© 2022 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

M. Adil et al., "Survey: Self-Empowered Wireless Sensor Networks Security Taxonomy, Challenges and Future Research Directions," in IEEE Sensors Journal, 2022, doi: 10.1109/JSEN.2022.3216824.

https://doi.org/10.1109/JSEN.2022.3216824

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

Survey: Self-Empowered Wireless Sensor Networks Security Taxonomy, Challenges and Future Research Directions

Muhammad Adil, *Member, IEEE*, Varun G Menon, *Senior Member, IEEE*, Venki Balasubramanian, *Member, IEEE*, Sattam Rabia Alotaibi, *Member, IEEE*, Houbing Song, *Senior Member, IEEE*, Zhanpeng Jin, *Senior Member, IEEE*, Ahmed Farouk, *Member, IEEE*,

***Abstract*— In the recent past, patient wearable devices and implantable biosensors revealed exponential growth in digital healthcare, because they have the capability to allow access to the information anywhere and every time to improve the life standard of multifarious disease effected patients followed by healthy people. Following these advantages, digital healthcare demands a secure wireless communication infrastructure for interconnected self-empowered biosensor devices to maintain the trust of patients, doctors, pharmacologists, nursing staff, and other associated stakeholders, etc. Several authentications, privacy, and data preservation schemes had been used in the literature to ensure the security of this emerging technology, but with time, these counteraction prototypes become vulnerable to new security threats, as the hackers work tirelessly to compromise them and steal the legitimate information of user's or disrupt the operation of an employed self-empowered wireless sensor network (SWSN). To discuss the security problems of SWSN applications, in this review article, we have presented a detailed survey of the present literature from 2019 to 2022, to familiarize the readers with different security threats and their counteraction schemes. Following this, we will highlight the pros and cons of these countermeasure techniques in the context of SWSN security requirements to underscore their limitations. Thereafter, we will follow-up the underlined limitations to discuss the open security challenges of SWSN that need the concerned authorities' attention. Based on this, we will pave a road map for the future research work that could be useful for every individual associated with this technology. For the novelty and uniqueness of this work, we will make comparative analysis with present survey papers published on this topic to answer the question of reviewers, readers, editors, and students that why this paper is in time and needed in the presence of rival papers.**

***Index Terms*— Self-empowered biosensors, digital healthcare, security challenges, authentication of biosensors, cyber-security, SWSN.**

I. Introduction

IN the past several years, the growth of patient wearable devices or biosensors technologies had shown a significant contribution in the healthcare industry [1]. To explore, they have been used in many disease detection and prevention processes that range from general to complex [2]. To satisfy the needs of clients (patients), supporting staff, physicians, family members, pharmacologists, etc, a reliable and secure communication infrastructure is required to be developed for these applications that could be capable to meet the Quality of Service (QoS) standards followed by the security protocols [3]. As mention, every parameter has its own advantages and consequences in these networks, but security is one of those problems, which have a direct link to all stakeholders' trust. Therefore, the main focus of this work is on the security of self-empowered patient wearable devices or biosensors that constitute a healthcare self-empowered wireless sensor networks (SWSN).

The general network architecture of SWNS follows the three-layer of the OSI model (open system interconnect) such as the physical layer (data collection layer), network layer (data communication layer), and application layer (data processing and analysis layer) [4]. To explore, a large number of self-empowered biosensors are deployed at the client-side (physical layer) to collect and process data in the network via wireless links (network layer) for the remote users, administrators, operators, etc. Therefore, it is very important for the industry experts and researchers to take care of the security of each layer while designing new security techniques or modifying the existing ones to ensure the integrity and confidentiality of SWSN. To familiarize, the readers with the

Muhammad Adil is with the Department of Computer Science and Engineering, University at Buffalo, NY 14260, USA. (Email: muhammad.adil@ieee.org)

Varun G Menon is with the Department of Computer Science and Engineering, SCMS School of Engineering and Technology, Ernakulam 683576, India (Email: varunmenon@scmsgroup.org)

Venki Balasubramanian is with the School of Science, Engineering and Information Technology, Federation University, Mount Helen VIC 3350, Australia (Email: v.balasubramanian@federation.edu.au)

Sattam Al Otaibi is with the College of Engineering, Taif University, Taif 21974, Saudi Arabia. (Email:srotaibi@tu.edu.sa)

Houbing Song is with the Department of Information Systems, University of Maryland, Baltimore County, Baltimore, MD 21250 USA (Email: h.song@ieee.org)

Zhanpeng Jin is with the Department of Computer Science and Engineering, University at Buffalo, NY 14260, USA. (Email addresses:zjin@buffalo.edu)

Ahmed Farouk is with Department of Computer Science, Faculty of Computers and Artificial Intelligence, South Valley University, Hurghada, Egypt. (Email: ahmed.farouk@sci.svu.edu.eg)

Corresponding Author: Zhanpeng Jin

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

security challenges, *Strielkina et al. [5]* present a detailed survey on this topic by highlighting the recently used attacks. *Bhuiyan et al. [6]* extended this discussion and presented a review article on the security concerns of these networks with different countermeasure techniques. In this article, the author underscored the limitation of different adopted techniques in the context of these network's requirements such as computation and communication costs followed by the processing time of an authentication request, etc, to set foundation for the future research work in this domain.

To follow up on this discussion, in this paper, we want to present a comprehensive survey of the latest literature associated with security aspects of SWSN from 2019-to-2022 to familiarize the readers with the existing challenges. Moreover, we will examine the current cyberattacks in coordination with counteraction schemes to identify their constraint and suggest possible research directions.

The key accomplishments of this work are recapitulated as below:

1) In the first phase, we will familiarize the readers with the taxonomy of self-empowered wireless sensor networks (SWSN). Following the security concerns of SWSN, we will narrow down our discussion with the evaluation of present review articles to set the foundation for this work by highlighting their contributions and limitations.
2) To fill up the gap of underscored limitations of the existing state-of-the-art review articles, we will focus on relevant literature to give a brief overview of different countermeasures schemes by following the layer-wise security threat model.
3) Likewise, we will outline the limitation of present literature to set the stage for open research challenges followed by future research directions that could be useful in the redressal of underlined challenges.
4) Finally, we will do a comparative analysis following the section-wise structure of our paper to claim the novelty and uniqueness of this work, and an answer of a question of the students, readers, reviewers, editors, and other relevant stakeholders that why this paper is required in the presence of rival review articles on this topic.

Remaining paper organization: Section II, of this article, overviews the taxonomy of self-empowered wireless sensor networks (SWSN), while Section III summarized the layer-wise security threats of SWSN technology. Following this, Section IV focus on relevant literature that had been used to address or counter the highlighted security threats in these applications, whereas Section V underlines the open security challenges followed by future research directions. Similarly, Section VII represents the comparative analysis results of our paper in presence of rival papers to demonstrate the distinctive factors and novelty of this work, while Section VII summarized and concludes the paper.

II. Taxonomy of SWSN and Related Review Articles

In this section, we will focus on the taxonomy of SWSN to set a preface for the understanding of security concerns of this emerging technology. For a visual representation, we have used figure 1 to summarize them such as enabling technologies, architectural requirements, SWSN platform architecture types, SWSN applications, and network topological. To explore figure 1, we have shortlisted different enabling technologies that have a direct or indirect role in the interconnectivity, communication, security, interoperability, and operation ability of SWSN. Following this, we have also underlined different applications of SWSN to acknowledge the essence of this newborn technology. With this, we have underscored the requirements of enterprise market stakeholders in the context of Business objectives to set a footstep for the researcher and industry stakeholders working in this domain. Despite this all, we have cited the architecture requirements that need to be considered by industry stakeholders and research community people working in this domain.

1) Enabling technologies of SWSN: In SWSN applications, the sensors devices need network connectivity to share their accumulated data in the network. To interconnect these devices in a network topological order, different routing protocols and communication technologies are used for this task such as low-range wireless area network (LoRaWAN), WiFi, software-defined networks (SDN), Zigbee, low-power personal area network (6LowPAN), Sigfox, and Celluar network, etc [6]. Sigfox has been used as a reliable technology in the communication or interconnectivity process of SWSN that works between Wifi and cellular networks. To explore, Sigfox is very useful to transfer data among interconnected self-empowered sensor devices in the network [7]. SDN is another useful technology that helps to minimize the complexity of the network with improved latency. Similarly, 6LowPAN, 6LowWAN, Zigbee, and WiFi is an IP-based network protocol that works in layer three to encapsulate message packers followed by the header compression processes. To continue, these technologies are very useful to support bidirectional communication in constraint-oriented networks such as SWSN, which is a good sign for them to strengthen their security parameters. For long-range communication cellular communication infrastructure such as (GSM/2G/3G/4G/5G) is in use, because it has great capabilities to ensure the integrity of data during transmission in resource-limited networks [8]. SDN is another alternative emerging technology that has demonstrated remarkable results while managing the network traffic and security to improve the performance of an employed SWSN application.

2) Applications of SWSN: In the last decade, SWSN applications have demonstrated significant contributions to the digitalized world. To exemplify, they have been used in smart cities, smart transportation, smart grids, smart healthcare, smart agriculture, smart homes, etc [9]. With the help of these applications, the people associated with this technology have been facilitated in many aspects of life. To explore, these applications are very valuable in transportation, because it helps to ameliorate traffic congestion at different points by providing alternative routes. Moreover, ML-enabled techniques also have confirmed reliable results during predictive analysis to minimize road casualties [10]. To extend this discussion, SWSN has also been very productive in smart homes, because it enables the inhabitants to remotely monitor and control

