Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Undergraduate Research in Wireless Sensor Security Course

Sumita Mishra, Yin Pan and Tae (Tom) Oh, *Rochester Institute of Technology*

Abstract – Wireless sensor networks (WSN) are used for military as well as commercial applications due to ease of deployment and low infrastructure cost. WSNs are being introduced for collecting patient data in healthcare and sensitive data in military applications. Hence, sensor security remains a major concern and is a challenging research area in the wireless networking community. In order to provide our undergraduate students an opportunity to exercise his or her creative side before graduation and encourage innovation and creativity, faculty at RIT have developed a course in wireless sensor network security. Our goal is to provide our undergraduate students with research experience and seed their research capability in an emerging networking area. This paper presents the authors' experience in developing an innovative course that will provide students with theoretical, practical as well as research-based knowledge. It discusses the design and methodologies to guide the students to work towards a research problem, implement and test the research ideas in a lab based environment and help them to publish the results.

Index terms – Wireless Security, Undergraduate research, Sensor Network Security

I. Introduction

W*ireless sensor networks* (WSN) are widely used for applications such as environment monitoring, habitat monitoring, forest fire control, border surveillance and health monitoring due to their capability of establishing communications among peer nodes in a self-organizing and adapting manner, without any infrastructure. Nodes in wireless sensor networks act as hosts as well as routers. With their wide-ranging applications and flexibility of deployment, WSNs are expected to be widely deployed in the near future.

One major design challenge in these networks is addressing the "security" needs. Loss of data confidentiality, integrity and availability along with various threats such as routing disruption attacks and resource consumption attacks are major risks associated with wireless communications in sensor networks. Besides the threats and vulnerabilities that exist in wired networks, such networks have additional security risks due to the openness of the wireless medium, lack of central infrastructure and dynamic topology changes. Sensor network security will impact the network considerably due to their ad hoc nature and can render them useless or very dangerous under certain conditions. Because of the sensitivity of data collected by these emerging WSNs, solutions that provide secure, reliable and robust communication among the sensor nodes are required. Being power constrained and sometimes mobile, the communicating nodes in such networks cannot employ complex security algorithms or schemes. The security concerns in WSNs have to be addressed differently due to the type of applications they target and the environment in which they operate. Hence sensor network security is a major research area in the wireless networking community.

We define undergraduate research as faculty-mentored, self-directed project that involves inquiry, research, discovery, and problem solving. Undergraduate research provides a great opportunity for students to expose different facets of science and technology, and develop important skills they need to get into graduate school. Sensor network security, as a relatively new research area, can be introduced to students to stimulate their creative thinking and develop their problem-solving strategies. The course is designed to provide students with theoretical, practical and ***research*** experience and seed our undergraduate students' research capability in an emerging networking area. The course is innovative as the instructors will closely monitor and guide the students to work towards a research problem, implement and test the research ideas in a lab based environment and help them to publish the results. Students will be encouraged to present the findings either in a technical conference or a workshop. This course attempts to exercise RIT President Destler's goal for innovation - "Looking at ways in which our curricula could be modified to encourage innovation and creativity and perhaps offer each student an opportunity to exercise his or her creative side before graduation".
The remainder of this paper is organized as follows. Section II describes the background knowledge needed for this course. The goals and expected outcomes of the course are presented in Section III. Detailed course content and lab designs are presented in section IV. Section V elaborates the course assessment methods followed by Conclusion and References in sections VI and VII respectively.

sumita.mishra@rit.edu, yin.pan@rit.edu, thoics@rit.edu
Department of Networking, Security & Systems Administration

II. BACKGROUND

Wireless Sensor Networks (WSN) pose several security challenges, including key establishment, data secrecy and authentication, robustness to denial-of-service attacks, secure routing, and intrusion detection challenges [1-6]. When implementing network security, we cannot consider security design as a standalone component of the overall system design. Instead, we need to integrate security in every component of the network design [1]. In this course, several WSN security topics are covered. Some of them are described below.

