School of Information Technology and Engineering (SITE)

Minutes of the First Doctoral Committee meeting held on 1st April 2017 at 12.30 pm , Venue : SITE Discussion Room

Research Scholar   : Ms. Ashwini B Abhale
School   : SITE
Category   : External Part Time (EPT) - Ph.D
Register Number   : 16PHD0645
Field of Investigation : Wireless Network Security
Topic of Research   : The Prevention Model for Anomaly Based Intrusion
                          Detection System in Wireless Sensor Network

Dr. Aswani Kumar Cherukuri   Chairman & Convener
Dean, School of Information Technology and Engineering
VIT University, Vellore- 632014.

Dr. S. S. Manivannan   Guide
School of Information Technology and Engineering
VIT University, Vellore- 632014.

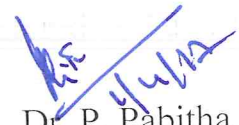Dr. A. Kannan   External Member
Dept of Information Science and Technology
College of Engineering
Anna University, Chennai-600025.

Dr.P. Pabitha,   External Member
Department of Computer Technology,
Madras Institute of Technology,
Anna University, Chennai-600044.
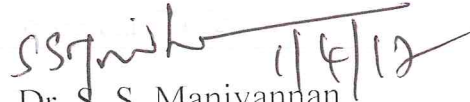
Dr. Dinakaran M,   Internal Member
School of Information Technology and Engineering
VIT University, Vellore- 632014.

- Convener welcomed all the DC members.
- Candidate was asked to give a brief presentation about the work carried out so far.
- Candidate presented her work on "The Prevention Model for Anomaly Based Intrusion Detection System in Wireless Sensor Network"

- The DC committee suggested the following courses
    1) RES 701 – Research Methodology
    2) Hacking and Intrusion Detection Methods
    3) Wireless Sensor Network and Security
    4) Machine Learning - Coursera Online Course

- RES 701 – Research Methodology course is registered in the current semester.

- Hacking and Intrusion Detection Methods course to be carried out as Self Study mode under the supervision of guide.

- Wireless Sensor Network and Security course to be carried out as Self Study mode under the supervision of guide.

- Machine Learning course to be carried out as online course in Coursera tool.

Dr. A. Kannan
External DC Member

Dr. P. Pabitha
External DC Member

Dr. Dinakaran M
Internal DC Member

Dr. S. S. Manivannan
Guide

Dr. Aswani Kumar Cherukuri
Dean & Convener
School of Information Technology and Engineering
VIT University, Vellore- 632014.

Research Methodology

L	T	P	C
3	0	0	3

COURSE CODE: RES 701

Objectives

1. To gain insights into how scientific research is conducted.
2. To help in critical review of literature and assessing the research trends, quality and extension potential of research and equip students to undertake research.
3. To learn and understand the basic statistics involved in data presentation.
4. To identify the influencing factor or determinants of research parameters.
5. To test the significance, validity and reliability of the research results.
6. To help in documentation of research results.

Expected Outcome

1. Ability to critically evaluate current research and propose possible alternate directions for further work
2. Ability to develop hypothesis and methodology for research
3. Ability to comprehend and deal with complex research issues in order to communicate their scientific results clearly for peer review.

UNIT I
Introduction to Research Methods

Philosophy of Science, Evolutionary Epistemology, Scientific Methods, Hypotheses Generation and Evaluation, Code of Research Ethics, Definition and Objectives of Research, Various Steps in Scientific Research, Types of Research; Research Purposes - Research Design - Survey Research - Case Study Research.

UNIT II
Data Collection and Sampling Design

Sources of Data: Primary Data, Secondary Data; Procedure Questionnaire- Survey and Experiments – Design of Survey and Experiments - Sampling Merits and Demerits - Control Observations - Procedures - Sampling Errors.

