Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

SWARM: Secure Wireless Ad hoc Robots on Mission
A course where wireless security meets robotics

Guevara Noubir, *Senior Member IEEE,*
College of Computer and Information Science
Northeastern University
Boston, MA, 02115, USA

Abstract – In this paper, we describe the SWARM course. SWARM was designed for Honor Senior students to learn and practice secure wireless communication in the setting of rescue mission type of applications* [1]. *The theoretical component of the course covers aspects such as cryptography, security protocols, and wireless communication protocols. On the practical side, the students' teams design a system composed of a smartphone, a sensor network, 2-3 robots controlled through a multihop network, and compete for quickly localizing an object that periodically transmits a beacon message. During the competition the students can interact with their robots only through their cellphone. Half of the competition time is for an adversarial scenario where teams have to achieve their mission under attacks (e.g., jamming, replay, nodes compromise communication interception, physical interception by robots) from other teams. We will describe the course component, how they inter-relate, and will discuss our preliminary conclusions.

Index terms – wireless, security, protocols, jamming, localization, robotics, cellphones.

I. Introduction

Information Assurance is a topic that requires as much attention to its real-world implications as its theoretical underpinnings. As such, Northeastern University's College of Computer and Information Science has endeavored to provide students in both the undergraduate and graduate curriculum with a program that gives them the opportunity to explore the practical elements of information security awareness and related design and deployment decisions in a secure lab while simultaneously acquiring a strong conceptual knowledge of the underlying theory in the more traditional classroom environment. The combination of these elements provides students with a vivid picture of how and why and how networked applications must be designed, implemented, and maintained in a secure fashion.

Our most recent addition to our curriculum is a course, currently limited to Honor Senior Undergraduate Students. The course is called SWARM (Secure Wireless Ad hoc Robots on Mission) and is taught during the current Spring 2006 semester. It aims at bridging the gap between Security, Wireless Communication, and Robotics.

The theoretical component of this course is designed to expose the students to the concepts underlying the design of robust and secure heterogeneous wireless networking of mobile robots. The course is mostly laboratory-focused with the goal of designing, and building rescue-mission oriented heterogeneous wireless systems, operating in adversarial environments. It integrates a competition as a pedagogical tool to motivate the students and challenge them to give their best. It makes use of state of the art technologies such as smartphones programming (i.e., J2ME [2], Bluetooth communication [3]), multi-hop sensor networks design and programming (i.e., ZigBee RF communication [4], ultra-low power embedded development).

There already exist several robot-based competitions. Most of them focus on the robotic aspect (http://palantir.swarthmore.edu/aaai05/, http://www.ecsel.psu.edu/~avanzato/robots/), and only few of them address the multi-robot coordination, and tasks planning aspect (e.g., http://www.fira.net, http://www.robocup.org/). However, to the best of our knowledge none of them is designed as a course for students to learn about the core technologies of embedded systems, network security, wireless communication, and robotics. Here not only the robots need to coordinate their actions to achieve a goal, but they also need to take into account energy efficiency in an adversarial environment, and make use of various types of wireless communication

ISBN 1-933510-98-6/$15.00

technologies. Moreover, our course provides the students with the adequate support throughout the semester to make continuous progress towards building their own system. In addition to the instructor's support, the students are provided with reference designs, libraries, and if necessary pre-made module to help them progress.

II. Class organization and outline

The class is organized into small teams of 4 students. Each team is provided with some equipment, and a small budget to extend its system. The detailed schedule of the course is available on the course webpage [1].

A. Prerequisites

The course is offered to Honor Senior students. These students are expected to be proficient in programming in Java and have a basic of knowledge of C/C++. These students are also expected to have an understanding of processor architectures, and network protocols fundamentals. No digital hardware design knowledge is mandatory but teams are encouraged to recruit at least one member with such knowledge.

B. Lectures (first eight weeks)

During the first eight weeks, the students attend lectures covering:

- Embedded development tools for sensor nodes (sensor nodes architecture, cross-compiling for TI-MSP430, Chipcon ZigBee features),
- Cryptography,
- Network Protocols,
- Network Security Tools,
- Authentication and Secure Communication Protocols,
- Wireless Communication Protocols (e.g., IEEE802.11, Bluetooth, ZigBee, Cellular Communication).

