A Survey of Different Security Methods in the Physical Layer of TCP/IP Model

Noor Raad Saadallah
Computer and Information Engineering Department
Ninevah University
Mosul, Iraq
noor.saadallah@uoninevah.edu.iq

Abdulrahman Kh. Alhafid
Electrical Department
University of Mosul
Mosul, Iraq
abdulrhman.alhafid@uomosul.edu.iq

Huda Aqeel Al-Tayyar
Electrical Department
University of Mosul
Mosul, Iraq
huda.aqeel@uomosul.edu.iq

Qutaiba I. Ali
Computer Department
University of Mosul
Mosul, Iraq
Qut1974@gmail.com

ABSTRACT

In the previous two decades, cybersecurity risks and challenges in communications networks, especially in wireless networks, have increased tremendously. Wireless networks are insecure and potentially come under attack from eavesdropping, jamming, and interference because of the nature of the wireless channel characteristics. As conventional technologies that are secure are insufficient for the physical layer of wireless systems. Security vulnerabilities at the physical layer became a focal point of discussion. Any assaults from an attacker or weaknesses in the network reflect a detrimental effect on the network's usual operation. The investigation of any threat and its countermeasures consider an important step to secure networks. While many network security surveys have been seen in the literature, a few studies address and focus on the physical layer security and its challenges, which plays an important role in communications. Therefore, in this paper, we will highlight the security mechanisms in the physical layer which can be used to protect data and obtain secure reliable communication. A modern overview of the current physical layer and its security studies are required on the dangers, detection, and anti-measuring strategies. in this study, several attacks on the physical layer are described and analyzed. Methods of detection and countermeasures are also discussed and contrasted for each assault. Also, attention to the challenges and future directions have been included in the rest of the paper.

Keywords: Wireless networks, Wireless Systems, Physical Layer, Network Security

I. THE AIM OF THIS RESEARCH

It has noticed that there is a great development in the technologies of wireless networks and they have increasingly progressed every day and everywhere. On the other side, wired networks have been eliminated gradually. One of the drawbacks of using wireless networks is that the wireless network may be vulnerable and could be exposed to interferences, malicious attacks, eavesdropper, jamming, spoofing and so on. That’s due to the essential nature of wireless signal transmission in open-air propagation. Anyway, wireless media and transmission techniques have worth to deep study to ensure the transmitted/received information be secure. The security policies in wireless networks are usually implemented in the highest layers of communication networks models. Most of the existing higher layer security techniques have developed using mathematically stated computational functions, which might limit their capabilities in physical layer of the wireless systems due to the limited power and resources. That's give a motivation to discover alternate solutions, so; the algorithms of cryptography could be simplified and designed with limited resources and processing capacity. Since the traditional cryptography techniques are vulnerable to a variety of attacks, its best to thought of using properties of physical layer in wireless networks to combat security concerns. As a result, physical layer security schemes have emerged as a promising contender in recent years and attracting a lot of interests as a way to achieve an effective and efficient security for wireless systems by exploiting physical connection features.

II. Introduction

The security in physical layer depends on a variety of techniques used for the exploitation of communication link attributes to enhance different aspects of security such as confidentiality, privacy and authenticity. Wireless systems have evolved from single-mode networks to multimode and multi-standard networks as information technology has progressed. (3G, 4G, wireless sensor networks, etc.) [1]. That invites to give more attention to the wireless physical layer. Anyhow, the nature of wireless communication which has inevitable broadcasting, mobility, signal channel instability .. etc. has made the physical layer vulnerable to different types of security threats such as (Denial of Service) DoS, interference, network flooding, eavesdropping, and traffic analysis [2]. The attackers will cause dangerous security problems when they are active attacks with high performance, as the development of the attacking techniques nowadays. On the other hand, passive attackers are resource-limited (e.g., antenna resource, power, and signal processing capability)[3].Although traditional cryptographic security procedures are critical to solving the larger challenge of safeguarding wireless networks, they do not immediately use the wireless domain's particular qualities to combat security threats. The wireless media provides a rich source of domain-specific data that may be used to supplement and improve standard security methods. Recently, Physical layer security has evolved as an alternative security paradigm for achieving secrecy and authentication by using the unpredictability of the wireless channel. The physical layer security technology has been a success story for over a decade, and it continues to provide a layer of defense in communications [4], [5]. In this paper, an introduction to the physical layer security concept has been viewed. The rest is organized as follows: the vulnerabilities and types of attackers that can threaten the physical layer in TCP/IP networks identified first and summarized in Section 2. Section 3 illustrated and classified existing security schemes and related work of physical layer security, an encompassing overview of physical layer secure schemes been viewed, those schemes are divided into three categories: spatial domain-based, time domain-based, and recurrence domain-based. The research investigates the directions in those fields and pointing out some security techniques in Section 4. At last, conclusions have been presented in Section 5.