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

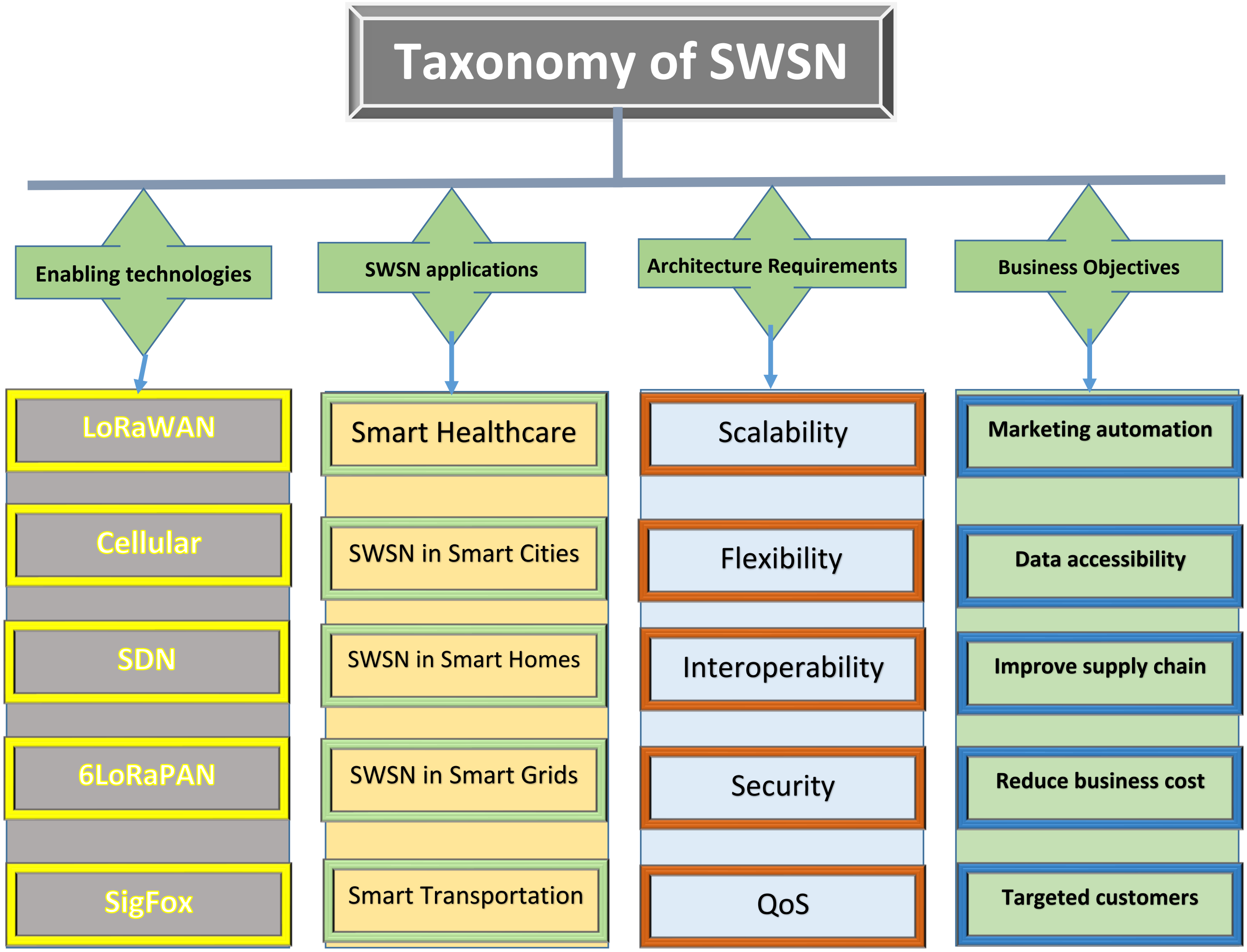


Fig. 1: SWSN visual representation

home appliances [11]. In smart healthcare, they have been used to monitor different detect diseases at an early stage or monitor the existing patients [12]. If we talked about this technology in the smart grids, they are useful to note the energy consumption at the client-side, and forward the recorded data to remote grids for further processing. In smart cities, it enables intelligent lighting, accessibility to markets, and transportation through low-cost and low-power self-empowered sensor devices that are connected through wireless links to share accumulated data in the network and facilitate people's daily lives. Despite this, in table I, we have summarized all possible applications, where SWSN has technology had been used.

3) Architectural Requirements of SWSN : New and existing SWSN applications need different architectural requirements to manage the issues of scalability, interoperability, flexibility, QoS, and security concerns of sensor devices followed by deployed networks [23]. Scalability of SWSN refers to the expandability of these networks, where voluminous sensor devices would be added to an employed network without losing the generality and performance issues. Whereas flexibility of SWSN defines the provision of firmware updates followed the application services such as an employed network devices software should be updated, programmed, and optimize according to certain requirements of applications and clients [24]. However, the interoperability of SWSN applications is very helpful to enable the interoperation among interconnected sensor devices in heterogeneous networks. Likewise, QoS is another most influential architectural requirement of these applications, because delay-sensitive data transmission evaluates the performance of an employed SWSN [25]. Therefore, every highlighted parameter have its own role and importance in these applications and need considerable attention from all stakeholder working with this technology during the implementation phase.

4) Antenna Requirements of Self-Empowered Sensors : In this subsection, we will talk about the onboard antenna of self-empowered sensor devices, because it plays a vital role in the communication of interconnected devices. To explore this topic, we have noted in the literature that antenna systems are getting popularity with the passage of time, because of the high demand for emerging technologies such as WSN and SWSN applications. According to the survey articles [26-29],

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

TABLE I: Summary of different surveys paper contributions followed by their limitations

Application Domain	***Description***	***Advantages***	***References***	***Future Objectives***
Military Applications	In the recent past, SWSN has used many subdomains of the Military sector such as battlefield surveillance, intruder detection, combat monitoring, and drones to facilitate different operations cost-effectively.	Special sensor such as Radiological, Biological, Chemical, Nuclear and Explosive (CBRNE) are helpful to detect the presence alike name substances.	Swamy et al. [13], Boukerche et al. [14], Deng et al. [15]	Easy accessibility to the specific entities such as mentioned
Environmental Applications	SWSNs had been used to enhance accessibility to environmental impediments such as continuous monitoring of ambient conditions like a forest fire, coastal area monitoring, abd flood monitoring, etc.	Water monitoring, air monitoring, temperature monitoring, humidity monitoring, and fire detection sensors are used to report hazardous information from inaccessible areas to remote location	Patil et al. [16], Rajasekaran et al. [17], Mao et al. [18]	Can be extremely helpful to prevent dangerous situation like this in the future
Flora and Fauna Applications	SWSN applications had demonstrated extraordinary results in flora and Fauna sectors to facilitate the different tasks.	Gas sensors, temperature sensors, conductivity sensors, RF sensors, and photographic sensors are used to manage the greenhouse effect, crop monitoring, and livestock farming, etc.	Vera-Amaro et al. [19], Hamouda et al. [20], Catini et al. [21], Zorbas et al. [22]	In the future, it can be very useful to improve the productivity of this sector.

it can help to improve spectrum use with enhanced quality of service metrics. Moreover, the authors discussed different aspects of an antenna in the context of its importance in different emerging technologies. Moreover, the specific security requirements of sensor devices in the context of antenna model are discussed in reference [30]. In [31], Curiac et al. discussed the importance of directional and omnidirectional antennas in the context of security challenges of the WSNs. Moreover, the authors highlighted the weak and strong aspects of these antennas by taking into account the real attacks and communication atmospheric to minimize the intruder anticipation in the network and improve the communication metrics with the least implementation cost.

5) Business Objectives Requirements of SWSN : In the recent past, it has been noted that SWSN applications have provided a lot of benefits to several businesses. To explore the business objectives of SWSN applications, it offers sale data access, marketing automation, targeted customer services, reduces the cost of delivery, and improves the supply chain processes [32]. Smart-SWSN applications create a knowledge base framework for the customers such as the buying pattern, order records, payment records, supply chain, and preferences, etc [33]. Despite this, it also allows the business stakeholders to find out the customer needs in real-time and they also make a prediction of the future demands of the customers based on recorded data. Following this, the customers order anything online to save time, and site visiting costs with one-way arrival time. These are examples of marketing automation and online shopping.

To continue this discussion, the interconnected devices of SWSN applications share tremendous amounts of data in the network in the context of customers' demands and orders. With this, the companies will know the what, why, and where the customer is demanding, and what they need to improve in the future for their better services. In addition, the supply chain and customer services can be improved up to a great extent by analyzing the generated data of self-empowered sensor devices to fulfill the requirements of customers and achieve business objectives.

A. Summary of Discussion ”Taxonomy”

In this segment, we are going to summarize the learned lesson from the preceding subsections. Undoubtedly, SWSN is an emerging technology and has numerous contributions in many sectors. Therefore, we familiarized the new readers, students, and enterprise stakeholders with the taxonomy of this technology followed by enabling technologies. Thereafter, we acknowledge the importance of this technology by highlighting its different applications, contributions, advantages, and future objectives. Following this, we have set a road map for the future work in the context of this technology application extendability in new domains, because it has the potential to enhance the productivity of any sector, where it can be used effectively. With this, we also underscored the architecture requirement to set a preface for this work.

B. Existing Review Articles

In this section, we will discuss the existing review articles that have been published on the security challenges followed by future research directions of SWSN. Although it is very hard to find out a particular paper on this topic, but we will consider the wireless sensor networks paper as well to acknowledge the distinctive factors of our work. In table II, we have summarized the present review articles in the context of their contribution followed by limitations.

III. Layer-wise security threats to SWSN

In this section, we shall discuss various layer-wise security threats that are associated with SWSN to set a foreword for concerned literature. To explore, SWSN uses a wireless communication medium to transmit data from source to destination by following the OSI model. During this process, many internal and external security vulnerability threats arise that can

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

TABLE II: Summary of different surveys paper contributions followed by their limitations

References	*Description and contribution of a paper*	*Limitations*
Osamy et al. [34]	In [34], the author presents a comprehensive survey regarding the different challenges of WSN by particularly taking into account AI-enabled techniques. In this paper, the authors considered a generalized structure of the network with different parameters such as QoS, security, interoperability, and routing protocols, etc.	This article lacks to present the true picture of the security challenges of WSN or SWSN applications.
Ijemaru et al. [35]	In this survey paper, the author presented a comprehensive survey of the existing literature associated with wireless power transfer and energy harvesting technologies WSN. Moreover, the author discussed different challenges related to the wireless power transfer of sensor devices.	In contrast, the authors did not discuss the security challenges that arise during the power transfer of sensor devices. Therefore, we believe that this article lacks to present the true picture of security challenges of these networks.
Ananthi et al. [36]	In this paper, the authors discussed general security challenges associated with WBAN. Furthermore, the authors also discussed different safety, data transmission, and reliability concerns associated with WBAN.	To highlight the limitation of this work, the authors did not follow the template of layerwise attacks to demonstrate the actual challenges that can hamper the operation of WBAN.
Sadkhan et al. [37]	In this review paper, the authors present a detailed survey regarding the present literature of biometric-based authentication schemes by taking into account WSN to highlight unresolved security challenges.	To underscore the limitations of this work, the authors only discussed the security challenges of biometric-based authentication WSN applications.
Al-Nasser et al. [38]	In this paper, the author presented a survey related to the security challenges by taking into account routing protocols in WSN. Different routing protocols have been discussed with their advantages and disadvantages in the context of the security of WSN.	In this paper, the authors only focused on the routing protocols literature associated with security concerns of WSN, but they did not elaborate on other security challenges that can impair the fair operation of these networks.
Huanan et al. [39]	In this survey paper, the authors talked about different applications of WSN followed by their security problems. Although they discussed several problem, but all of them were superficially.	To underline the limitations of this paper, the author superficially discussed the security problems of WSN applications, which does not give a concrete lesson to the readers.
Bhushan et al. [40].	In this paper, the authors highlighted several security threats associated with WSN applications. Despite this, they also discussed the existing authentication and data privacy schemes that had been used to counter them. Although, this was a balanced article for readers to know about different security problems associated with the WSN applications, but it was not good for the specialist, because of underscored limitations.	In contrast to its contribution, the authors did not discuss the potential research direction that can be handy in the solution of underlined security threats, which makes this article useless for the specialist working in this domain.

annihilate or fiddle with the communication process. For this, herein, we would like to highlight layer-wise security threats that had been used in the recent past to disrupt the operation of SWSN applications. Table III summarized these attacks with their expected consequences. For different security threats and their counteractions visual representation and superficial evaluation, we have used figure 2 in the paper. Moreover, we have highlighted different layer-wise attacks that had been used in the recent past to compromise the security of these networks. Following this, we have underscored the existing counteraction techniques that had demonstrated a significant contribution in the redressal of these problems.

IV. Different Countermeasure schemes

In this section, we will discuss the possible defensive counteraction schemes in the context of highlighted security threats. Following the aforementioned security threats, the confidentiality, integrity, authentication, accessibility, and availability of sensor devices accompanied by data transmission must be insured. As mentioned in the preceding section, SWSNs are susceptible to external and internal threats, therefore, both of the attacks should be considered, when it comes to the security concerns of these network applications. In the upcoming sections, we have explored different countermeasures schemes that had been used to mitigate the security threats in SWSN applications.