C. Assignments (first eight weeks)

Simultaneously with the lectures, the students are given **laboratory assignments** to practice:

- Embedded development (e.g., cross-compile and download blink-LED code, Wireless *echo* application between two sensor nodes).
- Smart Phones programming (e.g., write a simple chat application over a Bluetooth link between a smartphone and a Bluetooth-enabled Personal Computer).
- Simple modification of an off-the-shelf robot (robospian) to replace the IR control by a ZigBee/sensor node control.

Each team is also given a **research reading** assignment in an area topic related to the course. The teams are required to read three to four research papers in the area and are required to present them during WEEK 12. The proposed research topics are:

- Broadcast authentication in sensor networks.
- Multihop wireless ad hoc networks: capacity and protocols (e.g. DSR, AODV).
- Secure ad hoc network routing protocols (e.g., SAODV, Ariadne).
- Low-power medium access control protocols for sensor networks.
- Fault-tolerance in distributed systems (e.g., Byzantine generals problem, consensus, failure detectors).

D. System Design

With the help of the instructor the teams design their system and make a first presentation during WEEK 10. They present the:

- Hardware choices,
- Robust communication aspects and robots coordination,
- Security including protection against jamming and packets fabrication and replays.
- Localization of object to be rescued.
- Technique to attack other teams without exhausting their batteries.

More information on the system is provided in Section III.

E. Competitions

The course culminates in a competition, where each team has to find and rescue an "object" (called RF-Egg) that is hidden within the competition perimeter and might be located under some rubble. This year the RF-Egg is hidden in a white box (See Figure 2). One robot does not have the capability to succeed in the mission alone, but needs the co-operation of at least another robot. This is because the range of the radio interface will not allow single-hop communication from the coordination unit to the object to be rescued. Each team is allowed to jam the communication of the other teams (at the expense of depleting its batteries), or carry other physical or cyber denial of service attacks. During the competition the teams can only interact with the robots through a smart phone cell phone. The team members can establish data connections using the GPRS/EDGE cellular network or a Bluetooth connection to their Internet-worked central node. The central node will process the inputs to help coordinate the mobile nodes actions and securely relay it over the sensor network to the mobile robots. The sensor nodes should also be able to co-operate without always relying on the central node.

The competition is scheduled during two weeks: WEEK 10 (pre-competition), and WEEK 14 (final-competition). The pre-competition is basically a rehearsal to give the students a flavor of what to expect in terms of technical problems, adversarial activities, and stress. The pre-competition is followed by a presentation where the students need to describe the problems they encountered and how they plan to resolve them for the final competition. They also present the types of attacks they achieved and suffered from other teams. The pre-competition and final-competition are separated by 4 weeks to fine tune the system. The final competition is also followed by a presentation.

Both the pre-competition and final competition are split into two parts. During the first part, teams are not allowed to attack the other teams and have to focus on localizing the object to be rescued as quickly as possible and mark it. During the second part, the teams are allowed to attack each other. Both cyber attacks on the wireless sensor network, Bluetooth/GPRS link, applications, and physical attacks between the robots are allowed.

F. Presentations

The teams have to make three presentations:

- Briefing on the pre-competition results: techniques, attacks, success and failures, lessons learned.
- Briefing on the final-competition results.
- Summary of research reading assignment.

G. Core technologies covered in class

- Embedded Systems
- Wireless Communication
- Network Security
- Robotics

III. SYSTEM

With the guidance of the instructor, each team is required to build a system that consists of two mobile robots based on "monster trucks" and/or "robosapien" (http://www.robosapienonline.com/) or other of the shelf robot kits (e.g., http://www.roboticsconnection.com). The students are allowed to enhance their system with a servo-controlled arm, a low-power control and sensing embedded system (designed by the teams with the guidance of the instructor), and a low-power digital radio frequency communication network. This year all students are using the *moteiv* [5] sensor nodes as the embedded system to communicate and control the robots. The system should provide the following functionality:

- Multi-hop communication capability over heterogeneous wireless interfaces: smartphone – (*Bluetooth*) – laptop – (ZigBee) – sensor node.
- Control of robots.
- Security: confidentiality, integrity (protection against replays, packets fabrication, etc.).
- Resiliency to jamming.
- Fast localization of object to be rescued (RF-Egg).