III. Vulnerabilities and Attackers in Physical Layer:

In TCP/IP Model and other models, the physical layer is at the bottom of the network, for example, in wireless networks it is mainly responsible for frequency allocation, generation of carriers, and signal modulation and detection. It receives the signals from the channel, extracts the information as a data stream after the demodulation and, sends it to the upper layer. Physical assaults and threats (such as interference, jamming, eavesdropping, and traffic analysis) are divided into two types: active and passive, so; a classification of attacks will be presented in the next subsections [1].

A. *Active Attacks:*

This type of attack uses signals on some specific frequency bands to make interfere or affect the broadcasted signals between the transmitter and the recover. Depending on that, active attacks can be either interference or jamming (also the bandwidth of interference and jamming attacks can also be classified as narrowband and wideband). The connection between legitimate users and transceivers cannot be guaranteed if the link between the transmitter and receiver is completely jammed by active eavesdroppers [5].

- **Jamming Attacks:**

By means jamming attacks, which are mostly malicious attacks, trying to make a failure in the channel by occupying the channel. The jamming could be classified as [3]:

a. Spot Jamming: In this type, the jammer transmits a high enough power signal frequency signal to cover the original signal.

b. Sweep Jamming: The jammer transmits a jamming signal with frequency hops from one frequency to another, (although not at the same time) to be a viable counter-attack on frequency hopping technology.

c. Barrage Jamming: Unlike sweep jamming, this type transmits a jamming signal at the same time, with a wide variety of frequencies, and makes a considerable impact on the communication coverage. The jamming ability in this type is weak at a wide frequency range because of the limitations of transmission power.

d. Deceptive Jamming: This a very destructive type and not easy to be detected. Forged packets of data have been transmitted by the attacker in the network to deceive the receiver receiving them.

- **Interference Attacker:**

On the other hand of the active attack, interference attacks worsen the legal desired signal by interfering it with other of the same frequency causing receiving failure. The interference may not only happen by malicious attackers, but also could from other users around the signal using same frequency or channel. The interference attacker can be further divided into [4]:

a. Sustained Interference: This attacker is intending to affect the user's normal communication by sending an interference signal to occupy the channel and try keeping it busy as long as possible.

b. Random Interference: In this type, the interference time and cycle are uncertain. That's because the attacker makes an interface with the original user in a random manner. It needs less energy consumption by the attacker compared with the sustained interference.

c. On-Demand Interference: If the channel is idle, the attacker is in idle case too, or else, the attacker will transmit an interfering signal to interrupt the ongoing transmission

B. Passive Attacks:

The two main classes of the passive attackers are eavesdropping and traffic analysis. Because of the characteristic of channel medium, especially the wireless, it is hard to make a shielded signal in the transmission to isolate it from the unintended recipients. So, Signals can be received, analyzed, and used by both legal and illegitimate users within the transmission range.

a. Eavesdropping: The eavesdropping tends to disclose information of other users in the communication network due to the accessing the channel.

b. Traffic Analysis: This attacker trying to extract information in accordance with changes in the flow of information from ongoing transmission. It can estimate the location of the base station based on network traffic changes. which leads to paralysis of the entire wireless sensor networks.

The classification in the previews section which concludes a number of common categories of physical attack is listed in Figure 1.

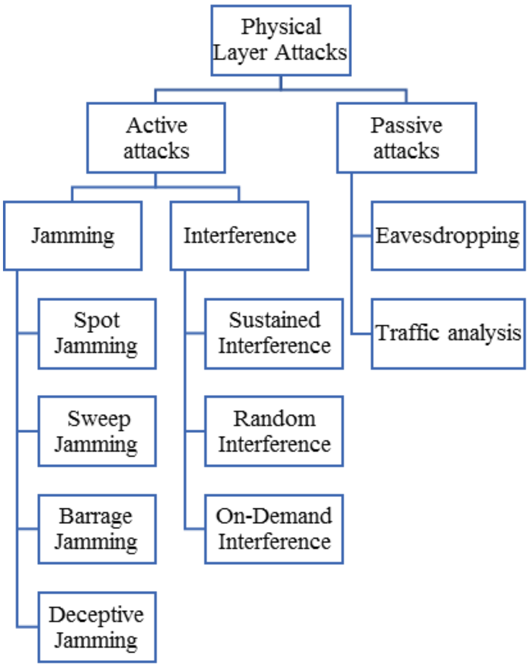


Fig. 1. Attackers in Physical Layer

IV. Related Works of Physical Layer Security

The physical layer security may be viewed from more than one point of view, it can be viewed according to the types of domain technologies such as time domain, frequency domain, and spatial domain also can be taken from the view of how to utilize specific security technologies from the physical layer's point of attack.