A. Key Management

In order to setup a secure communication framework in wireless sensor networks, one of the initial requirements is to establish cryptographic keys. Several key management protocols exist in literature to address this problem. However, most of these protocols have been proposed for other types of networks and are not practical for WSNs due to the energy and computational limitations of sensor nodes. Also key establishment techniques need to address scalability as some sensor applications have hundreds of nodes collecting data. The communication pattern in WSNs is different compared to traditional networks (convergecast versus peer-to-peer). Hence sensor nodes may need to setup different types of keys with their neighbors and the data collecting nodes (sinks). Development of an efficient key management scheme for WSNs is an open research problem.

B. Authentication and Secrecy

WSNs that are deployed for applications dealing with sensitive data require techniques that protect the data from eavesdropping, injection of spurious data and modification of data. Data encryption can be used to achieve this goal. However, end-to-end encryption requires cryptographic keys to be setup for communication between all nodes in the network. This can be a daunting task for large WSNs. Hence several link layer security frameworks have been proposed for these networks [2-4]. One of the research challenges in this area is to find the balance between software/hardware based cryptographic implementations.

C. Denial of Service (DOS) Attacks

Due to the inherent vulnerabilities of the wireless medium, adversaries can launch DOS attacks on WSNs which can severely hamper their functionality. This can be achieved by jamming the medium with high power signals, constant *Request-to-Send* (RTS) packet transmissions, and simultaneous transmissions [5]. Solutions such as spread-spectrum techniques need to be researched for the sensor network area.

D. Secure Routing

Since sensor nodes act as hosts as well as routers, routing protocols impose unique security vulnerabilities [5]. A malicious node can launch DOS attacks on the routing protocol, preventing all forms of communication between the participating nodes of the WSN. Also, false routing information can be injected in the network, leading to all communication traffic being directed towards the adversaries. Therefore developing secure routing protocols for WSNs is a hot research topic [6].

E. Intrusion Detection

WSNs are vulnerable to many different kinds of intrusion. Detection of these intrusions is challenging due to the lack of centralized control in these networks [7]. In wired networks, network anomalies are monitored at various concentration points of the network. Because of the distributed nature of WSNs and the energy constraints of the sensor nodes, design of a decentralized Intrusion Detection System (IDS) becomes extremely challenging.

Since this course is an upper level undergraduate course, it requires a range of prerequisite knowledge. It is expected that students who take this course have a basic understanding of Wireless Networking concepts and Cryptography. This course was primarily designed for senior students currently pursuing B.S. degrees in Information Security and forensics, Applied Networking and Systems Administration or Information Technology. This course begins with an introduction to wireless sensor networking concepts with emphasis on security. The unique security challenges in the sensor networking area are presented and the concepts are reinforced in a lab-based environment. Students will have a hands-on experience with sensor motes and related security frameworks. They will work on a related research problem identified in consultation with the instructors. The instructors will work with the students closely and guide them in the implementation and testing of the research ideas.

III. GOALS AND EXPECTED OUTCOMES

Presenting the right amount of basic knowledge in sensor security that allows students to start their research in this field is challenging. Before selecting course materials from various books and literature, the authors defined the audience, goals, and expected outcomes for students to achieve.

A. Goals

The goal of this course is to provide students with theoretical, practical and research experience, stimulate students' creative thinking and develop their problem-

solving strategies, and seed our undergraduate students' research capability in an emerging networking area.

This course also supports Networking, Security & System Administration (NSSA) department's B.S. program goals of providing a relevant and innovative curriculum at the forefront of the security field. Specific program goals supported by the course include:

1. Student should be able to communicate effectively with all levels of an organization.

2. Student should be able to analyze and manage security risks from the individual desktop to the enterprise.

3. Student should be able to describe ethical issues and their impact on individuals and the organization.

4. Student should be able to demonstrate knowledge and experience in the issues associated with working in teams and identifying approaches to resolving these issues.

