Protecting Wireless Sensor Networks from Internal Attacks

Muhammad Raisuddin Ahmed
Faculty of Education, Science, Technology and Mathematics
University of Canberra, ACT 2601, Australia

Thesis submitted in partial fulfilment of the requirements for the
Degree of Doctor of Philosophy
May 2014
Abstract

Recently, technological advances in the design of processors, memory and radio communications have propelled an active interest in the area of distributed sensor networking, in which a number of independent, self-sustainable nodes collaborate to perform information gathering and processing in real time. Networks of such devices are commonly referred to as Wireless Sensor Networks (WSNs), which are envisioned as a bridge between the modern broadband packet data networks and the physical world. WSNs have made possible real-time data aggregation and analysis on an unprecedented scale. Naturally, they have attracted attention and garnered widespread appeal towards applications in diverse areas including disaster warning systems, environment monitoring, health care, safety and strategic areas such as defence reconnaissance, surveillance, and intruder detection.

Due to the distributed nature, multi-hop communications and their deployment in remote areas, WSNs are vulnerable to numerous security threats that can adversely affect performance. Therefore, to ensure the functionality of WSNs, security is the first and foremost concern in almost all wireless sensor networking scenarios. WSN mechanisms cannot at present ensure that an attack will not be launched. For example, using a compromised node an adversary could perform an attack acting as a legitimate node of the network to acquire all the information. Such attacks are known as internal attacks. Therefore, it is important to protect the wireless sensor network from internal attacks, which is the purpose of this thesis.

This thesis investigates internal security issues in wireless sensor networks (WSNs) and proposes relevant solutions. The development of multi-stage mechanisms to protect WSNs from internal attacks is performed. The major contributions of this thesis to prevent internal attacks are summarised below.
Initially, this thesis developed misbehaviour identification mechanisms with multi agents through timing control, the pairwise key method and cosine similarity based on the abnormal behaviour identification method (ABIM). It is a fast, robust mechanism, and also gives good results when data sets are distinct or well separated from each other.

Secondly, this research investigated and took the advantage of the Dempster-Shafer theory (DST) to develop a novel algorithm for protecting WSNs from internal attacks. This algorithm observes neighbour nodes in a WSN and uses parameters to make judgments for the behaviour based on the DST. The DST considers the observed data as a hypothesis. If there is uncertainty about which hypothesis the data fits best, the DST makes it possible to model several single pieces of evidence within the relations of multi hypotheses. Using this method the system does not need any prior knowledge of the pre-classified training data of the nodes in a WSN.

Thirdly, this work extended the algorithm of the Markov Chain Monte Carlo (MCMC) – Metropolis-Hasting (MH) to our research to detect internal attacks on WSNs. With the MCMC method, it is possible to generate samples from an arbitrary posterior density and to use these samples to approximate expectations of quantities of interest. Moreover, it works in real time by constricting the sample chain and computes the changes together with an acceptance ratio. The new algorithm can decide the internal attacker based on the acceptance ratio.

This work used the fourth generation programming language MATLAB and Java based development J-Sim for simulations. The simulation results show that the algorithm for the detection of the internal attacks is effective. In a simulation, the accuracy of detection in one hop communication, in the three stages, is between 75% and 95% based on the percentage of the compromised node. The accuracy of detection is higher for compromised nodes less than 10% even though the system does not survive if the compromised node is more than 50%.
To my daughter Sarvia Rameen Ahmed
Acknowledgements

For the thesis support and encouragement comes from several sources in various ways. In particular, I would like to thank Professor Xu Huang for accepting me as a Ph.D. student at University of Canberra under his supervision. Prof. Xu always provided me with encouragement, support and sufficient room to think and grow. His understanding and advice have been crucial factors in the successful completion of this work. I consider myself really fortunate to have him as my guide and advisor. I would also like to express my deep-felt gratitude to my co-supervisor, Professor Dharmendra Sharma, for his advice and encouragement.