A. Time Domain Technologies

The concept of security in a physical layer which has a theoretical basis behind it has been built by Shannon's theory of complete secrecy in 1949 [3]. This notion was improved by Wyner got an expansion by Csiszar and Korner. Shannon proved that the security of the information could be achieved for exist channel codes if the length of the secret key is more than or equal to the length of the information transmission. Wyner demonstrated that the information can be transmitted in a secured manner when the channel for legitimate users has conditions superior to the eavesdropper [1]. Mohammed A.M. and others in [8], used in their research two encoding techniques such as Reed Solomon (RS) and Bose Chaudhuri Hocquenghem (BCH). They assess the security gap of common coding techniques such as Reed Solomon (RS) approaches and error correction jumbled codes in wireless sensor networks (WSNs). The security gap is defined as the mismatch between the signal of the eavesdropper to noise ratio (SNR) and the genuine receiver nodes' SNR. They look at the energy efficiency gap, as well as the security gap. The simulation results findings that the RS achieves technology similar security gap to scrambled error-correcting codes. The investigation shows, however, that the computational complexity of the is lower than that of the scrambled error-correcting codes, and discovered that Code for BCH requires less than RS energy. Imperfect temporal synchronization causes a random mismatch between the received cooperative jamming (CJ) and the reconstructed CJ, resulting in CJ cancellation performance reduction at the approved receiver. In [9] Wenbo G. and et.al introduced a method in their research about the performance of CJ cancellation with poor temporal synchronization is examined and assessed using the jammed cancellation ratio (JCR). The expectation and cumulative distribution function (CDF) of JCR are then supplied, assume that the time error is distributed equally within the accuracy of synchronization, and determining the precision of synchronization for CJ cancellation. The theoretical analysis is then confirmed by tests using SDR, which show that incorrect temporal synchronization can result in severe deterioration in CJ cancellation, especially for high received JNR. In [2] Bin Li and others published a survey about security at the physical layer in space information networks by providing some background information and a perspective on satellite Internet of Things (IoT), as well as discussing associated research issues that the evolving integrated network architecture faces. Then, they go through the most common satellite channel model, which is impacted by a variety of parameters, and they list the most widely used secrecy performance indicators. Also present an in-depth analysis of current physical layer security research in satellite communications, which divided into three categories: land mobile satellite communication networks, hybrid satellite-terrestrial relay networks, and satellite-terrestrial integrated networks. Yuan G., and others in [10] examined physical layer security characteristics in large-scale social networks in their paper. Traditional safety at the physical layer will confront new challenges in huge social networks, summarized by cross-layer optimization in the physical, link, and higher layers, also described the difficulties as a result of various optimum considerations: the identifying of wiretapping users, the use of high dynamic range, and the exchange of information in the cross-layer design. The basic idea of security in both (channel and source) type models is generating a secret key by both parties ‘Alice and Bob’. The requirements of this common key presented in [5] [6] as:

- The secret keys have a high similarity probability with Alice and Bob.
- The independence of keys of the observers and the public communication.
- The uniform distribution of keys over the key alphabet.

So, all parties have to know the applicable public communication technique codebook When there are active assaults, there is a probability of setting an end-to-end key inside the physical layer keys. The paper in [7] presented 3 techniques based on a strong model of secret sharing. However, the cost estimation for these cases is totally high, based on the attacker-controlled zone. Hence, the most significant aspect is to carefully evaluate the attacker's strength and to present a reasonable way of setting the model parameters when establishing secure end-to-end keys within physical layer keys. An and et al. [11] Secret performances for passive assault and aggressive attack of the country mobile satellite system (LMS) were studied, Where numerous antennas were set at both the legal receiver and the eavesdropper, and the secret message was received by the maximum ratio combining mechanism. In [12] the researcher discussed mobility management is presented and a (Long Term Evolution)LTE infrastructure that exploits the mobility was provided at the ICN (Information-Centric Networking) network layer proposed. The modern LTE authentication methodology has been investigated, as well as a handover protocol that makes use of the ICN communication style. Comparing to the current LTE protocol, The amount of messages necessary to authenticate or re-authenticate a device during mobility has been reduced as a result of the findings. The proposed LTE infrastructure authentication protocol that uses the ICN communication style is comparable to the LTE authentication protocol. This protocol enables you to:

- Mutual authentication between the connected device to the cellular system.

In a cellular system, cryptographic material is distributed to enable integrity and ciphering between the device and the access points. It's important to understand that ICN data must be authenticated using the creator's key (symmetric or private key). Management of authentication security and transferring the device data from the old to the new access point presented. In [12] create new handoff strategies without requiring any central unit, to distribute the cryptographic measures to the new access point. The importance of this model is the Simplicity of the LTE infrastructure and management and less cost for cellular system providers. So, this is a reason that would lead cellular system providers to deploy ICN model in their cellular infrastructure. In [13], a discussion of new paradigms of security that Utilize physical layer properties of the wireless medium, such as the wireless channel's fast shift in space, spectral, and temporal decorrelation. This model can enhance authentication and confidentiality services. Structures for these services and how such strategies can be combined to a larger security structure for a wireless system. The individuality and selectivity of a wireless channel, with the fact that the wireless channel de correlates away in space, so it can be used to prevent attacks. This maintains authentication for the valid transmitter. The channel enables the collecting of highly correlated information, which is then utilized to extract secret bits as part of a cryptographic keying system. In addition, the channel is used for enhancing confidentiality in wireless systems. In [2] Introduced an important foundation and viewpoint on the Internet of Things (IoT) in satellite and the satellite channel model with many influences. The common security performance metrics explained their paper with different architectures as well as land mobile satellite communication systems, systems of hybrid relays, and integrated systems.