A. RF-Egg

The goal of the systems designed by the teams is to find an RF-Egg (or Ultrasound-Egg) depending on the technology that is used to localize it. The RF/Ultrasound Eggs is built by the instructor. This year we are using an RF-Egg. The RF-Egg periodically transmits a beacon signal uniquely identifying the object. The beacon signal is transmitted at different power levels to make its localization easier. In the future, in order to protect against replays, the RF-Egg will implement a broadcast authentication technique based on fractal hash-chains [8]. With this technique sensor nodes can, at low-computation cost, authenticate the origin of the beacon signals. Without such a technique adversaries can replay and fabricate beacon messages. The advantage of this technique over an authentication based on public key signatures is the computation cost. The sensor nodes do not have the computation power to verify public key signatures.

B. Sensor nodes

The sensor nodes used this year consist of the moteiv motes [5]. They integrate a Texas Instruments' MSP430 ultra low-power micro-controller, and the Chipcon 2.4GHz transceivers (ZigBee compliant). The teams make use of three sensor nodes. One node is connected to the laptop, the two other motes are interfaced with the robots/cars. The sensor nodes are used to control the robots motion, relay packets, and help localize the RF-Egg based on the strength of the beacon packet.

C. Robots

A robosapien V1 [6] was given to the teams. It is the responsibility of the teams to select a second mobile robot. The selection criteria can be speed of mobility, flexibility in manipulating objects, cost. One of the first assignments given to the teams is to replace the Infra-Red remote controller of robosapien with a digital control from a sensor node. This year some teams choose the robosapien V2 [7] as the second robot, while other teams choose the Lego Mindstorm Car. The car has the advantage of speed and makes the localization faster. However, it required extra effort from the teams to

interface it with a sensor node (integration of digital switches controlled by the General Purpose Input/Output pins of the sensor nodes).

D. Coordination unit (internet gateway)

The robots actions are coordinated through a coordination unit connected to the internet and capable of communicating with the mobile robots. The coordination unit is a personal computer (usually a laptop) with ZigBee interface, a Bluetooth interface, and internet access. The coordination unit collects data from the sensor network, and instructions from the smartphone and generates commands for the robots. Feedback to the user is sent to the cellphone and can also be displayed on the laptop.

E. Smartphone (cellphone)

During the competition the smartphone is the only way the teams can send commands to their robots. The teams have to write a service running on the coordination unit that allows the smartphone to send instructions to the robots. The smartphone communicates with the coordination unit through either a Bluetooth link or a GPRS connection. This year all the students choose to use the Bluetooth link because of the low delay.

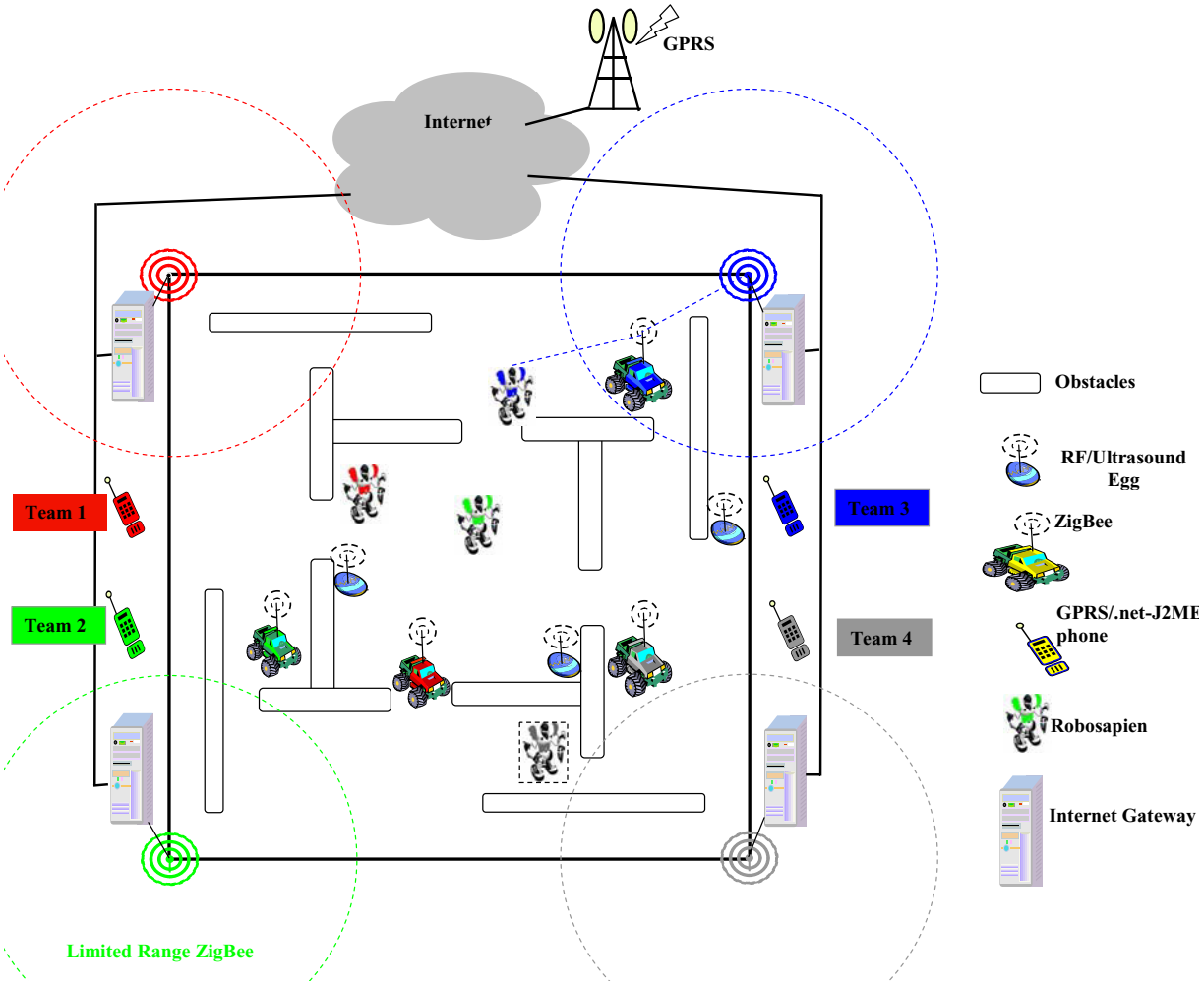

Figure 1. The competition setup.

IV. Competition Themes

The course provides students experience in the following topics:

- **Heterogeneous Multihop Wireless Communication:** the teams have to build a system that makes use of heterogeneous wireless communication capability (i.e., Bluetooth, GPRS/EDGE, Low-Power RF such as ZigBee, Internet). The teams need to design a low-power multihop communication protocol for the mobile nodes.
- **Jamming Resiliency:** To succeed in its mission the radio interfaces have to be used efficiently to conserve energy even against jammers. ZigBee allows communication over multiple channels. The teams have to design a cryptographic, synchronized channel-hopping mechanism to avoid narrow-band jamming. Another anti-jamming technique consists of using the physical mobility of the robots to propagate information. During the second part of the competitions are allowed to ham each other.
- **Applications and Protocols Security:** the design and source code of all the system is made available to all competing teams. The teams have to design the necessary security protocols (i.e., authentication, data integrity, confidentiality, and availability) to prevent other teams from taking over their nodes, intercepting their communication, or carrying a denial of service attack.
- **Localization:** the RF-Egg periodically transmits a beacon signal. The beacon signal is sent at multiple power levels. The beacon packet contains a sequence number, an identifier uniquely identifying the RF-Egg, and transmission power level. The mobile robots can be used to measure the receiver signal strength indicator (RSSI) and triangulate the source of the transmission. Additional localization considered by the teams rely on the imperfections of the sensor nodes antennas to determine the direction in which source of the beacons is located.

Figure 2. RF-Egg is hidden in one of the white boxes.

- **Resource Efficiency:** each team is given an energy budget for the duration of the competition (x mAh for communication and y mAh for mobility). A team is allowed to use part of their project financial budget to acquire and integrate a solar panel in their system. The teams are also be evaluated based on the ratio of, successfully located and brought back eggs, to the energy consumed.
- **Tasks Scheduling:** the teams have to design a task scheduler and planner to efficiently carry their mission. Given that the speed and functionality of the robots/car is not the same (e.g., the robots are much slower than the car but can manipulate objects more easily), the cars should be used for localization and robots for marking the RF-Egg. The teams has to take into account that other teams might be mimicking them and have to devise strategies to protect against it.

V. Competition Phases

In order to guarantee a continuous learning curve for the teams and avoid failures, we organized the course into multiple phases and with milestones. At the end of each phase the instructor can reshuffle the teams to balance their strengths. Also at the beginning of each phase teams are allowed to request some pre-made devices or software (e.g., embedded system, security library). The pre-made components are designed by the PIs. Each requested component carries a penalty.

- **Phase 1:** embedded system with wireless interface to control the robots.
- **Phase 2:** cell phone based remote control for mobile robots through the internet (or Bluetooth): *single-hop* case.
- **Phase 3:** cell phone based remote control for mobile robots through the internet the *multi-hop* case.
- **Phase 4:** RF/Ultrasound Eggs localization by mobile robots.
- **Phase 5:** final application for autonomous and cooperative eggs search and rescue.

VI. Competition Rules

- **Teams' composition:** the students are advised to create teams such that each one has a member with some basic digital-hardware design skills, a member with basic embedded-systems programming skills, a member with basic network-programming skills, and a member with basic robotics knowledge. All teams should have basic knowledge of communication protocols and network security.
- **Competition objectives:** find objects (40%); map area (20%); bring object to base (40%). The

evaluation criteria are the minimum energy cost per task and the minimum time for task completion.

- **Start/Finish time and location:** each part of the competition last 1 hour 40 minutes. The competitions take place on sunny afternoons (we have been lucky so far) in a dedicated open space on Northeastern University campus.

- **Allowed:**
  - The teams are allowed to interact with their robots using their cell phones (by developing their own control application).
  - The teams are allowed to program their transceivers to *jam* the wireless communication between the mobiles nodes and the gateway over the 2.4GHz frequency. However, jamming the cellular phones frequencies is not allowed. Obviously jamming has an impact on the battery lifetime of the jammers.
  - The teams are allowed to launch *denial of service* attacks on their opponents' network and system infrastructure (e.g., gateway). They can also use cross-technology viruses (e.g., cell phone, gateway, mobile nodes)
  - The teams are allows to use their mobile robots to *physically obstruct* other teams' robots.
- **Not allowed:**
  - The team members are not allowed to physically access the competition arena. The access to the competition arena is restricted to the mobile robots.
  - The teams cannot directly interact with their mobile nodes through the gateway. Only software upgrades are allowed from gateway.

VII. Resources for building the Competition system

The following resources were made available to the students:

- **Material:** microcontrollers (e.g., TI-MSP43), RF chips/boards (e.g., Chipcon), monster-trucks toys, robots (e.g., robosapien V1 and V2),
- **Equipment:** oscilloscope/logical analyzer, RF Spectrum Analyzer, multimeters, and soldering stations.
- **Reference designs:** for ultra-low power TI –MSP430 microcontroller board, RF board, techniques for modifying the robosapiens.
- **Sample code:** for RF communication (ZigBee), networking using GPRS and Bluetooth.
- **Budget:** a small budget is allocated to each team to purchase additional peripherals.