In addition I would like to thank our collaborators, Associate Professor Hongyan Cui from University of Posts and Telecommunications, China and Professor Li Shutao from Hunan University, China for their advice and support.

I am indebted to my family for their love, advice and support throughout my PhD study, to my mother for her constant encouragement and to my wife for her unlimited love support and understanding throughout the journey.
Contents

List of Figures ......................................................................................................................... xv

List of Tables ............................................................................................................................ xvii

Abbreviations .......................................................................................................................... xix

List of Publications from PhD Research ................................................................................... xxi

Chapter 1  Introduction ............................................................................................................. 1

  1.1 Motivation ......................................................................................................................... 2

  1.1.1 Motivation summary ..................................................................................................... 7

  1.2 Contribution ...................................................................................................................... 7

  1.3 Thesis Structure ................................................................................................................. 8

Chapter 2  Literature Review ................................................................................................... 11

  2.1 Wireless Sensor Networks ............................................................................................... 12

  2.2 Characteristics of WSNs ................................................................................................. 17

  2.3 Architecture of WSNs ...................................................................................................... 20

    2.3.1 Objectives of Architecture Design ............................................................................ 20

    2.3.2 WSNs Architecture .................................................................................................... 21

  2.4 Protocols of WSNs .......................................................................................................... 25

  2.5 Applications of WSNs ...................................................................................................... 27

  2.6 Existing Hardware Platform ........................................................................................... 28

  2.7 Network Security ............................................................................................................. 28

    2.7.1 Threats in WSNs ........................................................................................................ 29

    2.7.2 Generic Security Requirements ................................................................................ 32

    2.7.3 Security Challenges .................................................................................................. 33

    2.7.4 Nature and Types of Internal Attacks ........................................................................ 35
2.8 Suggestions in the Literature to Secure WSNs from Internal Attacks...... 41
2.9 Proposed Method......................................................................................... 50
2.10 Summary................................................................................................. 50

Chapter 3  Misbehaviour Identification............................................................. 53
3.1 System Model............................................................................................ 54
3.2 Sensing Model........................................................................................... 54
3.3 Multi-Agent Based..................................................................................... 57
3.4 Pair Wise Key Based ................................................................................. 67
3.5 Cosine Similarity Based ............................................................................ 73
  3.5.1 Dot Product ......................................................................................... 73
  3.5.2 Cosine Similarity ................................................................................ 74
  3.5.3 WSNs Implementation ........................................................................ 76
3.4 Summary .................................................................................................... 81

Chapter 4  Epistemic Uncertainties Decision..................................................... 83
4.1 Concepts of Dempster-Shafer Theory ......................................................... 85
  4.1.1 Bayesian Interface................................................................................ 85
  4.1.2 Dempster-Shafer Theory of Evidence Method ..................................... 88
4.2 Case Study and Implementation................................................................. 94
  4.2.1 Algorithm and Simulation.................................................................... 97
4.3 Summary .................................................................................................... 100

Chapter 5  Statistical Decision ........................................................................ 103
5.1 Bayesian Interface..................................................................................... 105
5.2 Monte Carlo Integration........................................................................... 107
5.3 Markov Chains......................................................................................... 108
5.4 Markov Chain Monte Carlo Sampling ..................................................... 112
List of Figures