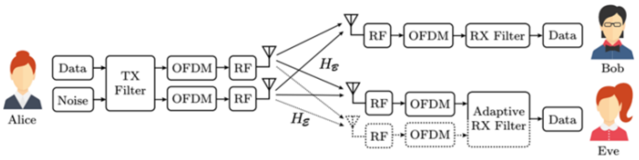
Many types of research on physical layer security in the field of LMS -Land Mobile Satellite-communications. As the first attempt, Petraki and et al. in [14] presented the physical layer security on satellite links operating above 10 GHz. The analytical expressions of the security capacity were introduced and extended to include the scenario of two users and two risky observers.

B.Frequency Domain Technologies

Attacks in the dynamic spectrum access category primarily aim to prevent SUs from dynamically accessing available spectrum gaps by detecting free channels. In this section, we'll go over one of the most significant attacks against access to the dynamic spectrum, in addition to how to identify and counteract it. In cognitive radio networks, selfish primary user emulation (PUE) is a severe security issue. A PUE attacker can greedily occupy additional channels by producing mimicked incumbent signals. As a result, A PUE attacker can prevent other secondary users from acquiring radio resources while also interfering with neighboring principal users. A surveillance method on occupied channels might be used to reduce selfish PUE. Surveillance tactics must be determined, especially in a multi-channel environment, to ensure network operating fairness. In cognitive radio networks, the authors in[15] described the monitoring procedure for mitigating multi-channel selfish PUE, and the selfish PUE assault Including and excluding the fallow set are both considered. The network management can recognize the selfish attacker by monitoring the occupied channels. Game-theoretic techniques are used to investigate the interaction between selfish assaults and the surveillance process. The commitment model was examined using Proper modeling of a defense's and an attacker's strategic interaction. The defense takes the initiative in this approach by committing to a monitoring plan. The intelligent attacker is required to take up the role of a follower in response to the defender's tactic to maximize the expected benefit. The SSE is used to invest in the surveillance process's relevant initiatives. The defender's projected payout is greatly increased when the defense commits to a surveillance approach, according to analytical and numerical statistics. Furthermore, in the commitment scenario, In the commitment situation, the time it takes to compute the equilibrium point is less than in the non-commitment situation. The research in [16]emphasis on the security issues that arise in CR networks as a result of Primary User Emulation (PUE) attacks. The authors provided a complete overview of PUE assaults, including everything from the attacking reason to the effects on CR networks, as well as detection and protection strategies. To protect CR networks from PUE assaults, a two-level database-assisted detection technique is presented. For rapid and reliable detection, energy detection and position verification are coupled, and to alleviate the performance loss of a CR network under a PUE attack, an admission control-based defense strategy is provided. The study investigates the trade-off between security and energy efficiency. [17]since energy efficiency and security are explored independently in the traditional Primary User Emulation Attack (PUEA) method of counter-measure technique in the Cooperative Spectrum Sensing (CSS) method. CSS can increase detection performance, but as the number of cooperating users grows, energy usage will skyrocket. To address this issue, As the best aim, they have chosen CSS energy efficiency in the presence of PUEA, with secured detection performance and secure false alarm threshold as limitations. The ideal problem is addressed in order to establish a balance between efficiency in energy use and comfort.

The security challenges of Cognitive Radio Networks (CRNs) have recently gotten a lot of attention in the research community. Legitimate PU signals may also be detected using detection techniques based on matching filters and cyclostationaries [18]. The PU signal and the SU received signal's convolution product are compared to a specified threshold in the matched filter sensing approach [19]. It only works when the PU signal characteristics are known, which isn't usually the case in real-world settings. In the context of PUE attacks, the authors suggested a safe authentication process utilizing a matched filter-based detection methodology in [18]. To securely transfer sensing data across SUs nodes, the proposed technique combines matching filter and cryptographic digital signature use of a detection. PU signal embedded characteristics from the SU received signal are extracted using cyclostationary based detection algorithms.

primary user emulation (PUE) attack, a new security concern, poses a significant challenge to Cognitive Radio Networks (CRNs). PUE is a CRN-specific attack that may result in severe denial of service (DoS) to CRNs. The authors in [20]introduced DECLOAK, a method for detecting primary user emulation (PUE) attacks based on second-order cyclostationary characteristics, To validate the source, the characteristics were calculated using the incoming signal's sub frequencies. However, because an attacker may readily imitate PU features (modulation, bandwidth, variance, operating frequency,



cyclostationary features, etc.), SUs were possibly unable to discriminate between valid PU and PUE signals. As a result, increased detecting efficiency approaches to validate the legal PU when PUE attacks the network are critically required.

In[21] ChunS. X. and et.al. suggested a new primary user emulation (PUE) detection system, The research presents a technique for acquiring and reconstructing signal activity patterns. Unlike the detection of current PUE techniques, the suggested approach does not require any previous knowledge about primary users (PUs) and has no restrictions on the types of PUs that may be detected. Through spectrum sensing, it obtains the signal's pattern of activity, Intervals of ON and OFF, for example. The measured signal activity pattern is then reconstructed using a reconstruction model. The suggested system can intelligently identify a PU's signal activity pattern from an attacker's signal activity pattern by assessing the reconstruction error. a PUE detection method based on the signal activity pattern (SAP) of PU signal transmitters, has been described. Based on the reconstruction error, it employs a SAP reconstruction model to reconstruct an observed SAP and determine if the SAP belongs to an attacker.

C. Spatial Domain Technologies

Nowadays, with the evolution of various technologies, many security technology methods have been used for physical layer security, such as SIMO (single-input multiple-output), MIMO (multiple-input multiple-output), and relay channel. These techniques may have improved PHY (physical layer) security and higher potential secrecy capacity, but they can only raise the network's channel capacity to a limited level. [21].Eventually, more than one technique can be combined with each other by the system to contribute enhancement of physical layer security. In [22] the authors aimed to improve the performance of the physical-layer secrecy using amplify-and-forward compressed sensing (AF-CS) framework against malicious eavesdropping nodes. he demonstrates that a small number of eavesdroppers has a zero probability of recovering the intended signal.

Fig. 2. The secure transmission using CSI preceding [2].

The transmission technology using multi-input multi-output (MIMO) employing orthogonal frequency division multiplexing (OFDM) shown in Fig.2 is adopted in several wireless standards therefore, secure transmission considered significantly in the literature. The channel state information (CSI) preceding at the transmitter side is one of the potential schemes that improve the bit error rate performance of the system in addition to eavesdropping avoidance. Direct feedback from the receiver is a frequent method for Alice to retrieve the CSIs of each receiver. Alice does this by sending out well-known training symbols to all recipients. Alice can connect with Bob in secret by transmitting within Eve's CSI's null-space. Alice uses the pseudo inverse of the block matrix consisting of Bob's and Eve's CSI to pre-code the sending data. Cross-talk is prevented by the preceding approach, known as zero-forcing beamforming, which eliminates interference produced by other contemporaneous broadcasts. Alice will have to adjust her communication technique if Eve's CSI cannot be believed. To maintain secrecy, Alice creates fake noise in Bob's CSI null-space to deceive Eve, as seen in Fig. 2.

The research in [5] identifies some flaws in the transition from classical security to physical layer security. According to the literature, most of the efforts are devoted to studying the physical layer security when the attack is considered as a single-antenna eavesdropper that is less effective. Therefore, Orthogonal blinding is one of the physical layer security schemes that is being studied. using CSI preceding, and the performance is evaluated in multiple eavesdropper settings. The system is revealed to be subject to assault counterparts to the "ciphertext-only attack" in the cryptography domain against a multi-antenna eavesdropper owing to the linearity and low entropy contents in the transmitted data. The artificial noise/interference is introduced in the literature as physical layer security approach to enable secure key exchange and management and other security purposes. The eavesdroppers are disturbed using friendly jamming interference to block the untrusted communication in the network without degradation the legitimate node reception. The system model consists of three entities, the legitimate entities (Alice and Bob) and the illegitimate entity (Eve) where friendly jamming is used during the key exchange between the legitimate parties as depicted in Fig. 3.

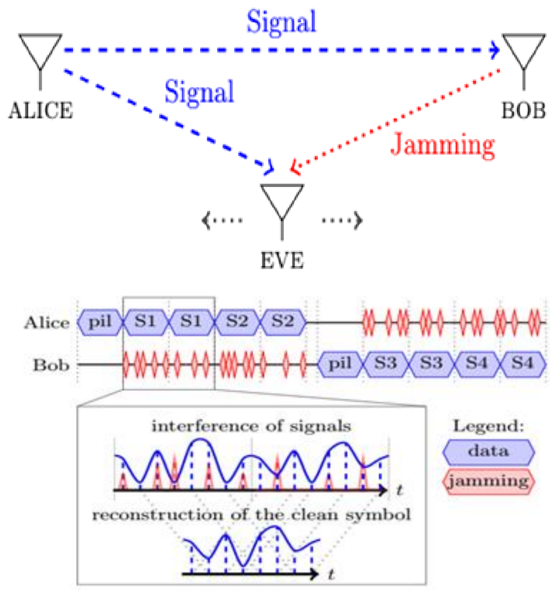


Fig. 3. The artificial noise based secure key exchange[5].

