EAI/Springer Innovations in Communication and Computing

Shishir Kumar Shandilya
Neal Wagner
V. B. Gupta
Atulya K. Nagar *Editors*

Advances in Nature-Inspired Cyber Security and Resilience

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor
Imrich Chlamtac European Alliance for Innovation, Ghent, Belgium

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at https://link.springer.com/bookseries/15427

Shishir Kumar Shandilya • Neal Wagner
V. B. Gupta • Atulya K. Nagar
Editors

Advances in Nature-Inspired Cyber Security and Resilience

Springer

EAI
RESEARCH MEETS INNOVATION

Editors
Shishir Kumar Shandilya
School of Computing Science and Engineering
VIT Bhopal University
Bhopal, India

V. B. Gupta
Devi Ahilya Vishwavidyalaya
Madhya Pradesh, India

Neal Wagner
Complex Systems Scientist
Modeling and Analysis Innovation Center, MITRE
Bedford, MA, USA

Atulya K. Nagar
School of Math, Computer Sci & Engg.
Liverpool Hope University
Liverpool, UK

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-90707-5 ISBN 978-3-030-90708-2 (eBook)
https://doi.org/10.1007/978-3-030-90708-2

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

In loving memory of my brother Sameer Shandilya
Always Loved, Never Forgotten, Forever Missed

Preface

Along with the rapid technological advancements in cyber defence methods, cyber threats are also growing constantly and utilizing more sophisticated methods for cyberattacks. Unfortunately, defensive techniques are finding difficulties in coping up with such advanced attacks as cybercriminals are now becoming more organised and equipped with latest technologies like artificial intelligence and machine learning. Most defensive methods still have conventional pattern-based response systems. This situation is worsening with each passing day; therefore, security practitioners and researchers are finding behavioural solutions to achieve a robust security system.

The prime objective of this book's focus is to discuss the novel, emerging and unconventional defensive methods to counter the ever-growing advanced attacks while maintaining integrity, safety, and protection. This book also focuses on some of the most important, latest, and cutting-edge techniques like nature-inspired cybersecurity which has the potential to safeguard systems and networks even in the future era of quantum computing.

The book discusses innovative cybersecurity methods with detailed description and respective experimental results to counter the cyberattacks proactively. This book attempts to provide a reference for students, researchers, scholars, professionals, and practitioners in the field of cybersecurity. The book brings together leading researchers and practitioners in the field and will be an important resource for cybersecurity students, with an aim to promote, present, analyse, and discuss the latest research in cybersecurity.

We extend our sincere gratitude to Ms Kadhambari Viswanathan, Assistant Vice President, VIT Bhopal, for her empathetic understanding and kind support in the most difficult time of the COVID-19 pandemic. We thank all the authors, reviewers, and publishers, especially Ms Eliška Vlčková, for their support throughout the

process of this publication. Special thanks to Prof Imrich Chlamtac for the guidance and inspiration. We hope that this book will be beneficial to all the concerned readers.

Bhopal, India — Shishir Kumar Shandilya
Bedford, MA, USA — Neal Wagner
Indore, India — V. B. Gupta
Liverpool, UK — Atulya K. Nagar

Contents

About the Editors

Shishir Kumar Shandilya is the deputy director of SECURE – Centre of Excellence in Cyber Security at VIT Bhopal University. He is working as a principal consultant to the Govt. of India for technology development and assessment in cyber security. He is also the executive director of the National Cyber Defence Research Centre, New Delhi. He is a visiting researcher at Liverpool Hope University in the United Kingdom, a Cambridge University–certified professional teacher and trainer, TEDx speaker, ACM Distinguished Speaker, and a senior member of IEEE. Shishir is a NASSCOM-certified master trainer for security analyst SOC (SSC/Q0909: NVEQF Level 7) and an academic advisor to National Cyber Safety and Security Standards, New Delhi. He has received the IDA Teaching Excellence Award for distinctive use of technology in teaching by the Indian Didactics Association, Bangalore (2016), and Young Scientist Award for two consecutive years, 2005 and 2006, by the Indian Science Congress and MP Council of Science and Technology. He has ten books published by Springer, IGI-USA, River-Denmark, and Prentice Hall of India. He has international and national patents and copyrights granted for adaptive cyber defence methods.