B. Expected Outcomes

Upon completion of this course, students will be able to

1. Synthesize the fundamental networking techniques of wireless sensor networks. Assessed through lab reports and exams.
2. Describe various sensor security issues, identify threats and impacts. Assessed through lab reports and exams.
3. Analyze the performance of the link layer security framework for sensor networks. Assesses through lab reports and exams.
4. Formulate a research plan based on the identified research topics. Assessed through interim reports.
5. Conduct literature search based on the identified research topics. Assessed through interim reports.
6. Present the research findings to the class. Assessed through project presentation.

IV. COURSE DEVELOPMENT

Once the goals and outcomes had been defined, the next step was to determine the information needed to be conveyed to allow students to reach them. This course incorporates lectures, labs and a final project to reach its goal of developing students' research and analytical skills in sensor security.

1. Lecture Material

The authors started their discussions anchored around a series of questions:

1) What fundamental knowledge should students acquire in order to do research in this area?
2) How to help students to start research?
3) Research procedure?
4) How to write a conference and Journal paper?

Even through there is a great amount of knowledge to be covered in the first half quarter [8], the authors all agreed that research methods should be introduced as early as possible. After the introduction section, students will select an interested topic area and start their own research while learning fundamental concepts in class in parallel. The lectures are designed to be covered in six weeks that leaves four weeks for students to work on their papers and presentations.

With these discussions, the course content and materials were modified and finalized.

The detailed topics are listed as follows:

Topics outline:

1) Introduction to Wireless Sensor Networks
   a. Wired versus wireless
   b. Infrastructure-based wireless versus multihop wireless
   c. Medium Access and Routing Challenges
   d. Sensor Hardware, Operating System and Simulation Environment - Mica2 Motes, TinyOS and TOSSIM
   e. Research Methods
      i. Literature Review using search engines, library resources, IEEE & ACM databases
      ii. Simulation versus Experiments versus Analytical Method
2) Security goals, vulnerabilities and attacks in sensor networks
   a. Security Goals
      i. Access Control
      ii. Authentication
      iii. Confidentiality
      iv. Integrity
   b. Vulnerabilities and Attacks
      i. Replay attack
      ii. Denial of Service Attack
      iii. Selective Forwarding
      iv. Sink Hole Attack
      v. Impersonation Attack
      vi. Protocol-specific attacks
3) Link layer security frameworks
   a. TinySec
      i. TinySec Design
      ii. Using TinySec in TinyOS applications
      iii. Limitations
   b. Zigbee

c. MiniSec
d. Triple Keys

4) Key Management in Wireless Sensor Networks
   a. Pair-wise key management
      i. LEAP (Localized Encryption and Authentication Protocol)
      ii. Low-energy key management protocol
   b. Group-wise key management
      i. Hierarchical Key Generation and Distribution Protocol
      ii. Group Key Distribution via local collaboration
   c. Network-wise key management
      i. Multi-tier security
      ii. TESLA
      iii. SPINS

5) Secure Routing
   a. Authenticated TinyOS beaconing
   b. INSENS
   c. Secure Implicit geographic forwarding
   d. Secured directed diffusion

6) Intrusion Detection Mechanisms
   a. IDS challenges in Ad hoc and Sensor Networks
   b. IDS Architectures for WSNs
      i. Neighbor Monitoring
      ii. IDS using Routing Protocols
   c. IDS for Sinkhole attacks and jamming

7) Research and paper
   a. Research proposal
   b. Research design and implementation
   c. Paper presentation

2. Effectiveness of the lecture materials

Lecture materials are an essential part of the development of any curriculum. There were three major elements targeted in the development of these materials:

1) Effectively impart information to students

As with any curriculum development, lecture materials should be effective in helping students absorb the most important material and concepts. To achieve this, the material, described under the Topics outline above, was carefully selected and tailored to directly address the goals and objectives developed for the course.

2) Keep students engaged

Students learn more effectively when they are highly motivated and actively engaged in classroom discussions. Every effort will be put forth to keep students interested. For example, we have scheduled a researcher to talk about her experience of finding a problem, analyzing and solving the problem.
Another element to this end was to develop lectures in multiple formats: some lectures will be presented with slides, some in seminar fashion and others in a question/answer format. This will enable our students to actively participate in the lectures.

