# Mobile Agent-Based Anomaly Detection and Verification System for Smart Home Sensor Networks

Muhammad Usman
Vallipuram Muthukkumarasamy
Xin-Wen Wu · Surraya Khanum

# Mobile Agent-Based Anomaly Detection and Verification System for Smart Home Sensor Networks

Springer

Muhammad Usman
Department of Computer Sciences
Quaid-I-Azam University
Islamabad
Pakistan

Vallipuram Muthukkumarasamy
School of Information and Communication Technology
Griffith University
Gold Coast, QLD
Australia

Xin-Wen Wu
School of Information and Communication Technology
Griffith University
Gold Coast, QLD
Australia

Surraya Khanum
Department of Computer Sciences
Quaid-I-Azam University
Islamabad
Pakistan

ISBN 978-981-10-7466-0 ISBN 978-981-10-7467-7 (eBook)
https://doi.org/10.1007/978-981-10-7467-7

Library of Congress Control Number: 2017962994



Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

*Dedicated to the research community...*

# Preface

The rapid technological developments in microelectronics and associated technologies have realized contemporary networking and computing paradigm, viz. shared sensor networks. This paradigm primarily relies on tiny sensor nodes, as key building blocks, to form a number of applications such as smart transport system, smart home, smart cities, smart irrigation system, and infrastructure and environment monitoring. The tiny sensor nodes, in the above-cited application domains, are vulnerable to in situ attacks, errors, and faults. On the similar account, the data sent by tiny nodes in the form of sensor readings is susceptible to transit attacks and errors. A multi-aspect and comprehensive anomaly detection and verification system is, therefore, desired to aptly identify anomalies (or abnormalities) and convey this information to a central node. The system is known as abnormality identification and confirmation system in the subsequent discussion. The contemporary abnormality identification systems are unable to accurately detect the causes of abnormalities. The solitary focus of existing systems is on the identification of abnormalities. To determine the root causes of abnormalities is imperative to remove them.

This book has elucidated an on-the-spot confirmation service for sensor networks, which leverages from the mobile agent technology to ascertain the root cause of abnormalities. A detailed system, which is not only able to detect abnormalities but can also identify the root cause of abnormalities, is introduced for smart home sensor networks. The system empowers mobile agents to employ data which is received through a synchronized resource management technique to carry out the in situ analysis of susceptible nodes. The synchronized resource management technique allows tiny nodes to share statuses of their resources with related cluster leader nodes for better network resource administration. Moreover, the key proposition of the work presented in this book is to use the information received through the synchronized resource management technique to identify numerous kinds of resource-consumption status-related abnormalities. Another key aim of the presented system is to maximize the usage of received synchronized resource management technique-based observations for abnormality identification. In this account, the statistical relationships between varied features of interest are exploited to identify abnormalities which occur due to faults on nodes and exhaustion of

resource and denial-of-sleep attacks. The system employs the data received from synchronized resource management technique-based observations using mobile agents to verify the root causes of abnormalities.

The frequent transmissions of mobile agents cannot be performed due to the fact that transmission is an energy-expensive operation as compared to processing operation. To solve this problem, two methods, namely weighted-sum optimization and 2-sigma, are presented. The nature of the proposed effective mobile agent transmission methods is generic. The proposed methods, therefore, can also be employed by other mobile agent-enabled applications for wireless sensor networks. This book has also introduced a mobile agent-enabled method that performs abnormality identification and confirmation using cross-layer features. It employs fuzzy logic and cross-layer optimization techniques to identify cross-layer abnormalities and optimize mobile agent transmission. A regions computation technique is presented, which employs statistical methods to facilitate decision making about mobile agent transmission and abnormality identification. A cross-layer rule-base, based on the fuzzy logic, is presented along with algorithmic specifications to identify abnormalities and to facilitate transmissions of mobile agents after taking into account the communication link states.

A non-validated system design may adversely affect the resources of a wireless sensor network or even it may go into a standstill state. Therefore, this study extends the theory of Petri net to the formal characterization and investigation of an abnormality identification and confirmation system which employs mobile agent technology in tiny resource-constrained sensor networks. Formal definitions, of the presented system, using standard Petri net, are elucidated to formalize and verify the behavioral characteristics and also flow of the work of the presented methods. A Generalized Stochastic Petri net (GSPN) model is formulated to study the time-based conduct of the presented system in an immensely non-deterministic communication environment of wireless sensor networks. The formal behavior is then verified by experiments that are carried out on a real test bed. The performance of the proposed methods is thoroughly analyzed through theoretical analyses, experimentation on a real test bed, extensive simulations, and comparisons with related schemes. The results indicate the abilities of the proposed methods to detect different nature of abnormalities with high accuracies and increase network lifetime by optimizing mobile agent transmission in addition to effectively identifying the sources of abnormalities.

This book has focused on a single node mobile agent itinerary model. In future work, the proposed work could be extended to a multi-node mobile agent itinerary model in large-scale networks. Another possible extension could be the exploitation of higher-order joins to detect more complex natures of abnormalities.

Islamabad, Pakistan — Muhammad Usman
Gold Coast, QLD, Australia — Vallipuram Muthukkumarasamy
Gold Coast, QLD, Australia — Xin-Wen Wu
Islamabad, Pakistan — Surraya Khanum

# Acknowledgements

The work elucidated in this text is based on the study carried out by the lead author under the supervision of co-authors Prof. Vallipuram Muthukkumarasamy and Dr. Xin-Wen Wu. Ms. Surraya Khanum has been involved in refining and improvement in certain aspects of the research work.

Authors are deeply indebted to Associate Professor Farooq Ahmed, a former colleague of the lead author, for introducing him to a rich body of knowledge, namely Petri net theory, which ultimately stimulated authors to explore structural and system-specific behavioral properties of the elucidated methods.

Authors acknowledge the generous financial support provided by Griffith University to fully fund this research study and to provide several travel grants to present and publish findings in multiple conferences and also publish in several top-tier journals. Authors would also like to thank Mrs. Robynee Barnes and others of GELI for their help in improving the presentation of this book.

Authors are also indebted to current and past members of the Network Security Research Group, Griffith University, for their criticism and suggestions which have helped authors to improve the quality of the work presented in this text.

# Contents

# About the Authors

**Dr. Muhammad Usman** received his Ph.D. from the School of Information and Communication Technology, Griffith University, Australia. He has obtained Juniper Networks, USA, certifications as an Internet specialist and Internet associate in enterprise routing and switching. He is a member of the Network Security Research Group and the Institute for Integrated and Intelligent Systems (IIIS), Griffith University, Australia. He is also a member of the Computer Science Teacher Association endorsed by the Association for Computing Machinery (ACM), USA. He is currently associated with the Department of Computer Sciences, Quaid-I-Azam University, Pakistan, as an Assistant Professor. His current research interests are security and privacy, cloud computing, Internet of things, distributed systems, and modeling and analysis. He has published over twenty-five research papers for international journals and conferences including prestigious journals such as IEEE Transactions on Consumer Electronics. He has been a recipient of several honors, awards, and grants throughout his industrial and academic career.

**Dr. Vallipuram Muthukkumarasamy** obtained his B.Sc. in Engineering from the University of Peradeniya, Sri Lanka, and his Ph.D. from Cambridge University, England. He is currently attached to the School of Information and Communication Technology, Griffith University, Australia, as an Associate Professor. His current research areas include the investigation of security issues in wireless networks, sensor networks, trust management in mobile ad hoc networks (MANETs), key establishment protocols and medical sensors. He currently heads the Network Security Research Group at the Institute for Integrated and Intelligent Systems at Griffith University. Also providing leadership with regard to innovative learning and teaching practices, he has received a number of best teacher awards.

**Dr. Xin-Wen Wu** received his Ph.D. from the Chinese Academy of Sciences, Beijing. He has worked in the University of California, San Diego (as a postdoctoral researcher), the Chinese Academy of Sciences, and the University of Melbourne (as a research fellow). He was also affiliated with the University of Ballarat, Australia. He joined Griffith University, Australia, in 2010 as a faculty

member at the School of Information and Communication Technology. His research interests include cyber security and data privacy, applied cryptography, coding techniques, and information theory and its applications. He has published extensively in these areas, including 3 books and over 80 research papers in leading journals of IEEE, Springer, and Elsevier, in addition to proceedings of international conferences. He is a senior member of IEEE.

**Ms. Surraya Khanum** received her M.S. (Computer Science) from International Islamic University, Islamabad, Pakistan. She has been associated with Griffith University, Australia, as a visiting research associate. She has also worked as a Lecturer at King Khalid University, Saudi Arabia, and as a Visiting Lecturer at Department of Computer Sciences, Quaid-I-Azam University, Pakistan. She has published numerous research papers, predominantly in the domains of mobile agent-based distributed systems and intrusion detection systems.

# Acronyms

| | |
|---|---|
| AA | Anomaly verification Agent |
| ADM | Anomaly Detection Module |
| ADVM | Anomaly Detection and Verification Module |
| AIS | Artificial Immune System |
| ARIMA | Auto Regressive Integrated Moving Average |
| ART | Adaptive Resonance Theory |
| AU | Aggregation Unit |
| BS | Base Station |
| BY | BatterY status |
| CAP | Contention Access Period |
| CFP | Contention Free Period |
| CLN | Cluster Leader Node |
| CRC | Cyclic Redundancy Check |
| CRM | Coordinated Resource Management |
| CU | Coordination Unit |
| DoS | Denial of Service |
| DTQ | Data Transmission Quality |
| DWT | Discrete Wavelet Transform |
| ECG | ElectroCardioGram |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EM | Expectation Maximization |
| GA | Genetic Algorithm |
| GEP | Gene Expression Programming |
| GPS | Global Positioning System |
| GSPN | Generalized Stochastic Petri Net |
| GTS | Guaranteed Time Slots |
| HMM | Hidden Markov Model |
| IDS | Intrusion Detection System |
| LEACH | Low-Energy Adaptive Clustering Hierarchy |
| LIFO | Last In First Out |

| | |
|---|---|
| LQI | Link Quality Indicator |
| MA | Mobile Agent |
| MAC | Medium Access Control |
| MAS | Mobile Agent Server |
| MAW | Mobile Agent Watermarking |
| NA | Nodal Agent |
| PAN | Personal Area Network |
| PCA | Principal Component Analysis |
| PER | Packet Error Rate |
| PHY | PHYsical layer |
| PN | Petri Net |
| RAM | Random Access Memory |
| RERR | Route ERRor |
| RF | Radio Frequency |
| ROC | Receiver Operating Characteristic |
| ROM | Read-Only Memory |
| RSSI | Received Signal Strength Indicator |
| RTS | Ready To Send |
| SA | Static Agent |
| S-MAC | Sensor-Medium Access Control |
| SR | Sensor Reading |
| SSH | Secure SHell protocol |
| SVM | Support Vector Machine |
| TDMA | Time Division Multiple Access |
| UoD | Universe of Discourse |
| VNL | Victim Node List |
| WSN | Wireless Sensor Network |

# Notations

Table 1 Notations and their definitions

| Notation | Definition |
|---|---|
| $a$ to $f$ | User set adjustment parameters |
| $a^*$ to $f^*$ | Variables to compute domains of fuzzy numbers |
| A | Anomalous fuzzy number |
| $A_r^l$ and $A_r^r$ | Left and right bounds of the anomalous region |
| $AA$ | Anomaly verification agent |
| $AO$ | Anomalous observations |
| $AS$ | Action set |
| $A_{rep}$ | Application repository |
| $A_{data}$ | Application data |
| $A_{unt}$ | Aggregation unit |
| $B_c^l$ | Battery current level |
| $B_t^l$ | Battery threshold level |
| $BA$ | Anomalous behavior |
| $BT_\eta$ | Tolerated category 1 behavior |
| $BT_\delta$ | Tolerated category 2 behavior |
| $BT_\zeta$ | Tolerated category 3 behavior |
| $Beh$ | $msn_q$ behavior |
| $CU$ | Coordination unit |
| $cln_q$ | $q_th$ cluster leader node |
| $d^ag$ | Aggregated sensed data |
| $d^al$ | Anomaly alarm |
| $d_i^ag$ | $i_th$ Aggregated sensed data |
| $d_i^al$ | $i_th$ anomaly alarm |
| **E** | Edges denoting communication links |

(continued)

(continued)

| Notation | Definition |
|---|---|
| $f$ | Received packet count |
| $f_i$ | $i_th$ feature |
| $F$ | Set of arcs |
| $a$ to $f$ | User-defined adjustment variables |
| $a$ to $f$ | User-defined adjustment variables |

Table 2 Notations and their definitions

| Notation | Definition |
|---|---|
| $F_q$ | Collection of values of features of $q_th$ node |
| $FS$ | Features of interest |
| $FS_1$ | Features $\lambda$, $\phi$, and $v$ |
| $FS_2$ | Features $\imath$ and $f$ |
| $G$ | A graph denoting a smart home sensor network |
| $h$ | Number of historical observations used to compute agent transmission score |
| $H(.)$ | Inhibition function |
| $I(.)$ | Input function |
| $msn_q$ | $q_th$ cluster member node |
| $m_{fx}^{fq}$ | Value of a fixed value feature |
| $m_{rg}^{fq}$ | Value of a continuous random variable feature |
| $M_j$ | $j_th$ marking state |
| $M_j^{'}$ | A marking state other than $j$ |
| $M_0$ | Initial marking state |
| $N$ | Normal fuzzy number |
| $N(\lambda, \imath)$ | First-order join for in situ fault or attack |
| $N(\imath, v)$ | First-order join for resource exhaustion attack |
| $N(\phi, v)$ | First-order join for fault on node and attack on resource node |
| $N(\phi, \imath)$ | First-order join for faulty node |
| $N(f, \imath)$ | First-order join for denial-of-sleep attack and faulty node |
| $O^+(.)$ | Output function |
| $O_j$ | $j_th$ observation |
| $p_i$ | $i_th$ place |
| $P$ | Set of places |
| $P_{fx}^{fq}$ | Normal profile value of a fixed value feature |
| $P_{rg}^{lb}$ | Lower bound of a continuous random variable feature |
| $P_{rg}^{ub}$ | Upper bound of a continuous random variable feature |
| $Prf_q$ | Normal profile bound of $q_th$ node |
| $R$ | In situ verification result |

(continued)

(continued)

| Notation | Definition |
|---|---|
| $RP$ | Repository |
| $RS$ | Resource status |
| $RM(M_0)$ | Reachable marking from initial state |
| $s^l$ and $s^r$ | Left- and right-side standard deviation values |
| $S^t_{AA}$ | Anomaly verification agent transmission score |
| $S_{msn_q}$ | Historical observation score to transmit anomaly verification agent |
| $S_msn_q$ | Segment of the stack memory of $msn_q$ |
| $S_agnt_q$ | Segment of the stack memory of $agnt_q$ |
| $t_i$ | $i_th$ transition |
| **T** | Tolerance fuzzy number |
| $T$ | Set of transitions |
| $T_i^{lb}$ | Start time of a timeslot |
| $T_i^{ub}$ | Finish time of a timeslot |
| $T_{ar}^{Fq}$ | Function to compute time of arrival of $Fq$ |
| $T_{ar}^{WR}$ | Time of arrival of a watermarked result |
| $TR$ | Trust value |
| $T_{ar}(F_q)$ | Function to compute time of arrival of $Fq$ |
| **V** | Vertices denoting nodes |
| $V_1$ | The laptop-class node (top-level node) |
| $V_2$ | Cluster leader node (intermediate-level node) |
| $V_3$ | Cluster member node (leaf-level node) |
| $WR$ | Watermark |
| $W(.)$ | Rate or weight for timed or immediate transitions |
| $\Pi(.)$ | Priority function |
| $\alpha_1$ | Weighting factor for tolerated instance of $f_i$ |
| $\alpha_2$ | Weighting factor for anomalous instance of $f_i$ |
| $\sigma$ | Firing sequence |

Table 3 Notations and their definitions

| Notation | Definition |
|---|---|
| $\lambda$ | Minimum to maximum bounds to sensor reading |
| $\iota$ | Time interval |
| $\phi$ | Values of entitled actions by cluster member node |
| $v$ | Resource status of cluster member node |
| $\kappa$ | Anomaly detection action |
| $\tau$ | Tuning action |
| $\psi, \zeta, \delta, \eta$ | Thresholds for agent transmission |