A. Physical and Data link Layer attacks Counteraction schemes of SWSN

In this segment, we will talk about different techniques that had been used counter the physical layer security threats of SWSN application. To begin, Hu et al. [66] proposed a continuous leakage and tampering resilient scheme for SWSN applications by utilizing a public-key encryption model to counter different external threats to these networks. During the evaluation, the authors checked the key update with a bounded number of tampering queries for an arbitrary key to monitor the time consistency during the authentication process. However, the complex authentication process of this model generates latency and congestion issues in the network. To deal with tampering attacks in WSN, Aldaya et al. [67] proposed an intelligent memory tampering detection-based framework for these networks with the help of a binary GCD-based modular inversion algorithm. Yang et al. [68] extend

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

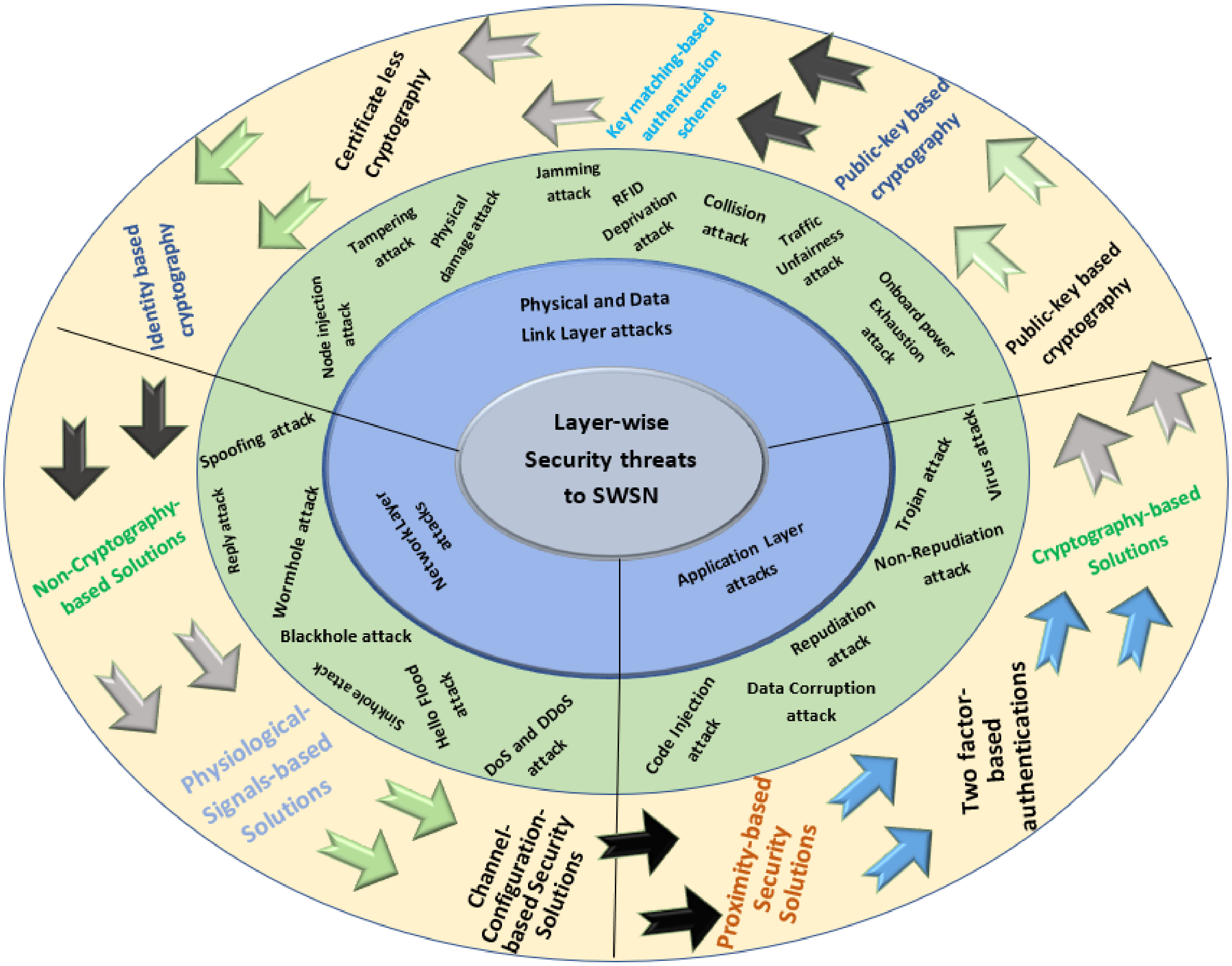


Fig. 2: Layer wise different attacks and their counteraction schemes

TABLE III: Summary of different layer-wise security threats

Layer-name	***Name of Attacks***	***Relevant references***	***Consequences***
Physical Layer attacks on SWSN	Sensor Tampering attacks, sensor physical damage attacks, illegal sensor injection attacks, jamming attack	Adil et al. [41], Osanaiye et al. [42], Sahu et al. [43], Huang et al. [44], Dora et al. [45]	Create signal distortion problems, Congestion, physically damage devices to disrupt their operation, Exhaust embedded battery power, misguide legal traffic with the induction of malicious devices
Data link Layer attacks on SWSN	Hardware based attacks, collision attacks, de-synchronization attacks, sleep deprivation attacks,	Tao et al. [46], Tolba et al. [47], Kim et al. [48], Aghili et al. [49]	create packet loss problems, transmission interference create latency problems, increase chances of contention and congestion
Network Layer attacks on SWSN	Replay attacks, node replication attacks, sybil attack hello flood, sinkhole, blackhole and wormhole attacks, IP spoofing attacks,etc.	De Roode et al. [50], Li et al. [51], Ali et al. [52], Govindasamy et al. [53]	Disturbs the transmission routes, False transmission routes, Data losses with traffic congestion, Fake message errors, Routing loops, Eavesdropping transmitted data, Hello flood
Cross Layer attacks on SWSN	Man in the middle attacks, de-synchronization attack, Denial of Service (DoS) attacks, distributed denial of Service (DDoS) attacks	Aliyu et al. [54], Chaudhry et al. [55], Lakshmi Narayanan et al. [56], Abidoye et al. [57], Liang et al. [58], Abidoye et al. [59]	Disrupt the integrity of transmitted data, reduces the network's ability to carry out anticipated collisions, exhausting energy resources, over functioning of the sensor devices, data transmission to the wrong destination
Application Layer attacks on SWSN	Malicious code injection attacks, spyware attacks, phishing attacks, social engineering attacks, malware injection attacks,etc.	Agrawal et al. [60], Eassa et al. [61], Xia et al. [62], Bera et al. [63], Piplai et al. [64], Pi et al. [65]	Access the legitimate information of clients, compromise the password of a client, misguide the client via illegal links,

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

this discussion and present a comprehensive regarding the present literature associated with the integrity of physical damage attacks followed by tampering attacks on WSN. For a comprehensive study, we suggest that readers and experts interested in tampering and physical attacks need to follow this article.

In self-empowered sensor devices, the EEPROM chip is vulnerable to tampering attacks, as discussed by Skorobogatov et al. [69]. With the security vulnerabilities, the authors also highlighted the possible countermeasure scheme that can be useful against different tampering attacks. In [70], it has been demonstrated that PUF is used as a valuable solution to tackle physical layer attacks such as tampering with devices and EEPROM chip of sensor devices in an operational network of WSN. For the case study of EEPROM chip attacks and their counteraction schemes, we suggested the readers to went through the article [71].

B. Network Layer Counteraction schemes of SWSN

In this segment, we highlight different schemes that are dealing with the security concerns of the network layer of SWSN applications. Farha et al. [72] proposed a timestamp-based scheme for WSN to mitigate replay attacks during communication among legitimate devices. This model was particularly designed for WSN technologies/applications that use ZigBee protocols for their interconnectivity. Likewise, Zhou et al. [73] suggested a permutation and entropy-based hybrid scheme to tackle the security concerns of WSNs associated with replay attacks. Moreover, the authors used the legitimate devices' transmission single regularity parameters to detect these types of attacks. In [74], the author proposed a stochastic coding scheme to handle malicious replay attacks in WSN applications generated by man-in-the-middle or compromised devices. To more comprehensively overview the existing literature associated with replay attacks mitigation schemes, the readers are advised to read the article [75-76].

Kim et al. [77], proposed a physical identification-based trust path routing (PITrust) scheme for WSN utilizing transmission signal strength indicator (RSSI) to detect and prevent Sybil attacks during operational network. To handle Sybil attack issues in the WSN applications employed in digital transportation, Syed et al. [78], proposed a two-phase security-based framework utilizing Public Key Infrastructure (PKI) and hash function algorithms. Different Sybil attacks counteractions are discussed in references [79], if anyone is interested to explore this topic, we suggest them to follow the highlighted survey articles.

In [80], the authors discussed sleep deprivation attacks and proposed a machine learning-enabled clustering-based binary search tree algorithm to address them effectively in WSN. Within this scheme, the authors used a decision tree, long and short-term memory, a support vector machine, and k-nearest neighbor algorithms to ensure the legitimacy of an employed WSN application. Ezhilarasi et al. [81] proposed a novel intrusion detection system for WSN to detect and prevent routing attacks such as hello flood attacks, sybil attacks, wormhole attacks and blackhole attacks, etc, in these networks. To continue this discussion, Raghav et al. [82], proposed a bio-inspired secure routing framework for WSN applications employing bee algorithms. This model uses two important metrics that are known as primary scout bee and secondary scout bee. Both of them are responsible to carry out security checks during transmission with the help of defined security parameters. For a detailed study regarding different routing attack counteractions schemes, we suggest the reader to follow up on the studies of references [83-84].

In [85], the author proposed a Discrete Event System (DES) based Intrusion Detection System (IDS) for WSN networks to tackle IP spoofing-based attacks in these networks. With this, the authors claimed that the suggested prototype is not merely efficacious against IP spoofing attacks, but it has also the capability to oppose the anticipation of malicious nodes in the network. Likewise, Visalakshi et al. [86] proposed an improved whale optimization (IWO) algorithm for WSN applications to tackle the IP spoofing attacks related issues. In this prototype, the authors basically used IDS, where they defined parameters for transmitted signal evaluation to ensure the legitimacy of the network traffic followed by connected devices. To explore the literature related to different countermeasure schemes of IP spoofing attacks by taking into account WSN applications, we suggest the readers and people working in this domain to go through the references [87-88].

C. Application Layer Counteraction schemes of SWSN

In this segment, we will discuss different prototypes that had been used to ensure the security of the application layer of WSN applications. For this, Elmalaki et al. [89] proposed a Context-Aware Adaptation Based Spyware (SpyCon) framework to counter application layer threats of WSN and IoT applications. Following this discussion, Huertas Celdrán et al. [90] proposed a machine learning intelligent framework to counter different application-layer attacks in resource-limited networks. In [91], the author proposed an invisible malicious code detection framework known as CAPPCHA to counter malware attacks in WSN applications. Nauriyal et al. [92] proposed an Artificial neural network (ANN) based framework for WSN applications to address malware-related security challenges in these applications. In this model, the authors considered different classes of data packets to segregate between legal and illegal traffic in the network. In [93], the author suggested an architecture-based model for the industrial internet of things (IIoT) and WSN application to detect and prevent malware anticipation in the network utilizing a hybrid image visualization and deep learning algorithm. Reference [94], present a machine learning-enabled framework utilizing four different datasets to counter malware attacks in WSN and IIoT applications. Here in this article, the authors claimed that the proposed model is very effective against false packet and code detection in real-time traffic, as the detection rate demonstrated 99.5 % accurate results.