Figure 1-1 : The complexity of WSNs ................................................................. 4
Figure 2-1 : A typical WSN ..................................................................................... 13
Figure 2-2 : Structure of a sensor node ................................................................. 22
Figure 2-3 : Protocol stack of WSNs ................................................................. 24
Figure 2-4 : Routing protocols of WSNs ................................................................. 26
Figure 3-1 : The model of a typical wireless sensor network environment .......... 58
Figure 3-2: Construction of a target node .............................................................. 60
Figure 3-3: Construction of a sink node ................................................................. 60
Figure 3-4: Construction of a sensor node (dashed line) ....................................... 61
Figure 3-5: Multi-agent system to control sink node sleeping and opening time 63
Figure 3-6: Simulation result with two target nodes and the transmission rate is one unit (normalized) ................................................................. 64
Figure 3-7: Simulation result with three target nodes and the transmission rate is one unit (normalized) ................................................................. 65
Figure 3-8: Simulation result with two target nodes and the transmission rate is three units (normalized) ................................................................. 65
Figure 3-9: Sink node opening window ................................................................. 66
Figure 3-10: Chart of the “normalized average delivery rate” vs. “percentage compromised nodes.” ................................................................. 71
Figure 3-11: Normalized resiliency degree ............................................................ 72
Figure 3-12: The projection of the vectors .............................................................. 74
Figure 3-13: Concept of implementation ............................................................... 76
Figure 3-14: Sensor field with abnormal node detection ....................................... 80
Figure 4-1: Three neighbours observing the attacker with one hop distance ..... 86
Figure 4.2: Measure of belief and plausibility ....................................................... 91

Figure 4.3: Three neighbours observing the attacker with one hop ....................... 94

Figure 4.4: Observation of node $A$ by $X, Y, \text{ and } Z$ .................................................. 99

Figure 4.5: Observation of node $E$ by $X', Y'$ and $Z'$ .......................................... 100

Figure 5.1: The graph of transition matrix ............................................................. 111

Figure 5.2: MCMC-MH based node acceptance ratio ............................................. 117
List of Tables

Table 2·1 : WSNs vs Wireless ad Hoc networks .................................................... 16
Table 2-2 : Sensor Platforms .................................................................................. 33
Table 2-3 : Layer Based Security Attacks .............................................................. 36
Table 2-4 : Layer Based DoS Attacks ..................................................................... 37
Table 3-1: The highest SNR with different cases .................................................. 66
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABIM</td>
<td>Abnormal Behaviour Identification Mechanism</td>
</tr>
<tr>
<td>ADC</td>
<td>Analog to Digital Converter</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CSIRO</td>
<td>Commonwealth Scientific and Industrial Research Organisation</td>
</tr>
<tr>
<td>DAC</td>
<td>Digital to Analog</td>
</tr>
<tr>
<td>DARPA</td>
<td>Defence Advanced Projects Research Agency</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DST</td>
<td>Dempster Shafer Theory</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>HIDS</td>
<td>Hybrid Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IIDS</td>
<td>Integrated Intrusion Detection System</td>
</tr>
<tr>
<td>IHIDS</td>
<td>Integrated Hybrid Intrusion Detection System</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>LEACH</td>
<td>Low Energy Adaptive Clustering Hierarchy</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MAS</td>
<td>Multi Agent System</td>
</tr>
<tr>
<td>MCMC</td>
<td>Markov Chain Monte Carlo</td>
</tr>
<tr>
<td>MH</td>
<td>Metropolis–Hastings</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Outputs</td>
</tr>
<tr>
<td>MIPS</td>
<td>Million Instructions Per Second</td>
</tr>
<tr>
<td>OFDMA</td>
<td>Orthogonal Frequency-Division Multiplexing</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>RTT</td>
<td>Round Trip Time</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal to Noise Ratio</td>
</tr>
<tr>
<td>SOSUS</td>
<td>Sound Surveillance System</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SVM</td>
<td>Support Vector Machine</td>
</tr>
<tr>
<td>TEEN</td>
<td>Threshold sensitive Energy Efficient sensor Network protocol</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>WAMR</td>
<td>Wireless Automatic Meter Reading</td>
</tr>
<tr>
<td>WSNs</td>
<td>Wireless Sensor Networks</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
</tr>
</tbody>
</table>
List of Publications from PhD Research

This Thesis is a monograph, which contains some unpublished material, but is mainly based on the following publications during my PhD research.

Conferences:


7. X. Huang, D. Sharma, M. Ahmed, H. Cui “Protecting an WSN from Internal Attack Based on Epistemic Uncertainties,” The 18th IEEE


Journals:

