COMPUTATIONAL INTELLIGENT MECHANISM FOR BOOSTING CLUSTER-BASED WSN SECURITY

A THESIS
SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN NETWORK SECURITY

BY
MOHAMED MAHDI SAIF ALSULTAN ALQAHTANI

TO
NETWORK SECURITY DEPARTMENT
THE COLLEGE OF COMPUTER AND INFORMATION SECURITY
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES

SUPERVISED BY
PROF. MOSTAFA G. M. MOSTAFA
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES

APRIL 2018
# Table of Contents

Abstract .......................................................................................................................... iv
Publication ....................................................................................................................... vi
Dedication ....................................................................................................................... vii
Acknowledgments ......................................................................................................... viii
Table of Contents .......................................................................................................... ix
List of Figures ............................................................................................................... xi
List of Tables ................................................................................................................ xii
List of Abbreviations ................................................................................................... xiii

1 Introduction ................................................................................................................ 1
   1.1 Overview ............................................................................................................. 1
   1.2 Research Goals ................................................................................................. 3
   1.3 Research Motivations ....................................................................................... 4
   1.4 Research Objectives ........................................................................................ 5
   1.5 Research Problems ........................................................................................... 5
   1.6 Research Questions .......................................................................................... 6
   1.7 Research Contributions .................................................................................... 7
   1.8 Research Structure .......................................................................................... 7

2 Background and Literature Review ........................................................................... 9
   2.1 Introduction ....................................................................................................... 9
   2.2 Definitions ........................................................................................................ 10
   2.3 Some of WSNs Threats and Possible Countermeasures to Mitigates ............... 12
   2.4 Trust in WSNs .................................................................................................. 14
       2.4.1 Node Trust Models .................................................................................... 14
       2.4.2 Data Trust Models .................................................................................... 16
       2.4.3 Trust Models to Secure Routing Protocols .............................................. 17
       2.4.4 Trust Models to Secure Data Aggregation .............................................. 18
   2.5 Computation Intelligence of Trust in WSNs ...................................................... 19
       2.5.1 Artificial Neural Networks (ANN) ............................................................. 19
       2.5.2 Evolutionary Computation (EC) ................................................................. 20
       2.5.3 Swarm Intelligence (SI) .......................................................................... 20
       2.5.4 Artificial Immune System (AIS) ................................................................. 21
       2.5.5 Fuzzy Logic Systems (FS) ....................................................................... 21
       2.5.6 Hybrid Paradigms ..................................................................................... 22
   2.6 Cluster-based Trust Models in WSNs ................................................................. 23
       2.6.1 Security Versions of Cluster-based Routing Protocol ............................. 24
       2.6.2 Power Consumption in Cluster-based Schemes ....................................... 24
   2.7 Summary ............................................................................................................ 27
3 The Proposed Methodology ...
3.1 Introduction ...
3.2 Trust Rating Parameters ...
3.2.1 Ability ...
3.2.2 Benevolence ...
3.2.3 Integrity ...
3.3 The Proposed Method ...
3.4 A Fuzzy Trust Rating Module ...
3.5 The Proposed Algorithm ...
3.6 Node Isolation Module ...
3.6.1 Artificial Immune System ...
3.6.2 WADS Technique ...
4 Results and Discussions ...
4.1 Implementation Environment ...
4.2 Simulation Experiments ...
4.3 Simulation Results ...
4.3.1 Detection and Classification ...
4.3.2 Isolation of Malicious Node ...
4.3.3 Discussions ...
4.4 Performance Analysis ...
4.4.1 Reliability ...
4.4.2 Scalability ...
4.5 Robustness ...
4.6 Security Analysis ...
5 Conclusions and Future Work ...
5.1 Conclusion ...
5.2 Limitations of the Current Work ...
5.3 Future Work ...
References ...
List of Figures

Figure 1: The Compound Annual Market Growth Rate (CAGR) for WSNs (Hatler et al., 2017). 4
Figure 2: Cluster-based topology....................................................................................... 26
Figure 3: Consensus-Aware Socio-psychological Algorithm ............................................... 27
Figure 4: Architecture of the Proposed Solution .................................................................. 31
Figure 5: Membership Function for a) input I, b) input B, C) input A and d) output Trust ....... 32
Figure 6: Trust Rating Module Process .................................................................................. 35
Figure 7: Proposed Algorithm ............................................................................................... 36
Figure 8: Example of Antigen vs Antibody (Rathore, Badarla et al. 2016) ......................... 38
Figure 9: Network A, 24 nodes, 50x50m^2 ............................................................................. 43
Figure 10: Network B, 24 nodes, 100x100 m^2 ................................................................. 43
Figure 11: Network C, 64 nodes, 100x100 m^2 ..................................................................... 44
Figure 12: Gaussian Random Distribution .......................................................................... 45
Figure 13: Trust vs Time....................................................................................................... 54
List of Tables

Table 1: Most Known WSNs Threats & Some Countermeasures ............................................................. 12
Table 2: Reasons Behind The Results Along With Possible Trust Rate ................................................ 33
Table 3: Threshold of Distance $d_0$ in Networks A, B and C .............................................................. 41
Table 4: Simulation Parameters Setting .................................................................................................. 44
Table 5: Network A, Detection Accuracy Due to Ability Decrease ......................................................... 46
Table 6: Network A, Detection Accuracy Due to Benevolence Sudden Change ...................................... 47
Table 7: Network B, Detection Accuracy Due to Ability Decrease ......................................................... 48
Table 8: Network C, Detection Accuracy Due to Ability Decrease ......................................................... 48
Table 9: Network C, Detection Accuracy Due to Benevolence Sudden Change ...................................... 49
Table 10: Network B, Detection Accuracy Due to Benevolence Sudden Change .................................... 50
Table 11: Isolation Module Analysis ....................................................................................................... 51
Table 12: Comparisons of Consensus-Aware algorithm & Proposed Algorithm ..................................... 52
Table 13: Reliability Assessment ........................................................................................................... 53
Table 14: Comparisons of Model A vs Model B ..................................................................................... 55
Table 15: Comparisons of Model B vs Model C ..................................................................................... 56
Table 16: Life Time of All Models ........................................................................................................ 56
Table 17: Robustness of Proposed Model ............................................................................................... 57
Table 18: Analysis of Models Resestances Against Attacks ................................................................. 57
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Explanations</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LoWPAN</td>
<td>Low-Power Wireless Personal Area Networks</td>
</tr>
<tr>
<td>A</td>
<td>Ability</td>
</tr>
<tr>
<td>AIS</td>
<td>Artificial Immune System</td>
</tr>
<tr>
<td>ANN</td>
<td>Artificial Neural Network</td>
</tr>
<tr>
<td>B</td>
<td>Benevolence</td>
</tr>
<tr>
<td>BTRM</td>
<td>Bio-inspired Trust Reputational Model</td>
</tr>
<tr>
<td>CAGR</td>
<td>Compound Annual Growth Rate</td>
</tr>
<tr>
<td>CH</td>
<td>Cluster Head</td>
</tr>
<tr>
<td>CI</td>
<td>Computational Intelligence</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity and Availability</td>
</tr>
<tr>
<td>CMs</td>
<td>Cluster Members</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Multiple Access</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DRBTS</td>
<td>Distributed Reputation Beacon Trust System</td>
</tr>
<tr>
<td>EC</td>
<td>Evolutionary Computation</td>
</tr>
<tr>
<td>EGT</td>
<td>Evolutionary Game Theory</td>
</tr>
<tr>
<td>EPFR</td>
<td>End-to-End Packet Forwarding Ratio</td>
</tr>
<tr>
<td>HTCW</td>
<td>Hybrid Trust Computation Scheme for Cluster-based WSNs</td>
</tr>
<tr>
<td>I</td>
<td>Integrity</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>ISRRRA</td>
<td>Immune System-inspired Routing Recovery Algorithm</td>
</tr>
<tr>
<td>LabVIEW</td>
<td>Laboratory Virtual Instrumentation Engineering Workbench</td>
</tr>
<tr>
<td>LEACH</td>
<td>Low-Energy Adaptive Clustering Hierarchy</td>
</tr>
<tr>
<td>LFTM</td>
<td>Linguistic Fuzzy Trust Mechanism</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MLAIS</td>
<td>Machine Learning Artificial Immune System</td>
</tr>
<tr>
<td>NBBTE</td>
<td>Node Behavior Strategies Binding Belief Theory of Trust</td>
</tr>
<tr>
<td>PDR</td>
<td>Packet Delivery Ratio</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
</tr>
<tr>
<td>RBANN</td>
<td>Radial Base Artifiel Neural Network</td>
</tr>
<tr>
<td>SI</td>
<td>Swarm Intelligence</td>
</tr>
<tr>
<td>TDMA/CDMA</td>
<td>Time Division Multiple Access/ Code-Division Multiple Access</td>
</tr>
<tr>
<td>WADS</td>
<td>Weighted Averaging and Decrease Sampling interval</td>
</tr>
<tr>
<td>WSNs</td>
<td>Wireless Sensor Networks</td>
</tr>
</tbody>
</table>
CHAPTER ONE

1 Introduction

1.1 Overview

The advances in the fields of microelectronics materials implies crucial improvement in sensors industries such as lower in cost, lower in power consumption, tiny in size, multifunctional features etc., These tiny sensor nodes consisting of sensing, data processing, power sources, and communication components. In addition to, the development of high speed broadband wireless technologies has led to the deployment of wireless sensor networks (WSNs). WSNs are expected to be solutions to many applications in different fields (Arampatzis, Lygeros et al. 2005, Sohraby, Minoli et al. 2007), i.e. military, environmental monitoring, health, control systems, smart building, tracking and commercials applications.

Any sensor nodes in a WSNs are suffering resource limitation. They have issues of such networks include, but are not limited to, the problems of size, energy factors, transmission media factors, topology complexity, technology standards proprietary solutions and scalability concerns etc.

The research trends related to WSNs are many, e.g. development of models and improvement existing tools for the design of better WSNs architecture and design of standard protocols in WSNs to work robustly on scenarios. The factors influencing sensor network design is highly important to be fully integrated of all factors that are driving the design of sensor networks and sensor node simultaneously (Akyildiz, Su et al. 2002). These factors work as a guideline to design related protocols, algorithm or approach i.e. reliability, scalability, robustness, complexity either time or space etc.
In communication networks, protocols control and determine activity specifications how networks fulfil their intended use (Fahmy 2016). The sensor network protocol stack is same the traditional network protocol stack (Sankarasubramaniam, Akyildiz et al. 2002), with the layers of application, transport, network, data link, and physical. Frequency selection and generation are a mission of physical layer as well as data encryption and modulations process. Data link layer is responsible for the multiplexing of data packets. The network layer takes care of routing task. The transport layer helps to maintain the data flow and its important when network connected to internet as in Internet of Thigs (IoT) technology. Different types of application software can be used on the application layer according to the network tasks. A common plane shared above layers aims to optimize a management purpose, a different research been conducted in this context. The aims of security in WSNs is to protect the information and resources from external offensive, includes to ensures that certain network activity is available, authorization to ensures that only authorized sensors providing information to the network, authentication which monitor the communication from one sensor to another is real, confidentiality which ensures that a given message cannot be understood by anyone other than the one who should be. Integrity which check that a message sent from one sensor to another is not change by any intermediate sensors. Forward and backward secrecy when a sensor should not be able to read any future messages after it leaves the network or when a joining sensor should not be able to read any previously message. Nonrepudiation means that a node can't refuse sending an information it has been sent previously. Finally, freshness implies that the data is recent and guarantee that adversary cannot replay old messages (Wang, Attebury et al. 2006).

Trust between nodes within WSNs is emerging as a crucial factor in WSNs security systems (Yu, Li et al. 2012). It has been increasingly studied by many researchers and remains an open and challenging field. Research on security in WSNs has also explored cryptography