UNIT III
Statistical Modeling and Analysis, Time Series Analysis

Probability Distributions, Fundamentals of Statistical Analysis and Inference, Multivariate methods, Concepts of Correlation and Regression, Fundamentals of Time Series Analysis and Spectral Analysis, Error Analysis, Applications of Spectral Analysis.

UNIT IV
Evolutionary Algorithms

Introduction to evolutionary algorithms - Fundamentals of Genetic algorithms, Simulated Annealing, Neural Network based optimization, Optimization of fuzzy systems.

UNIT V

Research Reports

Structure and Components of Research Report, Types of Report, Layout of Research Report, Mechanism of writing a research report

Text Book
    1. C.R. Kothari, Research Methodology Methods and Techniques, 2/e, Vishwa Prakashan, 2006.

Reference Books
1. Richard I Levin amp; David S.Rubin, Statistics for Management, 7/e. Pearson Education, 2005.
2. Donald R. Cooper, Pamela S. Schindler, Business Research Methods, 8/e, Tata McGraw-Hill Co. Ltd., 2006.
3. U.K. Srivastava, G.V. Shenoy and S.C. Sharma – Quantitative Techniques for managerial decisions, New Age International, Mumbai, 2005.
4. William G. Zikmund, Business Research Methods, Thomson, 2006.
5. D.M.Pestonjee, (Ed.) Second Handbook of Psychological and Social Instruments, Concept Publishing, New Delhi, 2005.

Mode of Evaluation: Evaluation by the course teacher – Continuous Assessments 1 and 2 (50% marks) / Term end examination (50% Marks).

Hacking & Intrusion Detection Methods (Self Study)

Unit 1   Web Based Hacking

Popular Web Servers Security Threats, Apache Vulnerability, Attack against IIS Console, Hacking Tools, Web Application Hacking, Web Application Threats, Web Based Password Cracking Techniques.

Unit 2   Wireless Network Hacking

Rogue Access Points, Tools to Generate Rogue Access Points, Scanning Tools, Securing Wireless Networks, Session Hijacking, Spoofing Vs Hijacking, Steps in Session Hijacking, Types of Session Hijacking, Protection against Session Hijacking

Unit 3   Wireless Intrusion Detection

Wireless IDS Architecture, Incident Response, Physical response, policy enforcement, Locating APs, Identification of Rogue APs, vulnerabilities of wireless networks

Unit 4   Network Layer Attack & Defense

Network attacks - Smurf, DoS, DDoS, Spoofing , Session Hijack and Routing attacks Network layer attack defense methods - Packet filtering, Encryption Protocols.

Unit 5 Application Layer Attack & Defense

Buffer Overflow attacks- Stack and Heap buffer overflow attacks, Web application and session hijack attacks. Defense methods – Creating Strong Session IDs, server supplied session IDs, Static Routing table, Two way authentication.

Text Books:

1. Hacking: The Art of Exploitation, Jon Erickson, 2nd Edition, No Starch Press, 2008
2. Practical Hacking Techniques and Countermeasures, Mark D. Spivey, Auerbach Publications Taylor & Francis Group, 2007
3. Hacking Techniques in Wireless Networks, PrabhakerMateti, Wright State University Press, 2007.
4. Intrusion detection systems with Snort: advanced IDS techniques, Rafeeq Ur Rehman, Pearson Education publishing as Prentice Hall, 2003.
5. Network Intrusion Detection, Stephen Northcutt, Judy Novak, New Riders publisher, 2003.
6. Implementing Intrusion Detection Systems: a hand on guide for securing network, Tim Crothers, Wiley Publications, 2002.

Wireless Sensor Networks and Security (Self Study)

Unit 1: Overview Of Wireless Sensor Networks

Introduction to Wireless Sensor Networks, Challenges for Wireless Sensor Networks, Enabling Technologies for Wireless Sensor Networks.

Unit 2: Architectures

Single-Node Architecture - Hardware Components, Energy Consumption of Sensor Nodes , Operating Systems and Execution Environments, Network Architecture -Sensor Network Scenarios, Optimization Goals and Figures of Merit, Gateway Concepts.

Unit 3: Overview of Wireless SensorNetwork Security

Security Goals in Sensor Networks, Threats in WSN, Security on Hardware Layer, Security Primitives, WSN Framework : "key pool" framework, mathematical framework, negotiation framework, and public key framework, Services : Trust Management, Intrusion Detection, Privacy Protection.

Unit 4: Vulnerabilities and Attacks in WirelessSensor Networks

Introduction, Security Goals in Sensor Networks,Attacking Wireless Sensor Networks,Implementation of AES,Digital Signature Schemes : ECDSA,RSA, Rabin and DSA Signatures,One-time signature schemes,Authenticated Key Establishment, Protocols for Authentication.

Unit 5: Intrusion Detection Techniques in SensorNetworks

Introduction, Wireless Sensor Network IDS Challenges, Wireless Sensor Networks Attacks,Wireless Sensor Network Intrusion Detection,Requirements for Intrusion Detection in Sensor Networks.IDS for Specific Intrusions and Operations.

Text Book

1. Holger Karl & Andreas Willig, "Protocols And Architectures for Wireless Sensor Networks" , John Wiley, 2005.
2. Feng Zhao & Leonidas J. Guibas, "Wireless Sensor Networks- An Information Processing Approach", Elsevier, 2007.
3. KazemSohraby, Daniel Minoli, &TaiebZnati, "Wireless Sensor Networks- Technology, Protocols, And Applications", John Wiley, 2007.
4. J. Lopez and J. Zhou (Eds.), Wireless Sensor Network Security, IOS Press, 2008.

Machine Learning
(Coursera Online Course ByStanford University)

About this course: Machine learning is the science of getting computers to act without being explicitly programmed. In the past decade, machine learning has given us self-driving cars, practical speech recognition, effective web search, and a vastly improved understanding of the human genome. Machine learning is so pervasive today that you probably use it dozens of times a day without knowing it. Many researchers also think it is the best way to make progress towards human-level AI. In this class, you will learn about the most effective machine learning techniques, and gain practice implementing them and getting them to work for yourself. More importantly, you'll learn about not only the theoretical underpinnings of learning, but also gain the practical know-how needed to quickly and powerfully apply these techniques to new problems. Finally, you'll learn about some of Silicon Valley's best practices in innovation as it pertains to machine learning and AI. This course provides a broad introduction to machine learning, datamining, and statistical pattern recognition. Topics include: (i) Supervised learning (parametric/non-parametric algorithms, support vector machines, kernels, neural networks). (ii) Unsupervised learning (clustering, dimensionality reduction, recommender systems, deep learning). (iii) Best practices in machine learning (bias/variance theory; innovation process in machine learning and AI). The course will also draw from numerous case studies and applications, so that you'll also learn how to apply learning algorithms to building smart robots (perception, control), text understanding (web search, anti-spam), computer vision, medical informatics, audio, database mining, and other areas.

Syllabus

WEEK 1

Introduction

Welcome to Machine Learning! In this module, we introduce the core idea of teaching a computer to learn concepts using data—without being explicitly programmed. The Course Wiki is under construction. Please visit the resources tab for the most complete and up-...

5 videos, 10 readings

- Graded: Introduction

Linear Regression with One Variable

Linear regression predicts a real-valued output based on an input value. We discuss the application of linear regression to housing price prediction, present the notion of a cost function, and introduce the gradient descent method for learning.

7 videos, 8 readings

- Graded: Linear Regression with One Variable

Linear Algebra Review

This optional module provides a refresher on linear algebra concepts. Basic understanding of linear algebra is necessary for the rest of the course, especially as we begin to cover models with multiple variables.

6 videos, 1 reading, 1 reading

WEEK 2

Linear Regression with Multiple Variables

What if your input has more than one value? In this module, we show how linear regression can be extended to accommodate multiple input features. We also discuss best practices for implementing linear regression.

8 videos, 16 readings

- Graded: Linear Regression with Multiple Variables

Octave/Matlab Tutorial

This course includes programming assignments designed to help you understand how to implement the learning algorithms in practice. To complete the programming assignments, you will need to use Octave or MATLAB. This module introduces Octave/Matlab and shows yo...

6 videos, 1 reading

Graded: Octave/Matlab Tutorial

WEEK 3

Logistic Regression

Logistic regression is a method for classifying data into discrete outcomes. For example, we might use logistic regression to classify an email as spam or not spam. In this module, we introduce the notion of classification, the cost function for logistic regr...

7 videos, 8 readings

- Graded: Logistic Regression

Regularization

Machine learning models need to generalize well to new examples that the model has not seen in practice. In this module, we introduce regularization, which helps prevent models from overfitting the training data.

4 videos, 5 readings

- Graded: Regularization

WEEK 4

Neural Networks: Representation

Neural networks is a model inspired by how the brain works. It is widely used today in many applications: when your phone interprets and understand your voice commands, it is likely that a neural network is helping to understand your speech; when you cash a ch...

7 videos, 6 readings

- Graded: Neural Networks: Representation

WEEK 5

Neural Networks: Learning

In this module, we introduce the backpropagation algorithm that is used to help learn parameters for a neural network. At the end of this module, you will be implementing your own neural network for digit recognition.

8 videos, 8 readings

- Graded: Neural Networks: Learning

WEEK 6

Advice for Applying Machine Learning

Applying machine learning in practice is not always straightforward. In this module, we share best practices for applying machine learning in practice, and discuss the best ways to evaluate performance of the learned models.

7 videos, 7 readings

- Graded: Advice for Applying Machine Learning

Machine Learning System Design

To optimize a machine learning algorithm, you'll need to first understand where the biggest improvements can be made. In this module, we discuss how to understand the performance of a machine learning system with multiple parts, and also how to deal with skewe...

5 videos, 3 readings

- Graded: Machine Learning System Design

WEEK 7

Support Vector Machines

Support vector machines, or SVMs, is a machine learning algorithm for classification. We introduce the idea and intuitions behind SVMs and discuss how to use it in practice.

6 videos, 1 reading

- Graded: Support Vector Machines

WEEK 8

Unsupervised Learning

We use unsupervised learning to build models that help us understand our data better. We discuss the k-Means algorithm for clustering that enable us to learn groupings of unlabeled data points.

5 videos, 1 reading

- Graded: Unsupervised Learning

Dimensionality Reduction

In this module, we introduce Principal Components Analysis, and show how it can be used for data compression to speed up learning algorithms as well as for visualizations of complex datasets.

7 videos, 1 reading

- Graded: Principal Component Analysis

WEEK 9

Anomaly Detection

Given a large number of data points, we may sometimes want to figure out which ones vary significantly from the average. For example, in manufacturing, we may want to detect defects or anomalies. We show how a dataset can be modeled using a Gaussian distributi...

8 videos, 1 reading

- Graded: Anomaly Detection

Recommender Systems

When you buy a product online, most websites automatically recommend other products that you may like. Recommender systems look at patterns of activities between different users and different products to produce these recommendations. In this module, we introd...

6 videos, 1 reading

- Graded: Recommender Systems

WEEK 10

Large Scale Machine Learning

Machine learning works best when there is an abundance of data to leverage for training. In this module, we discuss how to apply the machine learning algorithms with large datasets.

6 videos, 1 reading

- Graded: Large Scale Machine Learning

WEEK 11

Application Example: Photo OCR

Identifying and recognizing objects, words, and digits in an image is a challenging task. We discuss how a pipeline can be built to tackle this problem and how to analyze and improve the performance of such a system.

5 videos, 1 reading

- Graded: Application: Photo OCR