3) Incorporate student presentations and paper publication

The final project involves students' research and presentations. Through these activities, they will engage in critical thinking exercises, learn problem-solving techniques, share their innovative ideas and have an opportunity to publish in RIT sponsored workshops and regional IEEE conferences.

3. Lab Development

Labs provide students with the opportunity to understand and apply knowledge obtained from lectures. They also allow students to discover new ideas for their future research. Topics introduced in the lecture, especially the technologies related, are further explored in labs. For example, during the week of lectures covering the link layer security framework, TinySec, students are assigned a lab implementing TinySec to sensors for secure communications. Consequently, we designed four labs and one final project - each directly related to the materials presented in lectures.

Topics of the lab assignments are outlined in Table 1.

Table 1 – Lab topics

Lab 1	Sensor Network basics – Mica2 & TinyOS
Lab 2	Introduction to MoteWorks
Lab 3	Introduction to TinySec and Cryptographic key generation
Lab 4	Implementing Encrypted Communication of sensor data using TinySec

The goal of the labs is to allow students to identify sensor network security threats, sensor networks security challenges in the labs and provide them with hands-on experience in experimenting the existing sensor security solutions.

1) On what sensor modes and technologies do we focus?

As mentioned before, sensor-networks not only inherit the threats and vulnerabilities that exist in wireless networks, but also are more vulnerable to security threats due to the computation and power limitations.
Various sensor network security mechanisms are introduced trying to address the threats in this field. The

leading mechanisms include TinySec from UC Berkley, MiniSec and TripleKeys [2-4]. These mechanisms have their own strength in terms of overheads, strength of the encryption key and the effectiveness against sensor network attacks. All three mechanisms are covered in the lecture.
There are many sensor motes used in the sensor networks including MICA series, mica, m2Dot, Mica2, MicaZ [9] by Crossbow Technology, and Telos[10] by UC Berkley. Since UC Berkeley's TinySec works well with MICA series, the authors decided to use Mica2 so that both Berkley's TinySec and Crossbow's security implementations can be practiced in the course.

Besides providing hands-on experience in real sensor motes, we also designed lab activities using TinyOS mote simulator, TOSSIM. This allows students to effectively design and simulate a scalable wireless sensor network, and help in debugging TinyOS network in their research phase.

2) How do we design the labs?

First lab is designed to provide students with basic knowledge of the sensor kits. Students connect Crossbow's sensor equipment, MIB510 Serial Interface Programming Board, MICA2 Mote and MTS310 Multi Sensor Module, and upload simple programs to sensor motes in TinyOS development environment.

MIB510 Serial Interface Programming Board

MICA2 Mote **MTS310 Multi Sensor Module**

This lab will allow students to use sensors to collect light and temperature data for monitoring energy efficiency in a building. Embedded in this lab will be a study of possible security threats due to wireless monitoring in the buildings. The lab also provides students the opportunity to validate sensor networking theory and help them to identify limitations faced in real life by WSN users.

Second lab introduces Crossbow's sensor networks analysis tools to students. From this lab, students learn how to create a mesh network with more than two sensors, sniff packets in air, and analyze the packets. With this sniffing and analysis functionality, students are able to understand WSNs security threats and investigate new techniques to detect and prevent the threats for their final project. A number of Intrusion Prevention and Intrusion Detection techniques and schemes for WSN security have been proposed in the research literature. A select set of such schemes as identified by the instructors will be explored and evaluated by the students in a realistic environment. Understanding, practicing, comparing and evaluating the effectiveness of these techniques will immensely help the students in gaining practical knowledge of security in WSNs.

Students are introduced to UC Berkley's TinySec in Lab 3. By sniffing and packets analysis, students observe the behavior of encrypted traffic and understand the concept of cryptographic key generation.

Lab 4 focuses on developing students' skills in implementing TinySec with TinyOS. Students will learn TinySec cryptographic key mechanisms and distribution, write programs to communicate encrypted sensor data across wireless sensor networks, and convert an existing program with plaintext communication to encrypted communication using TinySec.

3) How do students setup the labs and save their work?

Imaging servers are used for students to store disk images of work in progress to a personal storage account. This mechanism gives them the option to continue with the lab exercise at a later time.

4) How these labs help students for their research?

After completing these labs, students are able to setup the sensors, monitor and analysis sensor communications, write program to communicate with other sensors securely. These labs provide knowledge and hands-on experience to prepare students for their further research.

4. Research Project

Research and publications in conferences and workshops is one component in the course. The course will be co-taught by faculty members who have research experience in WSN security. The instructors will present real world problems to students and prepare them with the required knowledge via lectures where the research aspects will be discussed. Students will work in groups on a select set of problems identified in consultation with the instructors. They will conduct literature review and present their approaches to the problems at the end of the quarter. Instructors will provide guidance to solve problems and write technical research papers.

The detailed steps of this project assignment are as follows:

1. Select one topic to do a thorough literature review.
2. Identify any limitations of current technologies.
3. Modify or extend functionalities.
4. Share results with classmates for their comments

This project should highly motivate students to conduct research and learn via innovation. Under the supervision of three professors, students will experience new research skills such as conference paper writing and technical paper presentation. Students with such enhanced skills will certainly be more attractive to the wireless networking industry. Some of them may be prospective PhD candidates.

V. Course Assessment

To measure the successfulness of this course, we will use following measurement.
(1) Number of accepted papers in technical conferences or workshops will be a good measure. The instructors will provide information to student on technical conferences and workshops to target. They will assist the students' to submit their papers to conferences.

(2) Student response through regular course evaluations will give us feedback in a timely fashion. As this is the first course of its type, we intend to have regular student feedback and evaluations as the course progresses. We will also collect students' ideas, concerns, and suggestions, and their feedback on the research component of the course. We will track students' progress through classroom discussions on the research project as it evolves to help the faculty tailor the research requirements of the course and address concerns in time.

(3) We also plan to trace these students' future path to find out the number of students who enroll in MS programs or PhD programs. This will evaluate the effectiveness of introducing research in our undergraduate curriculum.

VI. Conclusion

This paper presents the author's experience in developing a research oriented course based on wireless sensor security. The course has been listed as a core course for BS degree of the Information Security and Forensics in the department of Networking, Security, and System Administration. It will be first taught in spring of 2009. The course content, labs and research innovation have been discussed in detail. We believe that this course will be a role model for introducing research into the networking curriculum in one of the foremost research areas in Networking. The authors hope that this paper will encourage and help other educators to introduce similar research oriented courses and activities in their undergraduate curriculum.

Acknowledgements

The authors would like to acknowledge Kristian Stokes, a graduate student in the NSSA department, who has made substantial contributions to the lab designs for this course.

VII. References

[1] Perrig, Adrian, John Stankovic, and David Wagner. Security in Wireless Sensor Networks. *Communications of the ACM, Volume 47, Issue 6* (June 2004): 53-57.
[2] C. Karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, *SenSys'04*, 2004.
[3] Tanveer Zia and Albert Zomaya, A Secure Triple-Key Management Scheme for Wireless Sensor Networks, *INFOCOM,* 2006.
[4] Mark Luk, Ghita Mezzour, Adrian Perrig and Virgil Gligor, MiniSec: A Secure Sensor Network Communication Architecture, *Information Processing in Sensor Networks,* 2005.
[5] Wood, A.D. and J.A. Stankovic. Denial of Service in Sensor Networks. *IEEE Computer,* October 2002.
[6] Karlof, C. and Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications,* May 2003.
[7] Perrig, Adrian, Robert Szewczyk, Victor Wen, David Culler, and J.D. Tygar, SPINS: Security protocols for sensor networks, *The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001),* 2001.
[8] Cayirci E., Rong C., Security in Wireless Ad Hoc and Sensor Networks, John Wiley & Sons, 2009.
[9] Crossbow's sensor motes: http://www.xbow.com/Products/productdetails.aspx?sid=156
[10]Polastre, J. Szewczyk, R. Culler, D., Telos: enabling ultra-low power wireless research, *Information Processing in Sensor Networks*, 2005.