Neal Wagner is a complex systems scientist at the Modeling and Analysis Innovation Center, MITRE, USA. Dr Wagner has also worked in the Cyber Analytics and Decision Systems Group at MIT Lincoln Laboratory. His focus lies in developing problem-solving methods, tools, and techniques that combine computational intelligence and modelling and simulation to create automated/semi-automated cyber decision-making systems. Prior to joining Lincoln Laboratory in 2013, he was at SolveIT Software, where he specialized in the commercialization of bio-inspired computing techniques for supply chain optimization of large organizations. His academic experience includes stints as a faculty member of the Computer Science and Information Systems Departments at Augusta University and Fayetteville State University. Dr Wagner holds a BA degree in mathematics from the University of North Carolina at Asheville and an MS degree in computer science and a PhD degree in information technology, both from the University of North Carolina at Charlotte.

V. B. Gupta is professor and head of the School of Data Science and Forecasting at Devi Ahilya University, Indore, India. He has authored several national and international publications, and he works as a reviewer for reputed professional journals. His major research interest involves systems engineering, modelling and simulation, operations research, environmental management, technology diffusion, system dynamics, and S&T communication.

Atulya K. Nagar holds the foundation chair as Professor of Mathematical Sciences and is the pro-vice-chancellor for research at Liverpool Hope University, United Kingdom. He has been the dean of the Faculty of Science and head of the School of Mathematics, Computer Science and Engineering, which he established at the University. He received a prestigious Commonwealth Fellowship for pursuing his doctorate (DPhil) in applied nonlinear mathematics, which he earned from the University of York (UK) in 1996. He holds BSc (Hons), MSc (Mathematics), and MPhil (with distinction) in mathematical physics from the MDS University of Ajmer, India. Prior to joining Liverpool Hope, he was with the Department of Mathematical Sciences, and later with the Department of Systems Engineering at Brunel University, London. He is an internationally respected scholar working at the cutting edge of theoretical computer science, applied mathematical analysis, and systems engineering with his research expertise spanning both applied mathematics and computational methods for nonlinear, complex, and intractable problems arising in science, engineering, and industry. He has edited volumes on intelligent systems and applied mathematics. He is the editor-in-chief of the *International Journal of Artificial Intelligence and Soft Computing* (IJAISC) and serves on editorial boards for a number of prestigious journals. He is well published with over 450 publications in prestigious publishing outlets. Prof Nagar sits on a number of strategic UK-wide research bodies including the JISC Research Strategy group, and he is the fellow of the Institute of Mathematics and its Applications (FIMA) and fellow of the Higher Education Academy (FHEA).

Nature-Inspired Cybersecurity and Resilience: An Overview

Shishir Kumar Shandilya

1 Introduction

Cyberattacks and breach attempts are rising, and attackers are finding new ways to penetrate into the system or a network, through advanced methods that are trained through artificial intelligence (AI) and machine learning (ML) approaches. The attackers are also using high-performance machines against the target, and above all they are working in a more coordinated and organized way to plan and execute the attacks. Also, the various types of computing devices and different operating systems over the network make the situation more vulnerable and thereby favourable for the attackers. The attackers may have multiple windows for uploading the payloads if these windows are not properly configured and controlled. Majority of defence mechanisms fails some or the other way to identify and counter these malicious codes, and therefore safety and privacy are always on stake. The defensive mechanisms also need to be uplifted to cope with the growing intelligence of malicious activities, and therefore the researchers and security organizations are coming up with more sophisticated ways to be fully equipped by using AI, ML and data science approaches. Along with these, the current security solution providers and scientists are also exploring other avenues, through which the security can be established without compromising much on the processing speed and cost.