The security system used in [23] involves sending training pilots and duplicated sequences while the other legitimate node applying a jamming signal. The scheme in this research assumes that the jamming only distorts the symbol or its replica. The legitimate receiver will reconstruct the symbol via the cancellation of the jamming signal to produce the clean signal. Artificial noise cancellation involves sophisticated signal processing which is out of the scope of this review. However, the researchers argue that the adversary models used to assess the physical layer security based on artificial jamming typically assume that the adversary has the same configuration and capabilities as the legitimate nodes. This assumption is argued therefore, the adversary is equipped with multi-antennas and an efficient approach is discussed to detect the artificial interference. The authors concluded the adversary model has a significant impact on the secrecy capacity as the multi-antenna eavesdroppers pose limitations on the considered security model. The treatment of sensor readings as common random number generator, source of entropy, and device fingerprint to establish security solutions for key exchange, authentication, pairing, and access control. The physical layer attributes such as ambient audio contexts, luminosity modalities wireless channel measurements, and electromagnetic environmental fingerprints are investigated in the literature. The majority of physical layer assist security schemes are using the standard models shown in Fig. 4 that consists of channel estimation and probing, quantization, private information amplification and key verification.

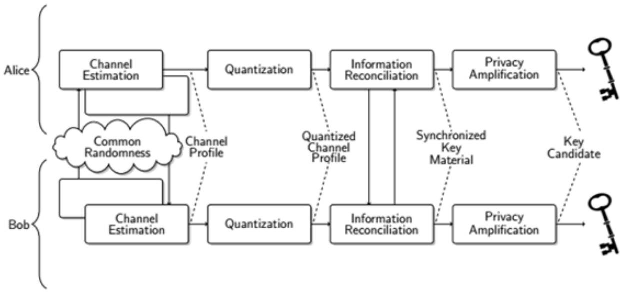


Fig. 4: The generic diagram of the key agreement with channel attribute estimation [23].

The authors in [24] argue that security analysis of physical layer security is usually investigated and studied from the perspective of a single component or using very wide abstractions of the randomness of the physical layer and not the whole computing system. In addition, the feasibility of such systems for low resource agents. To investigate the above arguments, the authors considered the key agreement protocols based on the recycling of Received Signal Strength Indicators (RSSI) and discussed two implementations on resource and non-resource constrained devices. It is demonstrated that an optimized realization of a key establishment system is feasible by deriving a shared secret from physical attributes on resource-constrained devices (popular ARM Cortex-M3 processor). In addition, the considered physical layer security approach is compared with well-known Elliptic Curve Diffie-Hellman (ECDH) realizations. The reported results are demonstrated that for present and future IoT systems, physical layer techniques might be a feasible option. The researchers in [25] presented a study on the possibility of exploiting the characteristics of the channel to provide the authentication for source massage and ensure the message integrity. The authentication method will be founded on a calculation of the communication pathways between the agents, which will operate as a transmission fingerprint, Each agent is believed to have access to several flat fading channels then the channel's fading coefficients will be gathered for analysis. They devised a physical layer strategy to provide Alice and Bob with authentication based on an accurate channel prediction and presuming a broad model for Eve's assault, and gave the ideal Eve method in the event of a single assault, as well as an estimate based on analysis of the (missed detection) MD probability averaged over channel data. Furthermore, They created a suboptimal multiple attack strategy for Eve, which included a sequence of messages and channel guesses targeted at compromising authentication. When the channel vector size is large enough and Eve just has a rudimentary understanding of the Alice-Bob channel, The study technique's benefits are validated by numerical data, which show that it performs well against both assault and defense methods. In [26] introduced a study to design and construct a simulation testbed and implementation that will allow for in-depth investigation of communication protocols, cyber-physical security functions, intelligent electronic device (IED) vulnerabilities, network setup, and physical security needs of an IEC 61850-based power distribution substation. it has demonstrated high efficiency in achieving cybersecurity He showed high efficiency in achieving cybersecurity after exposing the proposed system to two types of attacks.

Physical Attack Model comes in two types, the incremental attack and the abrupt attack, and network attack comes in three types: Process-Level Attacks, Station-Level Attacks, and Remote Attacks. This model shows a low-cost testbed concept that may be quickly installed and expanded to meet budgetary restrictions. Various IEC 61850 functionalities and settings that support security may be developed and tested using virtual IEDs thanks to our modular and independent architecture. Our methodology allows for network configuration testing and adjustment to improve security and performance, as well as research into the impact of network configuration changes. in[27] a group of Russian researchers designed a methodology for safe embedded systems based on a mix of security components. The method uses an optimization approach to take into account the functional and non-functional properties of security components as well as device limits. The methodology was used to build an integrated cyber-physical security system. This system consists of a combination of embedded devices for data collecting, preprocessing, and secure transmission, as well as a server for data storage and analysis. The approach chose the best microcontroller and other components for the job. Based on this, the best answer was found. The database, as well as the functionality and non-functional needs, are all directly dependent on the technology. It outperforms resources in terms of the proprietary database of position appropriateness and accuracy. In general, the design protects the back area by covering it. Expert choices should be replaced. A physical cybersecurity system that is integrated. The others researcher in [28]suggested a method to use a unique multi-attributes and multi-observation (MAMO) methodology to improve the reliability of physical-layer authentication. In addition, to ensure seamless integration of physical layer authentication and encryption systems, they also offer cross-layer assisted architecture, as well as physical key and Composite Security Key (CSK) creation. It's worth noting that the physical key successfully mitigates the brute-force search attack, which is a flaw in classical cryptography. Furthermore, owing to increasing network complexity, emerging 5G approaches will have a significant influence on present physical layer authentication. The suggested physical layer security context prediction and other new security techniques. “Cyber Physical Systems (CPS)” emerged as a result of the integration of embedded systems with communication technologies. These systems are used in a variety of industries, Automobiles, smart manufacturing, and healthcare are just a few examples. Because of the "dual nature" of such systems, providing both safety and cybersecurity is essential for their long-term success. A Norwegian research team in [29] a comprehensive survey was presented a thorough examination of safety and cybersecurity co-engineering methodologies, as well as a discussion of outstanding concerns and research difficulties. Despite the extensive literature on the subject, numerous areas of the issue remain unexplored. They went back over earlier surveys on cybersecurity and safety co-engineering methodologies and conducted a comprehensive literature review. For such methods, they created a multi-attribute taxonomy and utilized it to assess them. As a result, a thorough assessment of current breakthroughs in cybersecurity and safety co-engineering was offered. For more than three decades, academics in both domains have aimed to examine safety and security together. Despite the problem's endurance and the large number of research outcomes on safety and security co-engineering which have been developed in recent years, significant impediments remain. They recognized and addressed such concerns, as well as focus on building a graphical model-based, holistic, integrated, safety and security requirements elicitation co-engineering technique suitable to the autonomous vessel domain in the future, among the many conceivable research challenges in the field.

Fifth-generation (5G) network networks are required to be combined with a variety of radio communication methods, including satellite components, to provide customers with smooth networking and global reach. In [30] Min L. and others begin with a brief overview of existing policies and infrastructure design for the integration of satellite and 5G networks in this article. Then, for advanced 5G-satellite networks, they look at different ways to increase reliability or protection at the physical layer. The primary performance metric used to assess the protection and reliability trade-off is the successful achievable pace, which is supplemented by the implementation of a proposed beamforming scheme to quantify and incorporate the security and stability tradeoff for interconnected networks, they proposed a metric called "efficient achievable pace" and a BF scheme. their topic included a computer simulation that evaluated the success of different schemes. Finally, developments and problems of interconnected 5G-satellite networks were addressed.

In [31] Kun W. and others provided a study about the secure communication difficulties of cooperative wireless networks in the presence of several friendly but selfish intermediary nodes are addressed. To address this issue, they provided a relay and jammer selection approach in which intermediary nodes are used to pick the jammer and relay nodes, therefore improving the security of eavesdropping assaults. On the eavesdropper, the jammer is utilized to transmit fake interfering noise. The relay functions in the same way as a typical relay, retransmitting source signals from the source to the final destination. they offered a power allocation strategy of intermediate nodes that is structured as a price-competition Bertrand game in order to achieve the highest ability for the confidentiality of chosen nodes. also show that an ideal pricing strategy may enhance secrecy capacity while still providing the best revenues for selfish friendly nodes. Then, to get the price and node selection solution, a novel particle swarm with a simulated annealing optimization algorithm (PSSAO) is used. At the last, their theoretical understanding is supported by simulation results.

The research team in [32] In this research, we analyze the cognitive radio network (CRN), which includes a pair of major nodes, a number of minor nodes, and an eavesdropper. It also has a multiple-input-multiple-output (MIMO). In order to improve energy efficiency and spectrum efficiency, the secondary transmitter is powered by the primary transmitter's renewable energy. The secrecy range of the optimizing antenna selection (OAS) and sub-optimal antenna selection (SAS) scheme for underlay MIMO CRN The effects of energy collection on the standard space-time transmission channel model are investigated and contrasted, depending as to whether or not wiretap connections' channel state information (CSI) is accessible. The study of prospective attacks and threats, and the calculation of cybersecurity and safety, is important and complicated because of a strong dependency between the two domains. There are three types of dependencies that have been found [33].

- Conditional dependencies: cybersecurity-affected safety processes, such as malicious sensor or control model alterations, may prevent safety systems from safeguarding in the event of an accident. On the other hand, safety operations can be a condition for cybersecurity, such as when uncontrolled conditions reduce a system's security and lead to opportunistic negative activities.

- Reinforcement: Security and safety measures can work together; for example, event and activity tracking can be used for either attack detection and accident prevention, and also post-event analysis.
- Conflict: There is a possibility of conflicting the measurements of safety and cybersecurity, For an automated door closing system, for example, a safety need would be to keep the door open, but a security need would be to keep the door secured in the event of failure [29][34].

