analysis and experimental studies on the security of wireless networks. The projects are supported by grants from National Science Foundation (NSF), Office of Naval Research, Motorola, and Cisco.

#### **5 Reference**

- [1] "Battle Group Automated Maintenance Environment", white paper, R. Hogan, T. Cesarone, D. Dragun, NAVSEA and 3eTI, 2003, [http://enl.endiva.net/3eti/files/literature/2680.2708\\_BGA\\_AME\\_Paper\\_329.pdf](http://enl.endiva.net/3eti/files/literature/2680.2708_BGA_AME_Paper_329.pdf).
- [2] "Multiuser Second-Order Statistics Based Blind Channel Identification for Using a Linear Parameterization of the Channel Matrix", T. Krauss and M. D. Zoltowski, IEEE Trans. on Signal Processing, 2000.
- [3] "Future Combat Systems Communications Program", Fact Sheet, DARPA, 2001.
- [4] Optical Rings and Hybrid Mesh Rings Optical Networks, IETF draft, <http://www.ietf.org/proceedings/01mar/slides/ipo-6/>,
- [5] "Fault Tolerant Authentication in Mobile Computing", B. Bhargava, S. Kamisetty, and S. Madria, in Proceedings of International Conference on Internet Computing (IC, 2000), Special Sessions on New Paradigms in Computer Security, 2000.
- [6] "Detecting Service Violations and DoS Attacks", A. Habib, M. Hefeeda, and B. Bhargava, in Network and Distributed System Security Symposium (NDSS'03), 2003.

- [7] “On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks”, W. Wang, Y. Lu, and B. Bhargava, In Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom), 2003.
- [8] “Authorization Based on Evidence and Trust”, B. Bhargava and Y. Zhong, in Proceedings of International Conference on Data Warehousing and Knowledge Discovery (DaWak), 2002.
- [9] “On Detecting Service Violations and Bandwidth Theft in QoS Network Domains”, A. Habib, S. Fahmy, S.R. Avasarala, V. Prabhakar, and B. Bhargava, In Computer Communications, Elsevier, 2003.
- [10] “802.11e brings QoS to WLANs”, <http://www.nwfusion.com/news/tech/2003/0623techupdate.html>.
- [11] “Transaction Processing: Concepts and Techniques”, J. Gray, and A. Reuter, Morgan Kaufmann, San Mateo, CA, 1993.
- [12] “From Vulnerabilities to Trust: A Road to Trusted Computing”, L. Lilien and A. Bhargava, VIP Scientific Forum, International IPSI-2003 Conference, 2003.
- [13] “Rockville firm hoping to help the Navy go wireless”, The Washington Post, May 7<sup>th</sup>, 2002, <http://en1.endiva.net/aeptec/files/literature/1755.pdf>.
- [14] “GTSI: Mobile Enterprise IT at War”, [http://www.gcn.com/research\\_results/govunwired-5.html](http://www.gcn.com/research_results/govunwired-5.html).
- [15] “ERP, Security Rollouts Boost Troubled Navy Intranet Project”, Computer World, 2002, <http://www.computerworld.com/softwaretopics/erp/story/0,10801,79217,00.html>.
- [16] “Smart antenna for handsets”, T. Biedka, et al, DSPS Fest, 2000.
- [17] “Recent Advances in Reduced-Rank Adaptive Filtering with Applications to High-Speed Wireless Communications”, M. Zoltowski, SPIE's International Symposium on AeroSense, SPIE Proceedings Volume 4395: Digital Wireless Communications, 2001.
- [18] “Sensors and Wireless Communication for Medical Care”, A Bhargava, and M. Zoltowski, to appear in the Proc. of International Workshop on Mobility of Database and Distributed System (MDDS), 2003.
- [19] “Security Flaws in 802.11 Data Link Protocols”, N. Cam-Winget, R. Housley, D. Wagner, J. Walker, CACM, 2003.
- [20] “TESLA: Multicast Source Authentication Transform Introduction”, draft-ietf-msec-tesla-intro-01.txt, with Ran Canetti, Bob Briscoe, Dawn Song, and Doug Tygar, proposed IETF draft, 2003.
- [21] “Intrusion detection in wireless ad-hoc networks”, Y. Zhang and W. Lee, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom), 2000.

## **6 List of researchers at Purdue**

### **Bharat Bhargava**

Professor Bhargava's research involves both theoretical and experimental studies in security in wireless networks and distributed systems. 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>.

### **Michael Zoltowski**

Michael D. Zoltowski received the Ph.D. in Systems Engineering from the University of Pennsylvania in 1986. From 1982 to 1986, he was an Office of Naval Research Graduate Fellow and he was a Summer Faculty Research Fellow at the Naval Ocean Systems Center in San Diego, CA during 1987. In Fall 1986, he joined the faculty of Purdue University where he currently holds the position of Professor of Electrical and Computer Engineering. In this capacity, he was the recipient of the IEEE Outstanding Branch Counselor Award for 1989-1990, the Ruth and Joel Spira Outstanding Teacher Award for 1990-1991, and the 2001-2002 The Wilfred Hesselberth Award for Teaching Excellence. In August 2001, he was named a University Faculty Scholar by Purdue University (two selected from all of Engineering per year.)

Dr. Zoltowski was the recipient of the IEEE Signal Processing Society's 1991 Paper Award (Statistical Signal and Array Processing Area), "The Fred Eilersick MILCOM Award for Best Paper in the Unclassified Technical Program" at the IEEE Military Communications (MILCOM '98) Conference, and a Best Paper Award at the IEEE International Symposium on Spread Spectrum Techniques and Applications (ISSSTA 2000). He is also a co-recipient of the IEEE Communications Society 2001 Leonard G. Abraham Prize Paper Award in the Field of Communications Systems for the paper, "A Space-Time Model for Frequency Nonselective Rayleigh Fading Channels with

Applications to Space-Time Modems" appearing in the July 2000 issue of IEEE Journal on Selected Areas in Communications.

He was recently selected as a Distinguished Lecturer for IEEE Signal Processing Society. There are six Distinguished Lecturers chosen each year to represent the Society by giving lectures on their research around the world. The web site for the SPS Distinguished Lecturer Program indicates that "The Society's Distinguished Lecturer Program provides means for chapters to have access to individuals who are well known educators and authors in the fields of signal processing, to lecture at Chapter meetings."

He was also recently selected for the 2002 Technical Achievement Award from the IEEE Signal Processing Society As posted at SPS Technical Achievement Award Information , "The Technical Achievement Award honors a person who, over a period of years, has made outstanding technical contributions to the theory and/or practice in technical areas within the scope of the Society, as demonstrated by publications, patents, or recognized impact on the field. The prize shall be \$1500, a plaque and a certificate, and shall be presented at the ICASSP meeting held during the Spring following selection of the winner." The award will be conferred at ICASSP 2003 in Hong Kong during 6-10 April 2003.

He is a contributing author to Adaptive Radar Detection and Estimation, Wiley, 1991, Advances in Spectrum Analysis and Array Processing, Vol. III, Prentice-Hall, 1994, and CRC Handbook on Digital Signal Processing, CRC Press, 1996. He has served as a consultant to several companies in the telecommunications industry. He has served as an associate editor for both the IEEE Transactions on Signal Processing and the IEEE Communications Letters. Within the IEEE Signal Processing Society, he has been a member of both the Technical Committee for the Statistical Signal and Array Processing Area He is currently a member of both the Technical Committee on Signal Processing for Communications (SPCOM), the Technical Committee on Sensor and Multichannel (SAM) Processing. In addition, from 1998 to 2001, he was a Member-at-Large of the Board of Governors and Secretary of the IEEE Signal Processing Society. In 1998, he was elected a Fellow of IEEE. His present research interests include space-time adaptive processing for all areas of mobile and wireless communications, GPS, and radar. Detailed information can be found at <http://dynamo.ecn.purdue.edu/~mikedz/>.

### **Post Doctorates**

Dr. Leszek Lilien

Dr. Xiaoxin Wu

### **PhD Students**

Yi Lu (Passed Qualifier and Preliminary Exam, working on thesis)

Weichao Wang (Passed Qualifier Exam)

Gang Ding (Passed Qualifier Exam)

Issa Khalil (Passed Qualifier Exam)