Nature-inspired cybersecurity comprises computational methods derived from the natural defensive behaviours from various species. NICS is being taken up by the researchers as a robust solution to develop a more adaptive and effective security solution against the cyberattacks. NICS may provide multiple procedures ranging from executing multi-objective optimization, providing disguise information and

S. K. Shandilya (✉)
School of Computing Science and Engineering, VIT Bhopal University, Bhopal, India
e-mail: shishirkumar.s@vitbhopal.ac.in

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

S. K. Shandilya et al. (eds.), *Advances in Nature-Inspired Cyber Security and Resilience*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-90708-2_1

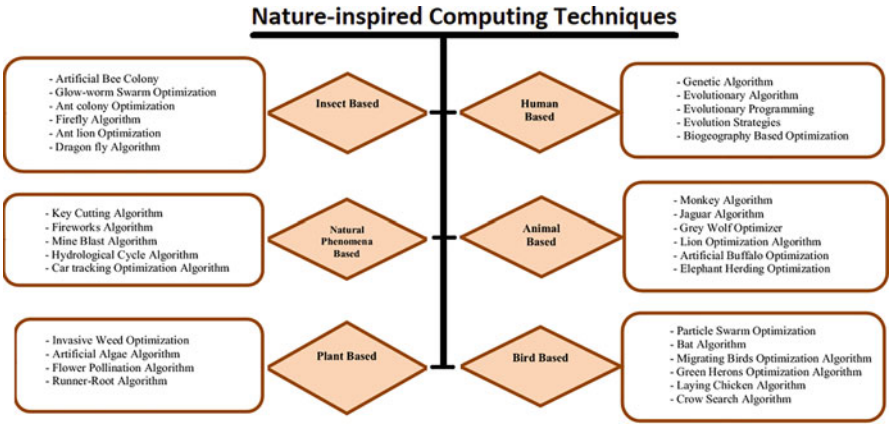

Fig. 1 Nature-inspired computing techniques [1]

utilizing the information and aggregating them for effective implementation of security. NICS in combination with AI/ML and data science can be a lethal security option against the advanced cyberattacks. NICS techniques can also be utilized to provide adaptability, self-organization, resilience, and robustness in the security solutions.

Figure 1 shows the classification of general nature-inspired techniques [1], which can be further used in cybersecurity after appropriate modifications and fine-tuning. Hybrid versions of these techniques are influenced by the recent developments in AI and ML which are more promising methods for NICS.

The implementation of NICS technique on application requires appropriate analysis on the parameters and fine-tuning of optimization. NICS can provide many novel features like autonomous threat detection and resolution, artificial immune system (a computationally intelligent self-learning algorithm modelled after mammalian immune system's characteristics of learning and memory for use in problem-solving), camouflaging of network architecture and self-healing programs. NICS also fundamentally supports and is having huge potential to achieve cyber immunity which is a point where the cost of attacking is very high to make it achievable for attackers. Therefore, many current researchers and organizations like Kaspersky are working extensively on this.

Figure 2 shows the general framework about how the NICS can be implemented to safeguard the critical assets. The main algorithm of NICS system generates the adaptive defence and suggests security decisions to security analysts or takes the decisions if configured appropriately. The NICS system can be implemented either as active or passive way.

The Active NICS defence deals with the real-time network parameters and holds control over the critical assets. The Active NICS is capable of learning by experience, and therefore attached AI/ML/DL model can be very useful for early identification of threats. As this functionality comes with cost and processing