Likewise, Jeon et al. [95] proposed a dynamic analysis framework for malware detection in IoT and WSN applications utilizing Convolution Neural Network (CNN) with trained datasets. To explore, the traffic analysis was enabled at the

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

cloud side rather than the edge side with an objective to minimize computation cost, but the edge side devices are still vulnerable to various external and internal threats. Therefore, the applicability of this model in real networks is in a fuzzy state. In [96], the authors proposed a hardware-level malware detection technique for IoT and WSN applications by using the behavior of signatures designed for sensor devices. To explore this topic more, we suggest the involved stakeholders to study references [97-98], for the most recently used counteraction schemes of malware detection in WSN applications.

D. Cross Layer Counteraction schemes of SWSN

In this segment, we will speak about the most recently used cross-layer authentication and data preservation countermeasure schemes of SWSN. To tackle cross-layer security threats in SWSN, WSN, and IoT applications, Kore, et al. [99] proposed a novel prototype known as Cross-Layer and Cryptography-based Secure Routing (CLCSR) scheme. This model is consist of two phases such as a cross-layer mechanism to secure sensor clusters and a lightweight cryptography scheme to ensure the privacy of the user's data in the network. Subashini et al. [100] proposed a secured energy-efficient framework (SEEF) for WSN applications to address the cross-layer security concerns of these applications. This model comprises of two layers to ensure the legitimacy of devices on the client-side followed by data preservation. Reference [101], suggested a cross-layer security framework for WSN to guarantee the security of participating sensor devices of the network. In [102], the author proposed a two-level security framework for WSN and IoT applications to detect malicious packets in real-time. In this first phase, a sniffer was used to assess network traffic based on a decision tree classifier, while in the second phase, they used the correct classified instances (CCIs) algorithms to report malicious packets, if any is detected during the assessment phase.

E. Cryptography and Non-Cryptography based Solutions

In this segment, we will talk about the various cryptographic techniques that had demonstrated remarkable results in the recent past to counter different attacks of the SWNS. To explore this discussion, first of all, we would like to familiarize the readers with different cryptographic breaches. To do so, we have started that these strategies are categorized into two major breaches such as Cryptography and Non-Cryptography techniques. However, these approaches are further categorized in to sub branches, which we will discussed in the upcoming subsections

1) Cryptography based Solutions: In the consequent subparts, we will discuss cryptography-based solutions that had been used to resolve the authentication and data privacy issues in SWNS. By doing this, we will give a broad overview of the latest literature to the readers that what has been done in the recent past and what is likely expected in the future in the context of utilization of these algorithms to address the security concerns of SWSN. To explore, cryptographic-based solutions are further classified into three categorizes, which are discussed below.

2) Public-key based cryptography: Before moving into the detailed discussion, herein, first, we would like to familiarize the readers with public key cryptography/asymmetric cryptography. In this cryptographic model, the authentication is enabled through pairs of key validation and verification such as public and private keys. The pair of keys are generated through the cryptographic technique, which uses and follows one-way functions and mathematical formulations.

a) Key matching based authentication schemes: In this segment, we will disclose different key-matching-based authentication schemes that had been used to ensure the integrity of WSN applications. Moghadam et al. [103], proposed a mutual authentication and key agreement protocol based on ECDH (elliptic-curve Diffie-Hellman) scheme for WSN applications. For comparative analysis, the author considered different communication metrics to claim the effectiveness of this model. Likewise, Alotaibi et al. [104] proposed an enhanced biometric-based anonymous user authentication and the key agreement scheme for WSN applications to ensure the legitimacy and integrity of clients and their information in the network. For formal security analysis, the author used the BAN-logic model to check the usefulness of this scheme against different security threats. For a comprehensive analysis of key-based authentication schemes, we suggest the involved stakeholders to follow up references [105-106].

3) Certificate-less based Cryptography: When it comes to the security of SWSN, the role of certificate-less cryptography can not be ignored, because it has revealed a significant contribution to maintain data integrity, privacy, and preservation. In [122], the author proposed a certificate-less public key cryptography scheme for wireless sensor networks to minimize the authentication complexity on the client side, and improve the operation of constraint-oriented devices. Likewise, Xie et al. [123] proposed an improved certificate-less aggregation signature scheme (iCLAS) for wireless sensor networks to resolve the authentication and data privacy issues in these networks. The results of this model were checked by taking into account different attacks scenario in the simulation environment. Kar et al. [124], extend this discussion and suggested a certificate-less aggregate signature scheme (CL-ASS) for WSN. In this model, the authors considered the storage space and transmission bandwidth of an employed network to improve the communication metrics with the security of WSN. Moreover, the authors checked the resilience of this model against two types of attacks in the context of the computational Diffie–Hellman (CDH) problem assumption.

4) Identity based authentication schemes: In the literature, it has been noted that the researchers used the identities of legitimate sensor devices for their security verification, authentication, and validation in the WSN applications [111]. Therefore, the importance of the identity-based authentication model can not be neglected in WSN applications. To overcome the authentication security challenges in WSN applications, Hassan et al. [112], proposed an identity-based authentication scheme for WSN and IoT applications by taking into account the agriculture sector. Despite the authentication of legitimate devices, the author used hyperelliptic curve cryptography (HECC) algorithm with a hash function to ensure data in-

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

tegrity during transmission. Likewise, Yuvaraj, et al. [113], proposed a lightweight identity based-authentication scheme for WSN and IoT applications utilizing a dual multicast communication infrastructure. In this model, the authentication and data preservation process was improved with help of the EdDS and EdDSA algorithms. To overview the most recently adopted identity-based-authentication schemes, we encouraged the readers and researchers working in this domain to follow up on references [114-115].

5) Signature based authentication schemes: The role of signature based-authentication schemes can not be ignored in the SWSN application. Following this, herein, we would like to highlight the most recently used signature-based-authentication techniques that have demonstrated remarkable results. Kumar et al. [107] proposed a Pairing-Free Identity-based Digital Signature (PF-IBDS) scheme for WSN applications utilizing the Modified Elliptic Curve Cryptography (MECC) and Battle Royal Optimization Algorithm (BROL). The objective of this model was to ensure data security during communication among sensors followed by a remote destination operator. Fathima et al. [108], extend this discussion and proposed a unique signature based-authentication prototype for WSN applications utilizing a simplified encryption technique. However, this model was very complex, therefore, the chances of its real applicability are very limited. Further information regarding the latest signature-based authentication schemes of WSN applications should be found in references [109-110].

6) Two factor based authentication schemes: In the literature, a two factor-based authentication scheme has been used by Wang et al. [116], to manage the authentication and validation problems in WSN applications. Likewise, Jiang et al. [117], had proposed a privacy-aware two-factor authentication scheme for WSN applications utilizing elliptic curve cryptography. Burrows–Abadi–Needham logic framework was used to check the reliability of the proposed model in the context of formal security analysis. In [118], Attkan et al. proposed a lightweight two-factor authentication scheme for WSN applications to resolve their security concerns particularly associated with the verification and validation of legitimate devices. Wu et al. [119] proposed a robust and lightweight two-factor authentication scheme for wireless medical sensor networks (WMSN to guarantee the legitimacy of participating sensor devices in the network. For formal security analysis, the authors used the Proverif tool to check the performance of their model against different security threats. However, for communication metrics, the proposed model was checked in the NS-3 simulation tool. The people interested in this topic are encouraged to overview references [120-121].

F. Non-Cryptography based Solutions

In the security SWSN, the role and importance of non-cryptographic solutions can not be neglected, because they had shown incredible results in the past couple of decades. To familiarize the readers with different techniques of non-cryptographic-based security solutions of SWSN. In the subsequent sections, we will discuss the sub-branches of non-cryptographic techniques that had been utilized in the prevention of different attacks in SWSN.

a) Physiological-Signals-based Solutions: In the recent past, physiological signals had been used as a non-cryptographic data preservation technique to counter different attacks in WSN and SWSN. As a case study, Zhao et al. [125] present a detailed survey of the existing literature to acknowledge the importance of this topic and familiarize the readers and experts with the effectiveness of different non-cryptographic algorithms. In [126], the authors proposed a multiple physiological signals-based data protection scheme for healthcare WSNs to detect transmission manipulation attacks. Nia et al. [127], proposed a physiological signals-based data preservation scheme for healthcare WSN utilizing the acoustic, visual, and electromagnetic signals of source and destination nodes. The resilience of this model was checked against different attacks in the simulation environment to verify its reliability. Moreover, they have compared the results statistics with existing works to ensure the effectiveness of this scheme in their presence of them.

b) Channel-Configuration-based Security Solutions : In WSN and SWSN, proprietary cryptographic algorithms had been used in the recent past to ensure the security of transmitted data by utilizing the client-side electronic devices processing chip. To exemplify this, Azriel et al. [128] suggested a novel non-invasive model using a scan chain approach to automatically detect malicious traffic during the traffic evaluation phase. Moreover, the proposed model scan chains model unfolds the sequential logic at the chip to form a combinational function that is capable to ensure the security of the communication channel before data transmission. Strobel et al. [129] presented a new model to extract malicious codes from the embedded system using the CPU electromagnetic emanation to prevent side-channel attacks in WSN and SWSN. To ensure the physical layer security of WSN and SWSN, Bang et al. [130] proposed a secure cryptographic-enabled modulation technique for these networks. In this model, the authors used a random constellation mapping rule for packet transmission in the network instead of a pre-defined mapping rule such as ”Gray-coded mapping” to guarantee the integrity of information during transmission from source to destination.

c) Proximity-based Security Solutions : In the literature, we have noted that it is very difficult to apply key-based authentication schemes in small-scale WSN/SWSN applications such as smart homes, smart markets, smart healthcare, smart street, etc., because these networks are constituted from mobile devices, which need simple, trustworthy, and reliable authentication models. For the redressal of this problem, the importance of a proximity-based-cryptographic security solution can not be overlooked, because it has the potential to handle this problem cost-effectively. To exemplify, Zhang et al. [131] proposed a proximity-based authentication model known as ”Move2Auth” for smart homes. In this model, the authors ensured the authentication of clients/users through the hand gesture by taking into account the different movements such as forward movement of hands and rotation of hands, etc., to match and validate different variations in a transmitted single to ensure the legitimacy of connected device/users. Xiao et al. [132] used a proximity-based lightweight authentication model for smart homes. In this model, the author considered

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

two scenarios mobility and communication of sensor devices to check the feasibility of validation that had been done successfully.

G. Summary of Discussion

In this part, we familiarized the readers with the different security threats of SWSN applications. The notation behind this familiarization was to set the stage for concerned literature that had been used to counter several existing attacks. Despite this, we have acknowledged the consequences of different attacks to ensure the importance of this topic for future research work. With this, we examined the existing cryptographic and non-cryptographic authentication and data preservation schemes to identify their disadvantages and limitations. Based on this, we have set the foundation for upcoming sections, which will follow these limitations in the context of open security challenges to make footprint for their redressal work.

V. Open research Challenges with Future Research Directions

In the preceding sections, we have discussed modern threats and their countermeasure schemes associated with the hardware, software, and communication SWSN, WSN, and IoT applications. With this, we have underlined the constraints of the existing counteraction schemes in the context of the requirements of SWSN applications. Despite the facts of underscored limitations, SWSN applications are comprised of self-empowered sensor devices, which are connected through Internet technology. Following their wireless communication and open area deployment, these networks offer several security challenges for the research community that is assumed to be an open door for attackers to compromise the security of an employed SWSN application. Therefore, we would like to underline the open security challenges with future research directions to create an atmosphere for all stakeholders interested in the utilization of this technology.