VIII. Lessons Learned

The course is still on-going and will finish at the end of April 2006. The *full* conclusions will be drawn after the main competition. Eleven students enrolled in the class and created three teams. Two teams choose a Robosapian V1 and a Robosapian V2. The third team choose a Lego Mindstorms in addition to the Robosapian V1. All teams where able to interface the sensor nodes with the robots/car and control them. All teams were able to control the robots from their cell phone. The commands are first sent over the Bluetooth link and then propagated through the two hops ZigBee links. The final competition was delayed by one week. One team gave up on implementing the security component while the other two teams are using the AES hardware encryption capability of the Chipcon ZigBee chip.

Preliminary feedback from the students indicated that they are enthusiastic about this type of courses. It allows them to put into practice concepts learned from various disciplines and bridging the gap between mathematics, computer science, and electrical engineering, spanning areas such as wireless communication, network security, cryptography, and robotics. While the amount of work initially looked overwhelming to one team and they were thinking that it is impossible to finish the project within a semester, they were quite happy to see that are able to control their robots over a multi-hop sensor network on WEEK 12. The competition and the possibility to attack other teams made the students aware of many security weaknesses of multi-hop communication systems. This was reflected in the design of the systems but also in the attack strategies.

Figure 3. Teams with their robots.

Figure 4. Two teams choose a Robosapien V1 and a V2. One team choose a Robosapian V1 and a Lego Mindstorm.

During the design presentation, the teams came up with many interesting defense and attack techniques.

A. Attacks

- **Jamming:** scanning channels and continuously jamming the channel.
- **Mimic attack:** replaying packets of teams or of the beacon.
- **Packets fabrication:** against a team that used a weak integrity protection mechanism.
- **Malformed packets:** sending packets with malformed header, or packet length.

B. Defense

- **Channel-hopping:** this is basically a frequency hopping technique to protect against continuous jamming. The channel sequence is cryptographically generated using a pre-shared secret.
- **Cryptographic protection:** packets use sequence numbers and integrity protected based on cryptographic hashing functions (HMAC-SHA1).

C. Competitions

So far, we have run only one part of the competition (no attacks yet). The teams were able to localize the RF-Egg after a non-trivial effort. The robosapian's proved to be extremely slow and the teams using a car as a second robot have a significant advantage. The fluctuations in the RSSI signal require multiple samplings of the beacons signal.

Partial information on the course is available through the course website [1]. A more complete website with movies from the competition, students' presentations, designs, and code will be made available after the final competition.

IX. ACKNOWLEDGMENTS

This course was developed as part of the National Security Agency Information Assurance Scholarship Program at Northeastern University. The author would like to thank Professor Agnes Chan for her support of the course and Yin Wang for his great work as a teaching assistant.

X. REFERENCES

[1] G. Noubir, "SWARM: Secure Wireless Ad Hoc Robots on Mission", Honor Senior Seminar, College of Computer and Information Science, Northeastern University, http://www.ccs.neu.edu/home/noubir/Courses/CSU610/S06.

[2] Sun Microsystems, "J2ME", http://java.sun.com/j2me/.

[3] Bluetooth, http://www.bluetooth.com/bluetooth/.

[4] ZigBee Alliance, http://www.bluetooth.com/bluetooth/.

[5] Moteiv, "tmote sky", http://www.moteiv.com/products-tmotesky.php.

[6] Wow Wee, "Robosapian V1", http://www.robosapienonline.com/.

[7] Wow Wee, "Robosapian V2", http://www.robosapienv2online.com/.

[8] Don Coppersmith, Markus Jakobsson, "Almost Optimal Hash Sequence Traversal", In Proceedings of the Fifth Conference on Financial Cryptography (FC '02), February 2002.

[9] G. Lin, G. Noubir, "On Link Layer Denial of Service in DATA Wireless LANs", in the Wiley Journal on Wireless Communications and Mobile Computing, Wiley, August, 2004.

[10] G. Noubir, "On Connectivity in Ad Hoc Network under Jamming Using Directional Antennas and Mobility", in International Conference on Wired /Wireless Internet Communications, Lecture Notes in Computer Science, Springer-Verlag, 2004.

[11] T. Kaya, G. Lin, G. Noubir, A. Yilmaz, "Secure Multicast Groups on Ad Hoc Networks ", in Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks, 2003.