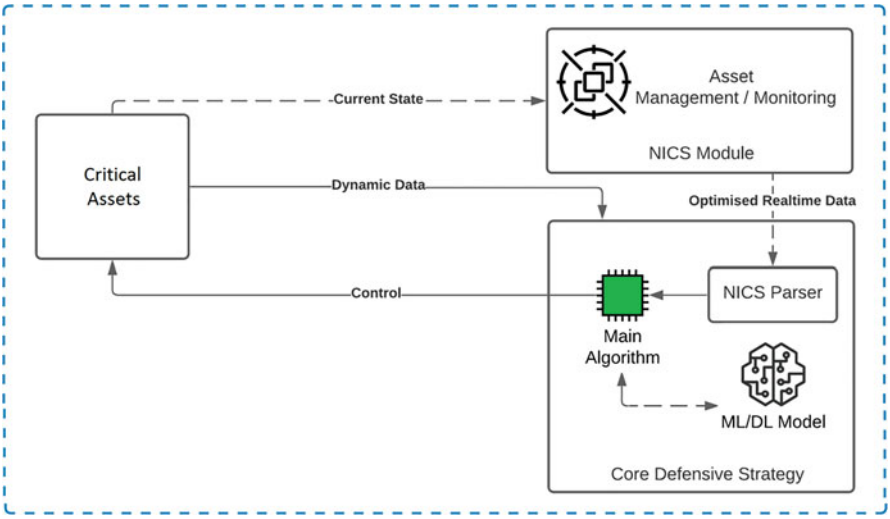

Fig. 2 Nature-inspired cybersecurity

overhead, it is an open research problem to minimize the overheads while making the learning component more cohesive to the NICS system.

The passive NICS defence on the other hand relies more on the AI/ML/DL models where the features are selected and used to train the model which then works as an assistant to the NICS defence system. It is a faster method but limited in scope. In another chapter of this book by Saket Updhayay, active and passive NICS defence systems are discussed in detail.

Along with many possibilities, there are also many challenges in implementing the nature-inspired phenomena in cybersecurity domain. It is difficult to understand and mimic the exact relationships and processes of nature and then to implement them for a stable security mechanism.

2 Literature Survey

In the early 1960s, computer starts sharing data and information to each other on "network". Most of the people at that time in America had never seen a computer. The US government recognized that as the data and information are shared on network progressively, there is a need to control and ensure that the computer did not allow any user to see data belonging to the other users [2]. In year 1968, West Germany's police caught an East German spy in IBM's German subsidiary, stating that it was the first case of cyber espionage. In year 1989, some high school students from Milwaukee, inspired by the thriller movie WarGames, got successful in invading military networks. In present scenario, cybersecurity issues are very

common. In every 2 minutes, at least one fraud or cybercrime is reported which makes it a serious issue to be taken care of.

For every organization, private as well as government, security of data/information is a top priority. As all the private information are confidently shared on digital media without knowing the severity of it, it has become a challenging task for the cyber defender to protect data from the cyberattackers.

I. H. Lim et al. [3] in year 2010 proposed a security protocol in distribution automation system (DAS) against cyberattacks. Communication technology is very important and sensitive, while the concern is towards power system. In their paper, they have highlighted the security problems in DAS. DAS is vulnerable as it is highly dependent upon communication and geographically widely spread terminal devices. They analysed many cyber threats on distributed system, and accordingly they proposed security protocol that considers the resource-constrained network nodes and avoids complex computation against encryption algorithm. They also proposed a secure key distribution protocol, and finally they demonstrated the feasibility of proposed protocol.

A central server collects current and voltage data, provided by distribution automation system to perform important operations like automatically detecting and restoring faults and monitoring and controlling feeder remote terminal units (FRTU). In this paper, the authors have mainly focused on possible attacks and analyse cryptography algorithm accordingly and invent security protocol against cyberattacks.

In year 2011 Chee-Wooi Ten et al. [4] proposed an anomaly detection algorithm for the substations. Their proposed algorithm detected cyber-intrusions while considering temporal anomaly. They ranked potential intrusion events according to impact factor of credibility. They used modified IEEE 118-bus system for simulation result. For systematic identification, the generated results have shown the effectiveness of anomaly detection. The researchers stated that it may work as a tool to detect cyber-intrusions which may cause the damages to the power grid.

In year 2012, Vandana Gandotra et al. [5] presented a three-phased threat-oriented security model based on the concept of proactive threat management. In this model, they provided a security for the known as well as for unknown threats. In the first phase, they applied threat modelling process to identify unknown threat. In the second phase, by using multi-agent system planning, concerned and necessary security measures were taking place to mitigate the identified threat. By using meta-agents in multi-agent environment, risk reduction has been evaluated. This model is basically focused on risk analysis segment of the spiral model for security enhancement.

In year 2013, Jaafar Almasizadeh and Mohammad Adollahi [6] proposed a state-based stochastic model which works on security matrix, and the degree of system security is counted by this matrix degree or level of system security. The model is parameterized based on time distribution. Basically this model describes the attackers' activity as well as systems reactions over the time. For this, they have implemented probability distribution function. This model was focused on time parameter which turned out to be very essential and important for capturing

Overarching policy	CYBER DEFENSE		
Situation in which Cyber Defense Technique is applied	War/Conflict		
		Peacetime	
Cyber Defense Technique	CNO	ACD	Non-ACD

Fig. 3 Applicability of cyber defence approaches [8]

the nature of attack process. For characterizing sequential aspect of the attacker and system behaviour, probability distribution function was used based on the mathematical model semi-Markov chain to calculate the security matrix.

Robert S. Dewar in year 2014 [7] explores the three types of cyber defences against the cybercrime – active cyber defence (ACD), fortified cyber defence (FCD) and resilient cyber defence (RCD). In military the term, ACD is very common as offensive action and counterattacks position to the enemy. The ACD defines a proactive measure not only to perceive and explore the security breaches and mitigate any damage caused but also upon aggressive countermeasures undertaken outside the victim networks. The concept of FCD is used to constructing systemically secure communications and information networks to establish defensive perimeters around key assets (like device, routers, switches) as well as minimize intentional or unintentional incidents or damage. The cybersecurity strategy of the USA and UK is adopting ACD for their national policies, while Germany on the other hand is promoting FCD. The third approach of cyber defence is RCD which focuses on decisive infrastructure and services which provide continuous network communication and services for which it is intended, instead of focusing on offenders who are aggressively looking for security breaches or establishing weaponry around key assets. According to this research, FCD is a more practical approach of cybersecurity defence as compared to ACD and FCD (Fig. 3).

2014 is the year where smart grid technology utilized cyber advancement to increase control and monitoring function throughout the electric power grid in America. Smart grid refers to the grid which is progressively dependent upon its cyber infrastructure. In this year, Aditya Ashok et al. [9] introduced a game theoretic approach to address the issues of cyber physical security. In their paper they also discussed the cyber physical security of Wide-Area Monitoring, Protection and Control (WAMPAC).

Every year technology changes bring new challenges for the cyber defender to defend the private data from the attackers. 2015 is the year where there were major technology changes while industries were progressively enabling IOT (internet of things). This year, Ricardo Neisse et al. [10] have proposed security toolkits. These toolkits were basically included into management framework which was integrated for IOT devices for the evaluation of security policies to protect user data. In this paper, they have considered the extended security policies for smart

devices which are connected to the Internet. In their research they addressed the following problems: (i) validity of security and privacy of users' data toward IOT and (ii) how to maintain trust between IOT technology and individuals who use this technology. Sensors added into IOT devices have created a new challenge as large amount of devices and systems attached with sensors and data collected from the sensors are itself huge as compared to normal Internet. Data collected from the IOT device maintain anonymity of data could be one mitigation approach to maintain the privacy and security of users' data. Security issues are more in IOT as compared to Internet. Therefore, there is a need of tool and technology which enforce the security policies for IOT actuators to avoid execution of unwanted actions against users' data. In their paper, they have proposed a model-based security toolkit "SecKit" to address these security challenges related to IOT.

In year 2016, Gaurav Varshney et al. [11] proposed a phishing detection system called as Lightweight Phish Detector (LPD). Web phishing is one of very known attacks used by the cyberattackers to steal users' information like username, password, debit card/credit card numbers, banking information and any other credential information from the Internet. LPD was used for phishing detection. In their research, they ran LPD on client side to detect phishing. LPD was developed using Google Chrome browser. In their paper, they have also compared all the search engines that based on the anti-phishing like Firefox, Internet Explorer, Netcraft toolbar and Cascaded Phish Detector. The working principle behind the LPD is: to check the authenticity of web pages running on a poplar search engine, there is a necessity to use right set of features associated with a web page. If the correct set of features is used, then the correct URL should appear in the top URLs in the search results. In the same year, D. Deore et al. [12] presented a survey of different automated software used to protect the data from hackers. To protect data virtual machine, they have used distributed cybersecurity automation framework. In their survey, they explained the various techniques used for developing new software like user virtualization, event log analysis, one-time password and malicious attack detection.

For online services security risk management, Jan Meszaros et al. [13] proposed a new framework. This framework is usable for both service providers and service consumers. They performed a case study for the validation of framework. Threat model and risk model were the two models which provided a specific feature of online services in public internet environment.

3 Noteworthy Contributions

Neal Wagner et al. [14] in the year 2018 proposed automatic generation of cyber architecture using nature-inspired algorithm. This architecture optimized for less cost, high security and mission performance. The proposed method has provided strong mitigation against cyberattacks. In the proposed work, network is partitioned into segments as well as restricting the communication between segments which

will inhibit the attacks' ability to move and spread infection. This hybrid approach includes nature-inspired algorithm with cyber risk modelling and simulation modelling. The optimization component is used to select the candidate architecture which is evaluated by the simulation process. If the candidate architecture is an effective one, then the process stops; otherwise, the evaluation is then fed back to the optimization component to generate the newer, more effective candidate architecture. These both work together to generate most promising architecture. Still there is no clear guidance regarding network segmentation and which architecture will provide the best security posture; however, the cybersecurity experts strongly recommend segmentation of defence against cyberattacks.

Vajiheh Hajisalem et al. [15] have proposed a hybrid classification Intrusion Detection System. This system was based on Artificial Bee Colony (ABC) and Artificial Fish Colony (AFC) algorithms. They have applied Fuzzy C-Means Clustering (FCM) to divide the training data set and Correlation-based Feature Selection (CFS) techniques to remove irrelevant features. Additionally, the CART technique generated If-Then rules. These rules distinguished the normal and anomaly records. Likewise their proposed method was trained via the generated rules. The proposed anomaly-based IDS, system stores the pattern of normal behaviours stored in IDS database. All the actions across the network were monitored and analysed accurately by the system.

Yu Li et al. [16] proposed a design for a framework for self-destructing wireless sensors. This framework ensures the security and performance of the wireless sensors. The proposed framework uses a cryptographic self-destructing mechanism. This mechanism enabled the autonomous self-destruction of a wireless sensor. If the sensor is lost, self-destruct sensor autonomously destroys the sensitive information. The sensor should have two capabilities: first sensor needs ability to determine whether it is lost and second within time the information needs to be destroyed. For self-destructing mechanism they have used discrete-time Markov chains (DTMC). The model categorized the attackers, the self-destructing mechanism, the catching strategy and the sensors' components.

4 Conclusion

Many of the existing nature-inspired techniques are not explored yet for improving cyber defence system. The ultimate goal of any cyber defence system is to have a strong and robust infrastructure which can deal with attacks in real time while maintaining the consistency and usability of data in the system. Also, the defence system is expected to be self-regulated and automatic in response to any type of cyberattacks. Different types and relative operations of network devices are making the situation difficult to have such a robust and automatic defence system. This situation can be taken care by nature-inspired computing approaches as they are proven fit for the application areas where data is incomplete, multivariant, multimodel or poorly mapped mechanisms. The advent of nature-inspired consensus

protocols and modern game theory methods paved the way for development of similar nature-inspired technology in cyber data security also. This chapter described the potential and suitability of nature-inspired methods and established their relevance in cybersecurity while discussing key research in this domain to achieve self-regulated, automatic nature-inspired defence system.

References

1. R. Gautam, P. Kaur, M. Sharma, A comprehensive review on nature inspired computing algorithms for the diagnosis of chronic disorders in human beings. Prog. Artif. Intell. **8**, 401–424 (2019). https://doi.org/10.1007/s13748-019-00191-1
2. M. Warner, Cybersecurity: A pre-history. Intell. Natl. Secur. **27**, 10 (2012)
3. S. Hong, M.S. Choi, S.J. Lee, T.W. Kim, S.W. Lee, B.N. Ha, I.H. Lim, Security protocols against cyber-attacks in the distribution automation system. IEEE Trans. Power Deliv. **25**(1), 448–455 (2010)
4. J. Hong, C.-C. Liu, C.-W. Ten, Anomaly detection for cybersecurity of the substations. IEEE Trans. Smart Grid **2**(4), 865–873 (2011)
5. V. Gandotra, A. Singhal, P. Bedi, Threat-oriented security framework: A proactive approach in threat management. Procedia Technol. **4**, 487–494 (2012)
6. J. Almasizadeh, M.A. Azgomi, A stochastic model of attack process for the evaluation of security metrics. Comput. Netw. **57**(10), 2159–2180 (2013)
7. R. Dewar, The "triptych of cyber security": A classification of active cyber defence, in *International Conference on Cyber Conflict, CYCON*, (NATO CCD COE Publications, 2014), pp. 7–21
8. R. Dewar, *Active Cyber Defense, Cyber Defense Trend Analysis* (Center for Security Studies (CSS), ETH Zürich, 2017). https://doi.org/10.13140/RG.2.2.19236.17287
9. A. Ashok, A. Hahn, M. Govindarasu, Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. J. Adv. Res. **5**(4), 481–489 (2014) Cyber Security
10. R. Neisse, G. Steri, I.N. Fovino, G. Baldini, Seckit: A model-based security toolkit for the internet of things. Comput. Secur. **54**, 60–78 (2015)
11. G. Varshney, M. Mishra, P. Atrey, A phish detector using lightweight search features. Comput. Secur. **62**, 213–228 (2016)
12. U.D. Deore, V. Waghmare, A literature review on cyber security automation for controlling distributed data. Int. J. Innov. Res. Comput. Commun. Eng. **4**(2), 2013–2016 (2016)
13. J. Meszaros, A. Buchalcevova, Introducing OSSF: A framework for online service cybersecurity risk management. Comput. Secur. **65**, 300–313 (2017)
14. N. Wagner, C.S. Sahin, J. Pena, W.W. Streilein, Automatic generation of cyber architectures optimized for security, cost, and mission performance: A nature-inspired approach, in *Advances in Nature-Inspired Computing and Applications*, (Springer International Publishing, Cham, 2019), pp. 1–25
15. V. Hajisalem, S. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. Comput. Netw. **136**, 37–52 (2018)
16. Y. Li, X. Wang, D.W. Kim, J. Zhang, R. Dai, Designing self-destructing wireless sensors with security and performance assurance. Comput. Netw. **141**, 44–56 (2018)

Detection of Reconnaissance Attacks on IoT Devices Using Deep Neural Networks

Mohammed M. Alani

1 Introduction

In simple terms, Internet-of-Things (IoT) refers to Internet-connected devices that contain sensors and/or actuators [12]. These devices usually have lower processing powers, storage capacity, and memory in comparison to personal computers. IoT devices have witnessed unprecedented growth in adoption in the recent few years [1].

The following subsections will explain background information about IoT devices, reconnaissance attacks, and reconnaissance attacks in IoT. The second section will discuss related previous works. In Sect. 3, we discuss the methodology by which the experiments were done. Section 4 explains the details of the implementation environment, and implementation steps. Results are shown in Sect. 5. In Sect. 6, we discuss the results and their interpretation, while Sect. 7 presents conclusions and suggestions for future work.

1.1 IoT

Most IoT devices are comprised of the components shown in Fig. 1. At the hardware layer, the device includes a processor or controller, in addition to Random Access Memory (RAM) and storage components. In addition, the hardware layer includes a communication module that helps the device connect to the Internet. Most IoT devices include a sensor module that helps the device collect data in some format.

M. M. Alani (✉)
Seneca College, Toronto, ON, Canada
e-mail: m@alani.me

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

S. K. Shandilya et al. (eds.), *Advances in Nature-Inspired Cyber Security and Resilience*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-90708-2_2