A. Security of SWSN with Scalability ⇒ Challenges 1

Maintaining the security of existing SWSN applications during the scalability of these networks is one of the challenging tasks for the research community, because of the induction of new sensor devices in the network. Following this discussion, how these devices should be synchronized with the existing devices in terms of authentication and validation. Secondly, it is also challenging for people to ensure data privacy during transmission when there is a continuous induction of new devices in the network. Thirdly, secure processing of a high volume of data with scalability is another challenging task, because a large number of devices are interconnected in the network. Fourthly, how the computation complexity of these devices should be managed, when it comes to a large number of devices authentication in a heterogeneous network, as these devices are resource-limited in terms of memory, processing, and energy, etc.

1) Future Research Direction ⇒ Challenges 1: To address the highlighted challenges correlated with the scalability of SWSN applications in the context of security concerns. We suggest the research societies and industry stakeholders to consider blockchain technology infrastructure while designing new security hardware chips, software, routing protocols, authentication, and data preservation schemes because it has the capability to ensure decentralized authentication and data privacy during the communication process among self-empowered sensor devices followed remote destination. With the utilization of blockchain technology, many computation problems can be resolved with reliable communication metrics. Despite this, incremental Learning should be used as an alternative technology to resolve this problem effectively. Therefore, we believe that the involved stakeholder will use this technology to manage the security concerns of SWSN applications in the future.

B. Security of SWSN with Interoperability ⇒ Challenges 2

In SWSN applications, the interoperability of sensor devices, application requirements, organization standards, and client needs arise numerous security challenges for the research community that can hamper the operation of an employed network followed by the use of concerning technology in the future. Therefore, we would like to emphasis on the open security challenges that can play a vital role in the future of this technology. To explore this topic, herein, we would like to accentuate different interoperability challenges.

Firstly, when it comes to the interoperability of different sensor devices (different vendors) how cost-effective authentication should be ensured among participating devices in the network. Secondly, how the organizational standard would be maintained with proper security protocols when different vendor devices are communicating with each other in one network topological order. This is another challenging task for the research community. Thirdly, how secure firmware updates should be enabled for the client-side devices during operational network, this is also a very hectic problem, when it comes to the interconnectivity of different vendor devices. Fourthly, the application accessibility omnipresent is another challenging task, because of how the users should be familiarized with the security protocol. Following the aforestated challenges in the below part, we will suggest the possible research directions that could be helpful in the redressal of these problems.

1) Future Research Direction ⇒ Challenges 2: To manipulate the interoperability challenges associated with security concerns of SWSN applications, we suggest the researcher's communities to focus on the interoperability technology such as APIs, routing protocols, software, and hardware of self-empowered devices during the design, connectivity, and interoperability phase. This will be helpful to maintain the security protocols in these applications with significant results in terms of authentication, access control policies, data privacy, and service authorization. With the help of these technologies, we believe that they will not only fix the security problems of the SWSN applications but will also be in position to improve

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

the communication metrics in terms of QoS standards to gain the attention of new interested stakeholders in utilization of this technology in the future. Moreover, ML and DL-enabled techniques should be also used the manage the interoperability concerns of these applications securely. Following this, we suggest the involve stakeholders to set international security standards for the interoperability of SWSN applications because this will help to compel the industry and research community to follow them while working on the new hardware, software, protocols, APIs and interconnectivity of these applications.

C. Security problems with heterogeneous network key distribution ⇒ Challenges 3

In this segment, we will discuss the open security problems key distribution in SWSN applications. Keeping in view the limited resources of self-empowered sensor devices, it is hard for them to manage a large number of keys in their built-in memory. To address this problem, the research community needs to work effectively to design reliable key distribution and authentication schemes for these applications. Moreover, the existing literature follows a centralized authentication authority for key distribution and management, which creates congestion and contention problems in the network. For redressal of this problem, new reliable key distribution and management schemes are the utmost requirement of these networks.

1) Future Research Direction ⇒ Challenges 3: In this segment, we will discuss different future research directions that could be useful to tackle the key distribution problem in heterogeneous SWSN applications. To enable decentralized key distribution, authentication, and management in SWSN applications, the role of SDN technology can not be ignored, because it has the capability to manage the aforesaid concerns of key manipulation of keys via SDN controllers. With the help of these controllers, the computation complexities during authentication and key distribution can be minimized up to a great extent that would be useful to improve the communication metrics of these networks. Therefore, we suggest the people working in this to think about SDN technology for future research work, when it comes to the decentralized key authentication and management of SWSN applications. Likewise, DL and RL-enabled could be helpful as well to manage the key distribution of an employed network, because it has the capability of intelligence. Thus, we also suggest the research community to design reliable datasets, when it comes to the distribution of SWSN applications to improve the communication metrics of these networks in the future.

D. Security problems with Syntactic and Semantic ⇒ Challenges 4

In heterogeneous SWSN applications, the legitimate self-empowered devices and transmitted data are susceptible to various security threats, due to syntactic and semantic interoperability, because different vendors devices create these problems. To explore, this is very challenging task for the researchers to ensure the security of self-empowered devices, when it comes to the syntactic and semantic synchronization during operational network. To continue, in SWSN applications different vendors devices are communicating with each other for the sake of one objective to achieve the required goal. But these devices have firmware, which makes the authentication process, due to syntactic and semantic problems. Therefore, this challenging task also need the involved stakeholder attention to address them within the range of define security protocols.

1) Future Research Direction ⇒ Challenges 4: To address the security challenges associated with Syntactic and Semantic interoperability of SWSN applications, the role of machine learning algorithms and Natural Languages Processing (NLP) can be skipped, because they have the capability to anomalies in the network based on their past behavior. Despite this, NLP is capable to detect new attacks without the past knowledge of their behavior. Therefore, we believe that artificial intelligence, machine learning algorithms, and NLPs could be extremely useful to in the future to address the challenges interlinked with the Syntactic and Semantic interoperability of SWSN applications.

E. Security Problems with Management and Automation ⇒ Challenge 5

SWSN applications used in the industry enable and allow the machines to operate in an automated fashion. With this feature, they have shown significant contributions in the productivity of different industrial products. Although they are very useful in their task handling, but, at the same time, they are very sensitive in terms of operations, if an intruder misguides them, then they disrupt the whole operation of an industrial set-up. Therefore, secure management of these devices in real-time is a challenging task for the research community and enterprise market producers to ensure their reliable operation. For this, some work has been done in the recent past, but it does not support heterogeneous networks. Therefore, we suggest the concerned stakeholders to pay attention to this important issue and devise security schemes for this technology.

1) Future Research Direction ⇒ Challenges 5: To address this security challenge, the research community and industry stakeholders need to design a reliable firmware and software platform. Moreover, we also suggesting the research community that the new paradigm would be capable to authenticate each connected device with pre-firmware update time to ensure the legitimacy of participating devices in the network.

VI. Lesson Learned and Comparative analysis

Here in this section, we would like to summarize what we have learned in this article by taking in account the existing security threats of SWSN, WSN, and IoT applications followed by their counteraction schemes, while considering the requirement of these applications. To explore, we would like the answer the question of reviewers and editors of why this review article is needed in the existence of state-of-the-art review articles on this topic. For this, we will consider each section of our article and compare it with competitors'

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

TABLE IV: Distinctive Results analysis with Competitor papers
Superficially overviewed (⊖), comprehensively discussed (√), Haven't discussed (⊗),
Open Research Challenges (ORC) and Future research directions (FRD)

Name of Comparative Metrics	***Osamy et al. [34]***	***Ijemaru et al. [35]***	***Ananthi et al. [36]***	***Sadkhan et al. [37]***	***Al-Nasser et al. [38]***	***Huanan et al. [39]***	***Our survey paper***
Physical Layer Counteraction schemes	⊖	⊖	√	⊖	√	⊗	√
Network Layer Counteraction schemes	⊖	√	⊖	⊖	√	√	√
Cross Layer Counteraction schemes	⊗	⊖	⊗	√	⊗	√	√
Applications Layer Counteraction schemes	⊗	⊗	⊖	√	√	√	√
Security Challenges with Network Scalability ⇒ Challenges 1	⊖	⊗	⊗	⊖	√	⊗	√
Security Challenges with Syntactic and Semantic ⇒ Challenges 2	⊗	⊗	⊗	⊗	⊖	⊖	√
Security Challenges with Interoperability ⇒ Challenges 3	⊖	√	⊖	⊖	⊖	√	√
Security Challenges with Heterogeneity ⇒ Challenges 4	⊖	⊗	√	⊗	⊖	⊖	√
Future Research Direction ⇒ Challenges 1	⊗	⊗	⊗	⊖	⊖	⊗	√
Future Research Direction ⇒ Challenges 2	⊖	⊗	⊗	⊗	⊗	⊗	√
Future Research Direction ⇒ Challenges 3	⊗	√	⊖	⊖	⊗	⊖	√
Future Research Direction ⇒ Challenges 4	⊖	⊗	√	⊖	√	⊖	√

survey papers to acknowledge that what are those important points that we have addressed in this paper, and missed by rival papers. To do so, we have added table IV, in the paper for comparative analysis.

VII. Conclusion

In this paper, we have presented a comprehensive survey regarding the current literature associated with the susceptibility and counteraction schemes of SWSN applications. Initially, we familiarize the readers with the taxonomy of SWSN, while in the consequent phase, we have explored the layer-wise security threats of these applications to set a preface for the relevant literature that had been used to counter these threats. After a detailed discussion of the latest counteraction schemes, we moved one step forward to identify the open security challenges of SWSN applications by following the requirements of these networks. Based on identified challenges, we set the road for future research by highlighting potential areas that could be productive in these network security and communication. Finally, we conducted a comparative study in order to assert the originality of this work in the presence of competitive articles, and provide an explanation for why this paper is necessary in their existence. With the collection of these all, we have presented a complete package for the students, industry stakeholders, and researchers working in this domain to design a foolproof security framework for SWSN application in the future that could be capable to achieve better communication and computation metrics.

Acknowledgment

Authors would like to thank Taif University Researchers for Supporting Project Number (TURSP-2020/228), Taif University, Taif, Saudi Arabia.

References

[1] Adil, M., Alshahrani, H., Rajab, A., Shaikh, A., Song, H., & Farouk, A. (2022). QoS Review: Smart Sensing in Wake of COVID-19, Current Trends and Specifications with Future Research Directions. IEEE Sensors Journal.

[2] Adil, M., Attique, M., Khan, M. M., Ali, J., Farouk, A., & Song, H. (2022). HOPCTP: A Robust Channel Categorization Data Preservation Scheme for Industrial Healthcare Internet of Things. IEEE Transactions on Industrial Informatics.

[3] Jan, M. A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., & Stergiou, N. (2021). LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. IEEE Transactions on Green Communications and Networking, 5(3), 1202-1211

[4] Zhou, Z., Wang, Z., Yu, H., Liao, H., Mumtaz, S., Oliveira, L., & Frascolla, V. (2020). Learning-based URLLC-aware task offloading for internet of health things. IEEE Journal on Selected Areas in Communications, 39(2), 396-410.

[5] Strielkina, A., Illiashenko, O., Zhydenko, M., & Uzun, D. (2018, May). Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 67-73). IEEE

[6] Zhang, J., Ma, M., Wang, P., & Sun, X. D. (2021). Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions. Journal of Systems Architecture, 117, 102098.

[7] Ujjan, R. M. A., Pervez, Z., Dahal, K., Bashir, A. K., Mumtaz, R., & González, J. (2020). Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems, 111, 763-779.

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

[8] Ullah, R., Ullah, S., Faisal, F., Ullah, R., Mabrouk, I. B., Al Hasan, M. J., & Kamal, B. (2021). A novel multi-band and multi-generation (2G, 3G, 4G, and 5G) 9-elements MIMO antenna system for 5G smartphone applications. Wireless Networks, 27(7), 4825-4837.

[9] Busari, S. A., Huq, K. M. S., Mumtaz, S., & Rodriguez, J. (2019, May). Terahertz massive MIMO for beyond-5G wireless communication. In ICC 2019-2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[10] Qiao, F., Wu, J., Li, J., Bashir, A. K., Mumtaz, S., & Tariq, U. (2020). Trustworthy edge storage orchestration in intelligent transportation systems using reinforcement learning. IEEE Transactions on Intelligent Transportation Systems, 22(7), 4443-4456.

[11] Song, Z., Ye, W., Chen, Z., Chen, Z., Li, M., Tang, W., ... & Fan, Z. (2021). Wireless self-powered high-performance integrated nanostructured-gas-sensor network for future smart homes. ACS nano, 15(4), 7659-7667.

[12] Adil, M., & Khan, M. K. (2021). Emerging iot applications in sustainable smart cities for covid-19: Network security and data preservation challenges with future directions. Sustainable Cities and Society, 75, 103311

[13] Swamy, T. J., Ramamurthy, G., & Nayak, P. (2019). Optimal, secure cluster head placement through source coding techniques in wireless sensor networks. IEEE Communications Letters, 24(2), 443-446.

[14] Boukerche, A., Wu, Q., & Sun, P. (2019). Efficient green protocols for sustainable wireless sensor networks. IEEE Transactions on Sustainable Computing, 5(1), 61-80.

[15] Deng, Z., Wu, Q., Lv, X., Zhu, B., Xu, S., & Wang, X. (2019, August). Application analysis of wireless sensor networks in nuclear power plant. In International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plant (pp. 135-148). Springer, Singapore.

[16] Patil, S. A., & Deshpande, P. (2019, May). Monitoring Air Pollutants Using Wireless Sensor Networks. In International Conference on Computer Networks and Inventive Communication Technologies (pp. 1-8). Springer, Cham.

[17] Rajasekaran, T., & Anandamurugan, S. (2019). Challenges and applications of wireless sensor networks in smart farming—a survey. Advances in big data and cloud computing, 353-361.

[18] Mao, F., Khamis, K., Krause, S., Clark, J., & Hannah, D. M. (2019). Low-cost environmental sensor networks: recent advances and future directions. Frontiers in Earth Science, 7, 221

[19] Vera-Amaro, R., Angeles, M. E. R., & Luviano-Juarez, A. (2019). Design and analysis of wireless sensor networks for animal tracking in large monitoring polar regions using phase-type distributions and single sensor model. IEEE Access, 7, 45911-45929

[20] Hamouda, Y. E., & Msallam, M. M. (2019). Smart heterogeneous precision agriculture using wireless sensor network based on extended Kalman filter. Neural Computing and Applications, 31(9), 5653-5669.

[21] Catini, A., Papale, L., Capuano, R., Pasqualetti, V., Di Giuseppe, D., Brizzolara, S., ... & Di Natale, C. (2019). Development of a sensor node for remote monitoring of plants. Sensors, 19(22), 4865.

[22] Zorbas, D., & O'Flynn, B. (2019, May). A network architecture for high volume data collection in agricultural applications. In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 578-583). IEEE

[23] Hajar, M. S., Al-Kadri, M. O., & Kalutarage, H. K. (2021). A survey on wireless body area networks: Architecture, security challenges and research opportunities. Computers & Security, 104, 102211

[24] Gundall, M., Strufe, M., Schotten, H. D., Rost, P., Markwart, C., Blunk, R., ... & Wübben, D. (2021). Introduction of a 5G-enabled architecture for the realization of industry 4.0 use cases. IEEE access, 9, 25508-25521

[25] Adil, M., Ali, J., Khan, M. S., Kim, J., Alturki, R., Zakarya, M., ... & Kim, S. M. (2021). An Intelligent Hybrid Mutual Authentication Scheme for Industrial Internet of Thing Networks. CMC-COMPUTERS MATERIALS & CONTINUA, 68(1), 447-470

[26] Alibakhshikenari, M., Virdee, B. S., Azpilicueta, L., Naser-Moghadasi, M., Akinsolu, M. O., See, C. H., ... & Limiti, E. (2020). A comprehensive survey of "metamaterial transmission-line based antennas: design, challenges, and applications". IEEE Access, 8, 144778-144808.

[27] Alibakhshikenari, M., Babaeian, F., Virdee, B. S., Aïssa, S., Azpilicueta, L., See, C. H., ... & Limiti, E. (2020). A comprehensive survey on "Various decoupling mechanisms with focus on metamaterial and metasurface principles applicable to SAR and MIMO antenna systems". IEEE Access, 8, 192965-193004.

[28] Alibakhshikenari, M., Ali, E. M., Soruri, M., Dalarsson, M., Naser-Moghadasi, M., Virdee, B. S., ... & Limiti, E. (2022). A comprehensive survey on antennas on-chip based on metamaterial, metasurface, and substrate integrated waveguide principles for millimeter-waves and terahertz integrated circuits and systems. IEEE Access.

[29] Nadeem, I., Alibakhshikenari, M., Babaeian, F., Althuwayb, A., Virdee, B. S., Azpilicueta, L., ... & Limiti, E. (2021). A comprehensive survey on" circular polarized antennas" for existing and emerging wireless communication technologies. Journal of Physics D: Applied Physics.

[30] Shi, W., Xu, W., You, X., Zhao, C., & Wei, K. (2022). Intelligent Reflection Enabling Technologies for Integrated and Green Internet-of-Everything Beyond 5G: Communication, Sensing, and Security. IEEE Wireless Communications.

[31] Curiac, D. I. (2016). Wireless sensor network security enhancement using directional antennas: State of the art and research challenges. Sensors, 16(4), 488.

[32] Mohapatra, H., & Rath, A. K. (2021). An IoT based efficient multi-objective real-time smart parking system. International journal of sensor networks, 37(4), 219-232

[33] Tam, N. T., Hung, T. H., & Binh, H. T. T. (2021). A decomposition-based multi-objective optimization approach for balancing the energy consumption of wireless sensor networks. Applied Soft Computing, 107, 107365

[34] Osamy, W., Khedr, A. M., Salim, A., AlAli, A. I., & El-Sawy, A. A. (2022). Recent Studies Utilizing Artificial Intelligence Techniques for Solving Data Collection, Aggregation and Dissemination Challenges in Wireless Sensor Networks: A Review. Electronics, 11(3), 313

[35] Ijemaru, G. K., Ang, K. L. M., & Seng, J. K. (2022). Wireless power transfer and energy harvesting in distributed sensor networks: Survey, opportunities, and challenges. International Journal of Distributed Sensor Networks, 18(3), 15501477211067740.

[36] Ananthi, J. V., & Jose, P. (2021). A perspective review of security challenges in body area networks for healthcare applications. International Journal of Wireless Information Networks, 28(4), 451-466

[37] Sadkhan, S. B., & Jafar, M. S. (2021, October). Biometric Based Wireless Network Security-Status, Challenges and Future Trends. In 2021 International Conference on Advance of Sustainable Engineering and its Application (ICASEA) (pp. 236-241). IEEE.

[38] Al-Nasser, A., Almesaeed, R., & Al-Junaid, H. (2021). A Comprehensive Survey on Routing and Security in Mobile Wireless Sensor Networks. International Journal of Electronics and Telecommunications, 67.

[39] Huanan, Z., Suping, X., & Jiannan, W. (2021). Security and application of wireless sensor network. Procedia Computer Science, 183, 486-492.

[40] Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Personal Communications, 98(2), 2037-2077.

[41] Adil, M., Almaiah, M. A., Omar Alsayed, A., & Almomani, O. (2020). An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks. Sensors, 20(8), 2311.

[42] Osanaiye, O., Alfa, A. S., & Hancke, G. P. (2018). A statistical approach to detect jamming attacks in wireless sensor networks. Sensors, 18(6), 1691

[43] Sahu, M., Sethi, N., & Das, S. K. (2022, April). A Survey on Detection of Malicious Nodes in Wireless Sensor Networks. In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 710-715). IEEE

[44] Huang, D. W., Liu, W., & Bi, J. (2021). Data tampering attacks diagnosis in dynamic wireless sensor networks. Computer Communications, 172, 84-92

[45] Dora, J. R., & Nemoga, K. (2021). Clone node detection attacks and mitigation mechanisms in static wireless sensor networks. Journal of Cybersecurity and Privacy, 1(4), 553-579

[46] Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2018). Secured data collection with hardware-based ciphers for IoT-based healthcare. IEEE Internet of Things Journal, 6(1), 410-420.

[47] Tolba, A. M. R. (2018). Trust-based distributed authentication method for collision attack avoidance in VANETs. IEEE Access, 6, 62747-62755.

[48] Kim, S. Y., & Moon, J. S. (2021). Sleep Deprivation Attack Detection Based on Clustering in Wireless Sensor Network. Journal of the Korea Institute of Information Security & Cryptology, 31(1), 83-97.

[49] Aghili, S. F., Ashouri-Talouki, M., & Mala, H. (2018). DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT. The Journal of Supercomputing, 74(1), 509-525.

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

[50] De Roode, G., Ullah, I., & Havinga, P. J. (2018, December). How to break IOTA heart by replaying?. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-7). IEEE

[51] Li, L., Xu, G., Jiao, L., Li, X., Wang, H., Hu, J., ... & Gao, H. (2019). A secure random key distribution scheme against node replication attacks in industrial wireless sensor systems. IEEE Transactions on Industrial Informatics, 16(3), 2091-2101

[52] Ali, S., Khan, M. A., Ahmad, J., Malik, A. W., & ur Rehman, A. (2018, April). Detection and prevention of Black Hole Attacks in IOT & WSN. In 2018 third international conference on fog and mobile edge computing (FMEC) (pp. 217-226). IEEE

[53] Govindasamy, J., & Punniakody, S. (2018). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology, 5(3), 735-744

[54] Aliyu, F., Sheltami, T., & Shakshuki, E. M. (2018). A detection and prevention technique for man in the middle attack in fog computing. Procedia computer science, 141, 24-31

[55] Chaudhry, S. A. (2021). Combating identity de-synchronization: an improved lightweight symmetric key based authentication scheme for IoV. Journal of Network Intelligence, 6, 12.

[56] Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y., & Shanmuganathan, V. (2021). Machine learning based detection and a novel EC-BRTT algorithm based prevention of DoS attacks in wireless sensor networks. Wireless Personal Communications, 1-25.

[57] Abidoye, A. P., & Obagbuwa, I. C. (2018). DDoS attacks in WSNs: detection and countermeasures. IET Wireless Sensor Systems, 8(2), 52-59.

[58] Liang, L., Zheng, K., Sheng, Q., & Huang, X. (2016, December). A denial of service attack method for an iot system. In 2016 8th international conference on Information Technology in Medicine and Education (ITME) (pp. 360-364). IEEE.

[59] Abidoye, A. P., & Ochola, E. O. (2018). Denial of service attacks in wireless sensor networks with proposed countermeasures. In Information Technology-New Generations (pp. 185-191). Springer, Cham

[60] Agrawal, S., Das, M. L., & Lopez, J. (2018). Detection of node capture attack in wireless sensor networks. IEEE Systems Journal, 13(1), 238-247

[61] Eassa, A. M., Elhoseny, M., El-Bakry, H. M., & Salama, A. S. (2018). NoSQL injection attack detection in web applications using RESTful service. Programming and Computer Software, 44(6), 435-444.

[62] Xia, H., Li, L., Cheng, X., Liu, C., & Qiu, T. (2020). A dynamic virus propagation model based on social attributes in city IoT. IEEE Internet of Things Journal, 7(9), 8036-8048

[63] Bera, B., Das, A. K., Obaidat, M. S., Vijayakumar, P., Hsiao, K. F., & Park, Y. (2020). AI-enabled blockchain-based access control for malicious attacks detection and mitigation in IoE. IEEE Consumer Electronics Magazine, 10(5), 82-92.

[64] Piplai, A., Ranade, P., Kotal, A., Mittal, S., Narayanan, S. N., & Joshi, A. (2020, December). Using knowledge graphs and reinforcement learning for malware analysis. In 2020 IEEE International Conference on Big Data (Big Data) (pp. 2626-2633). IEEE

[65] Pi, W., Yang, P., Duan, D., Chen, C., Cheng, X., Yang, L., & Li, H. (2020). Malicious user detection for cooperative mobility tracking in autonomous driving. IEEE internet of things journal, 7(6), 4922-4936.

[66] Hu, C., Yang, R., Liu, P., Li, T., & Kong, F. (2019). A countermeasure against cryptographic key leakage in cloud: public-key encryption with continuous leakage and tampering resilience. The Journal of Supercomputing, 75(6), 3099-3122

[67] Aldaya, A. C., Brumley, B. B., Sarmiento, A. J. C., & Sánchez-Solano, S. (2019). Memory tampering attack on binary gcd based inversion algorithms. International Journal of Parallel Programming, 47(4), 621-640.

[68] Yang, B., Guo, L., Li, F., Ye, J., & Song, W. (2019). Vulnerability assessments of electric drive systems due to sensor data integrity attacks. IEEE Transactions on Industrial Informatics, 16(5), 3301-3310.

[69] Skorobogatov, S. (2018). Hardware security implications of reliability, remanence, and recovery in embedded memory. Journal of Hardware and Systems Security, 2(4), 314-321.

[70] Mall, P., Amin, R., Das, A. K., Leung, M. T., & Choo, K. K. R. (2022). PUF-based authentication and key agreement protocols for IoT, WSNs and smart grids: a comprehensive survey. IEEE Internet of Things Journal

[71] Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), 17-25.

[72] Farha, F., Ning, H., Zhang, W., & Choo, K. K. R. (2020). Timestamp scheme to mitigate replay attacks in secure ZigBee networks. IEEE Transactions on Mobile Computing

[73] Zhou, M., Zhang, Z., & Xie, L. (2021). Permutation entropy based detection scheme of replay attacks in industrial cyber-physical systems. Journal of the Franklin Institute, 358(7), 4058-4076

[74] Ye, D., Zhang, T. Y., & Guo, G. (2019). Stochastic coding detection scheme in cyber-physical systems against replay attack. Information Sciences, 481, 432-444.

[75] Singh, M., & Pati, D. (2020). Countermeasures to replay attacks: A review. IETE Technical Review, 37(6), 599-614

[76] Wang, X., Yan, Z., Zhang, R., & Zhang, P. (2021). Attacks and defenses in user authentication systems: A survey. Journal of Network and Computer Applications, 188, 103080

[77] Kim, J. D., Ko, M., & Chung, J. M. (2022). Physical Identification Based Trust Path Routing Against Sybil Attacks on RPL in IoT Networks. IEEE Wireless Communications Letters, 11(5), 1102-1106

[78] Syed, S. A., & Prasad, B. V. V. S. (2019, April). Merged technique to prevent SYBIL Attacks in VANETs. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[79] Bang, A. O., Rao, U. P., Kaliyar, P., & Conti, M. (2022). Assessment of Routing Attacks and Mitigation Techniques with RPL Control Messages: A Survey. ACM Computing Surveys (CSUR), 55(2), 1-36.

[80] Pu, C. (2020). Sybil attack in RPL-based internet of things: analysis and defenses. IEEE Internet of Things Journal, 7(6), 4937-4949.

[81] Ezhilarasi, M., Gnanaprasanambikai, L., Kousalya, A., & Shanmugapriya, M. (2022). A novel implementation of routing attack detection scheme by using fuzzy and feed-forward neural networks. Soft Computing, 1-12

[82] Raghav, R. S., Thirugnansambandam, K., & Anguraj, D. K. (2020). Beeware routing scheme for detecting network layer attacks in wireless sensor networks. Wireless Personal Communications, 112(4), 2439-2459

[83] Naik, A. S., & Murugan, R. (2018). Security attacks and energy efficiency in wireless sensor networks: A survey. International Journal of Applied Engineering Research, 13(1), 107-112.

[84] Sharma, N., Kaushik, I., Agarwal, V. K., Bhushan, B., & Khamparia, A. (2021). Attacks and security measures in wireless sensor network. Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 237-268.

[85] Ray, D., Bhale, P., Biswas, S., Nandi, S., & Mitra, P. (2021, December). DAISS: Design of an Attacker Identification Scheme in CoAP Request/Response Spoofing. In TENCON 2021-2021 IEEE Region 10 Conference (TENCON) (pp. 941-946). IEEE

[86] Visalakshi, P., & Prabakaran, S. (2020). Detection and prevention of spoofing attacks in mobile adhoc networks using hybrid optimization algorithm. Journal of Intelligent & Fuzzy Systems, 38(2), 1691-1704.

[87] Nandhini, P. S., Kuppuswami, S., & Malliga, S. (2021). Energy efficient thwarting rank attack from RPL based IoT networks: A review. Materials Today: Proceedings.

[88] Hijazi, S., & Obaidat, M. S. (2019). Address resolution protocol spoofing attacks and security approaches: A survey. Security and Privacy, 2(1), e49.

[89] Elmalaki, S., Ho, B. J., Alzantot, M., Shoukry, Y., & Srivastava, M. (2019, May). Spycon: Adaptation based spyware in human-in-the-loop iot. In 2019 IEEE Security and Privacy Workshops (SPW) (pp. 163-168). IEEE.

[90] Huertas Celdrán, A., Sánchez Sánchez, P. M., Sisi, F., Bovet, G., Martínez Pérez, G., & Stiller, B. (2022). Creation of a Dataset Modeling the Behavior of Malware Affecting the Confidentiality of Data Managed by IoT Devices. In Robotics and AI for Cybersecurity and Critical Infrastructure in Smart Cities (pp. 193-225). Springer, Cham.

[91] Guerar, M., Merlo, A., Migliardi, M., & Palmieri, F. (2018). Invisible CAPPCHA: A usable mechanism to distinguish between malware and humans on the mobile IoT. computers & security, 78, 255-266.

[92] Nauriyal, V., Mittal, K., Pundir, S., Wazid, M., & Singh, D. P. (2020, May). ANN-Based Multi-class Malware Detection Scheme for IoT Environment. In International Conference on Information and Communication Technology for Intelligent Systems (pp. 269-277). Springer, Singapore.

[93] Naeem, H., Ullah, F., Naeem, M. R., Khalid, S., Vasan, D., Jabbar, S., & Saeed, S. (2020). Malware detection in industrial internet of things based on hybrid image visualization and deep learning model. Ad Hoc Networks, 105, 102154

[94] Pundir, S., Obaidat, M. S., Wazid, M., Das, A. K., Singh, D. P., & Rodrigues, J. J. (2021). MADP-IIME: malware attack detection protocol in IoT-enabled industrial multimedia environment using machine learning approach. Multimedia Systems, 1-13

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

[95] Jeon, J., Park, J. H., & Jeong, Y. S. (2020). Dynamic analysis for IoT malware detection with convolution neural network model. IEEE Access, 8, 96899-96911

[96] Bahador, M. B., Abadi, M., & Tajoddin, A. (2019). HLMD: a signature-based approach to hardware-level behavioral malware detection and classification. The Journal of Supercomputing, 75(8), 5551-5582.

[97] Wazid, M., Das, A. K., Rodrigues, J. J., Shetty, S., & Park, Y. (2019). IoMT malware detection approaches: analysis and research challenges. IEEE Access, 7, 182459-182476.

[98] Naseer, M., Rusdi, J. F., Shanono, N. M., Salam, S., Muslim, Z. B., Abu, N. A., & Abadi, I. (2021, April). Malware detection: issues and challenges. In Journal of Physics: Conference Series (Vol. 1807, No. 1, p. 012011). IOP Publishing

[99] Kore, A., & Patil, S. (2022). Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. Wireless Networks, 28(1), 287-301

[100] Subashini, S., & Mathiyalagan, P. (2020). A cross layer design and flower pollination optimization algorithm for secured energy efficient framework in wireless sensor network. Wireless Personal Communications, 112(3), 1601-1628

[101] Devaraju, B. M., & Raju, G. T. (2018, December). Cross Layer and Management Plane Integration Approach for Detection and Prevention of Malicious Activities in WSN. In 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1831-1838). IEEE

[102] Amouri, A., D. Morgera, S., A. Bencherif, M., & Manthena, R. (2018). A cross-layer, anomaly-based IDS for WSN and MANET. Sensors, 18(2), 651

[103] Moghadam, M. F., Nikooghadam, M., Al Jabban, M. A. B., Alishahi, M., Mortazavi, L., & Mohajerzadeh, A. (2020). An efficient authentication and key agreement scheme based on ECDH for wireless sensor network. IEEE Access, 8, 73182-73192

[104] Alotaibi, M. (2018). An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access, 6, 70072-70087.

[105] Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 1-27.

[106] Sundararajan, A. D. D., & Rajashree, R. (2022). A Comprehensive Survey on Lightweight Asymmetric Key Cryptographic Algorithm for Resource Constrained Devices. ECS Transactions, 107(1), 7457.

[107] Kumar, V., & Ray, S. (2022). Pairing-free identity-based digital signature algorithm for broadcast authentication based on modified ECC using battle royal optimization algorithm. Wireless Personal Communications, 123(3), 2341-2365.

[108] Fathima, N., Banu, R., & Ahammed, G. F. A. (2022). A signature-based data security and authentication framework for internet of things applications. International Journal of Electrical & Computer Engineering (2088-8708), 12(3).

[109] Hussain, S., Ullah, S. S., Ali, I., Xie, J., & Inukollu, V. N. (2022). Certificateless signature schemes in Industrial Internet of Things: A comparative survey. Computer Communications, 181, 116-131.

[110] Mehta, M., & Patel, K. (2022). A Survey on IoT Authentication Security Service: Open Issues, Security Threats, and Future Solution Direction. International Journal of Systems and Software Security and Protection (IJSSSP), 13(1), 1-13.

[111] Kumar, Ashish, Rahul Saha, Mauro Conti, Gulshan Kumar, William J. Buchanan, and Tai Hoon Kim. "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions." Journal of Network and Computer Applications (2022): 103414.

[112] Hassan, B., AlSanad, A. A., Ullah, I., Amin, N. U., Khan, M. A., Uddin, M. I., & Wu, J. M. T. (2022). A Cost Effective Identity-Based Authentication Scheme for Internet of Things-Enabled Agriculture. Wireless Communications and Mobile Computing, 2022.

[113] Yuvaraj, N., Raja, R. A., Karthikeyan, T., & Praghash, K. (2022). Improved authentication in secured multicast wireless sensor network (MWSN) using opposition frog leaping algorithm to resist man-in-middle attack. Wireless Personal Communications, 123(2), 1715-1731.

[114] Garg, S., Nayak, S., Bavani Sankar, A. B., & Maity, S. (2022). Applications of Identity-Based Cryptography in Smart Home and Healthcare: A Recent Review. Cyber Security in Intelligent Computing and Communications, 227-241

[115] Puli, S., & Smitha Chowdary, C. H. (2022). A Survey on Trust-Based Node Validation Model in Internet of Things. In Pervasive Computing and Social Networking (pp. 351-360). Springer, Singapore.

[116] Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics, 14(9), 4081-4092.

[117] Jiang, Q., Kumar, N., Ma, J., Shen, J., He, D., & Chilamkurti, N. (2017). A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks. International Journal of Network Management, 27(3), e1937

[118] Attkan, A., & Ahlawat, P. (2020). Lightweight two-factor authentication protocol and session key generation scheme for WSN in IoT deployment. In Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies (pp. 189-198). Springer, Singapore.

[119] Wu, F., Li, X., Sangaiah, A. K., Xu, L., Kumari, S., Wu, L., & Shen, J. (2018). A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems, 82, 727-737

[120] Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. (2019, February). Multi-factor authentication in cyber physical system: A state of art survey. In 2019 21st international conference on advanced communication technology (ICACT) (pp. 279-284). IEEE

[121] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1

[122] Kumar, P., Kumari, S., Sharma, V., Sangaiah, A. K., Wei, J., & Li, X. (2018). A certificateless aggregate signature scheme for healthcare wireless sensor network. Sustainable Computing: Informatics and Systems, 18, 80-89.

[123] Xie, Y., Li, X., Zhang, S., & Li, Y. (2019). $iCLAS$: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks. IEEE Access, 7, 15170-15182.

[124] Kar, J., Liu, X., & Li, F. (2021). CL-ASS: An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks. Journal of Information Security and Applications, 61, 102905.

[125] Zhao, H., Xu, R., Shu, M., & Hu, J. (2016). Physiological-signal-based key negotiation protocols for body sensor networks: A survey. Simulation Modelling Practice and Theory, 65, 32-44.

[126] Chen, L. L., Zhang, A., & Lou, X. G. (2019). Cross-subject driver status detection from physiological signals based on hybrid feature selection and transfer learning. Expert Systems with Applications, 137, 266-280.

[127] Nia, A. M., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2015). Physiological information leakage: A new frontier in health information security. IEEE Transactions on Emerging Topics in Computing, 4(3), 321-334

[128] Azriel, L., Ginosar, R., & Mendelson, A. (2017, May). Revealing on-chip proprietary security functions with scan side channel based reverse engineering. In Proceedings of the on Great Lakes Symposium on VLSI 2017 (pp. 233-238).

[129] Strobel, D., Bache, F., Oswald, D., Schellenberg, F., & Paar, C. (2015, March). Scandalee: a side-channel-based disassembler using local electromagnetic emanations. In 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 139-144). IEEE

[130] Bang, I., & Kim, T. (2020). Secure Modulation Based on Constellation Mapping Obfuscation in OFDM Based TDD Systems. IEEE Access, 8, 197644-197653.

[131] Zhang, J., Wang, Z., Yang, Z., & Zhang, Q. (2017, May). Proximity based IoT device authentication. In IEEE INFOCOM 2017-IEEE conference on computer communications (pp. 1-9). IEEE.

[132] Xiao, X., Guo, F., & Hecker, A. (2020, December). A Lightweight Cross-Domain Proximity-Based Authentication Method for IoT Based on IOTA. In 2020 IEEE Globecom Workshops (GC Wkshps (pp. 1-6). IEEE.

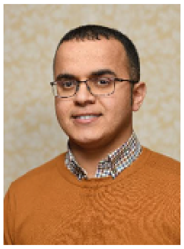
© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

Muhammad Adil is currently a PhD student in the Department of Computer Science and Engineering at the University at Buffalo, The State University of New York, USA. He received the Chair's Fellowship from the department in 2022. He received his BS and MS degrees in Computer Science from the Virtual University of Lahore, Pakistan, in 2017 and 2020 respectively. He has CCNA and CCNP certifications. Mr. Adil's research interest includes Networking, Cybersecurity, Cyber-Physical Systems (CPS), Unnamed Aerial Vehicles (UAVs), Internet-of-Things (IoT), Wireless Sensor Networks (WSN). He has many publications in prestigious journals such as IEEE Internet of Things, IEEE Transactions of Intelligent Transportation, IEEE Transactions on Industrial Informatics, IEEE Transactions on Network Science and Engineering, IEEE Sensor Journal, IEEE Access, IEEE Micro Magazine, ACM Transactions on Sensor Networks, Computer Networks Elsevier, Sustainable Cities and Societies, MDPI Sensor, and many more. In addition, he is member of IEEE computer society, IEEE Industrial Electronics, IEEE Cybersecurity, IEEE Young professionals, and London Journal Press Club-UK, as an Honory member. He is reviewing for prestigious journals, such as IEEE IoTJ, IEEE Sensors, IEEE Systems, IEEE TII, IEEE TCCN, IEEE TITS, IEEE TGCN, IEEE WCL, IEEE Communication Magazine, IET Communication, Computer Networks Elsevier Journals, and Telecommunication System, etc.

Dr. Varun G Menon (SM' 19) is currently Associate Professor and Head of the Department in Computer Science Engineeringat SCMS School of Engineering and Technology, India. He is a Senior Member of IEEE and Distinguished Speaker of ACM. He is an Associate Editor of Physical Communications Journal Elsevier, Alexandria Engineering Journal Elsevier and IET Quantum Communications. He is also a Technical Committee member of Computer Communications Journal Elsevier and an Editorial Board Member of IEEE Future Directions: Technology Policy and Ethics. He completed Ph.D. in Computer Science and Engineering from Satyabhama University, India in 2017. Dr. Menon received the Top Peer Reviewer Award by Publons in 2018 and 2019.He has served over 20 conferences like IEEE INFOCOM 2020, ACM Mobicom 2020, ICC 2020, ICCCN 2020, IEEE COINS 2020, SigTelComin leadership capacities including program co-Chair, track Chair, session Chair, and Technical Program Committee member. His research interests include Internet of Things, 5G communications, Fog Computing and Networking, Underwater Acoustic Sensor Networks, Hijacked and Predatory Journals, Ad-Hoc Networks, Opportunistic Routing, Wireless Sensor Networks.

Venki Balasubramanian received the PhD degree in body area wireless sensor network (BAWSN) for remote healthcare monitoring applications. He is the pioneer in building (pilot) remote healthcare monitoring application (rHMA) for pregnant women for the New South Wales Healthcare Department. His research established a dependability measure to evaluate rHMA that uses BAWSN. His research also opened up a new research area in measuring time-critical applications. He contributed immensely to e-Research software research and development that uses cloud-based infrastructure and a software architect for the several projects sponsored by Australian National Data Service (ANDS). He contributed heavily in the field of healthcare informatics, sensor networks, and cloud computing. He is the founder of, Anidra Tech Ventures Pty Ltd, a smart remote patient monitoring company.



Sattam Al Otaibi works as an assistant professor with the Department of Electrical Engineering, Taif University, Taif, Saudi Arabia. He is a researcher and an academician specializing in electrical and electronic engineering and nanotechnology. His practical experience in the field of industry, education, and scientific research has been formed through his research work and through his mobility among many companies, institutions, and universities as well as active participation in research centers that resulted in many scientific researches published in refereed scientific bodies.

Houbing Song Song (M'12–SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012. He is currently a Tenured Associate Professor of AI and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), University of Maryland, Baltimore County (UMBC), Baltimore, MD. Prior to joining UMBC, he was a Tenured Associate Professor of Electrical Engineering and Computer Science at Embry-Riddle Aeronautical University, Daytona Beach, FL. SONG Lab graduates work in a variety of companies and universities. Those seeking academic positions have been hired as tenure-track assistant professors at US universities like Auburn University, Bowling Green State University, and University of Tennessee. He has served as an Associate Technical Editor for IEEE Communications Magazine (2017-present), an Associate Editor for IEEE IoT-J (2020-present), IEEE TITS (2021-present), and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS) (2020-present), and a Guest Editor for IEEE J-SAC, IEEE IoT-J, IEEE Network, IEEE TII, IEEE Sensors Journal, IEEE TITS, and IEEE JBHI. He is the editor of eight books. He is the author of more than 100 articles and the inventor of 2 patents (US &amp; WO). His research interests include cyber- physical systems/internet of things, cybersecurity and privacy, AI/machine learning/big data analytics, edge computing, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. His research has been sponsored by federal agencies (including National Science Foundation, US Department of Transportation, Federal Aviation Administration, Air Force Office of Scientific Research, US Department of Defense, and Air Force Research Laboratory) and industry. His research has been featured by popular news media outlets, including IEEE GlobalSpec& 39;s Engineering360, Association for Uncrewed Vehicle Systems International (AUVSI), Security Magazine, CXOTech Magazine, Fox News, U.S. News & amp; World Report, The Washington Times, New Atlas, Battle Space, and Defense Daily.

Zhanpeng Jin (S'07-M'10-SM'15) is currently an Associate Professor and Director of Graduate Studies in the Department of Computer Science and Engineering at the University at Buffalo, State University of New York (SUNY-Buffalo). He was an Associate Professor in Electrical and Computer Engineering, and Biomedical Engineering, at Binghamton University, as well as a Postdoctoral Research Associate at the University of Illinois at Urbana-Champaign (UIUC). He received his Ph.D. degree in Electrical Engineering from the University of Pittsburgh. His research interests include ubiquitous computing, human computer interaction, and AI-powered smart health and smart home. He is a Senior Member of ACM and IEEE, and serves as an Associate Editor for the following journals: ACM Computing Surveys, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), and Elsevier Computers in Biology and Medicine. He has published over 100 papers in international journals and conferences. He received the IEEE Region 1 Technological Innovation Award. His pioneer work in brain biometrics was selected and named as one of the "Future Technology: 22 Ideas About to Change Our World" by BBC Science Focus.

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in IEEE Sensors Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JSEN.2022.3216824

Ahmed Farouk Member, IEEE) received the M.Sc. and Ph.D. degrees from Mansoura University, Mansoura, Egypt. He is currently an Assistant Professor, before that he was a Postdoctoral Research Fellow with Wilfrid Laurier University, Waterloo, ON, Canada, and Ryerson University,Toronto, ON, Canada. He is one of the Top 20 technical co-founders of the Quantum Machine Learning Program by Creative Destruction Lab at the University of Toronto, Toronto, ON, Canada. He is also selected as Top 25 of Innovate TO 150 Canada to showcase the best of Toronto's next generation of change-makers, innovators, and entrepreneurs. He is exceptionally well known for his seminal contributions to theories of Quantum Information, Communication, and Cryptography. He has authored or coauthored 62 papers in reputed and high-impact journals, such as Nature Scientific Reports, and Physical Review A. The exceptional quality of his research is recognized nationally and internationally. He was selected by the scientific review panel of the Council for the Lindau Nobel Laureate Meetings to participate in the 70th Lindau Nobel Laureate Meeting. His volunteering work is apparent since he was appointed as the Chair of the IEEE Computer Chapter for the Waterloo-Kitchener area and editorial board for many reputed journals, such as Nature Scientific Reports, IET Quantum Communication, and IEEE ACCESS. He is also selected for IEEE and IET Young Professional Ambassador and as a Moderator for the new IEEE TechRxiv. He is currently an Associate Editor for IEEE Canadian Review.

© 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
Authorized licensed use limited to: University of Maryland Baltimore Cty. Downloaded on November 22,2022 at 20:18:52 UTC from IEEE Xplore. Restrictions apply.