In [35] the authors presented the similarities and variations between safety and security features with a focus on their interdependencies. Kriaa et al. [36] discussed the safety and security methods and analyzed them to use in industrial control systems. Assessment of various risk methods of safety and security, and categorization based on the field of applicability, were analyzed by Chockalingam et al. [37], Abulamddi [38] current programs for safety and security standards were established. A comprehensive evaluation of the literature was carried out by Lisova et al. [39] that concentrated on the developed safety and security and systems that have been assessed. Lyu et al. [40] provided a brief survey that looked at five strategic safety and security solutions. In [41] Paul and Rioux from the early 1990s presented an extensive bibliography on safety and cybersecurity techniques without assessing them. They investigated IoT medical device safety and security. An analyst is able to evaluate security threats accidents that disturb safety. The analyst is able to combine the EFT and the Defense Tree (DT) approaches to perform a good analysis. The approach consists of six stages: stage1: identifying the hazards, accidents, and safety restrictions; stage2: the construction of the system control structure in accordance with STPA. stage 3 and 4: identifying Using the EFT and DT approaches, we may identify dangerous control activities and hazards' causative components. stage 5: calculation the occurrence probability of the essential events of the EFT that was developed in stage 4; The calculation is based both on statistical data and the opinions of stakeholders. Finally, stage 6: performing the choice of the suitable measures based on estimations of the probability of stage 5. This suggested the method has been implemented used for diabetic patients in an insulin pump.

In [42], the authors' proposed Processes for threat modeling and hazard calculation for driverless vehicles titled Security Automotive Risk Analysis (SARA). This method provides a conflict between safety and security threats. This is obtained by evaluating the impact on the assault goal's safety, and by assessing the safety severity and metrics of controllability. SARA is divided into four sections: feature description, threat specification, risk assessment, and countermeasures. In the third block (risk assessment), security and safety specialists identify assaults as well as key indicators for risk calculation, such as severity, observation, controllability, and the chance of the most severe assault. The suggested approach was tested on an autonomous automobile to see how a hostile attacker or observer would affect it, as well as how damaged road infrastructure would affect it.

According to [43], methods that attempt to combine analysis methods of safety and security will reduce the designer's understanding of the analyzed system and prevent a systematic analysis of each characteristic; As a result, there are safety and security concerns. Combining approaches, on the other hand, yields more findings and allows for possible conflicts.

V. CHALLENGES AND FUTURE DIRECTIONS

There have been proposals for several detections and defend approaches to increase the safety of communication networks across the physical layer. These strategies pertain to the accessible data on the main, secondary, and malevolent users [44]. Despite this effort, the physical layer's safety still faces several challenges in addressing and mitigating the problems presented by the assailants [45]. For example, localizing approaches rely on primary user's information located in actual circumstances, which is not always available. Higher energy consumption, design complexity, and efficiency are necessary for advanced methods of threats defending [46]. They are resource constraints such as electricity and bandwidth for cryptography-based approaches[47]. Cryptographic solutions, therefore, demand extremely confident and secure infrastructure. The Federal Communication Committee (FCC) also restricts authentication-based procedures. Intrusion detection systems-based solutions demand substantial capacity of memory to analysis and traffic analysis flow, excluding Selfish Users (SUs) with limited memory. They are also high false alarm rates which cause extra overhead network. They are also high false alert rates which cause extra overhead network. Note that in actual circumstances, users might be extremely mobile and information about the channel status cannot be utilized for PU authentication as the hardware introduces random noise. It is also difficult to include numerous classes of Primary Users (PUs) with distinct models of signal activity. For systems based on spectrum detection, hostile actions in the network are not effectively detected. Energy-based sensing systems are not effective and cannot discriminate between real signals and noise. Coordinated, filter-based approaches are not capable of distinguishing between valid and malicious signals. Because fraudulent users may readily replicate PU features and act like authentic PU, cyclostationary-basic approaches are limited [44]. Their efficiency depends mostly on how this threshold is chosen for threshold-based approaches. The efficacy of such technologies is reduced by fixed and established limits to validate specific radio parameters. However, these procedures must be measured [45], which in many situations is difficult. For tactics based on functionality, attackers may easily emulate legitimate PU signal functions, another network security challenge [46]. Anti-eavesdroppers allow aggressive attacks to be detected and blocked, but the passive eavesdropper may always retain a list in quiet mode, to get information for further research in advanced anti-eavesdropping systems. With regard to the management of measurement uncertainty, few studies study the influence of network security on uncertainty[47][48]. Thus, realistic detection and protection mechanisms that can function with real network faults need to be developed and investigated. Models are taught in advance for machine-based approaches before the system is attacked so that it can react when there are known problems[49]. The learning process is hampered by the rising amount of training data available via antennas, as well as the movement of users over time. Although the 5G wireless communications standards are complete, 5G and satellite systems integration are still underway and many problems require more investigation. The following tendencies in the study difficulties may need attention to utilize in 5G networks, the full potential of satellite systems, in addition to the major issues outlined above.

The use of friendly jamming or generated noise in the integrated 5G-satellite networks (IFSNs) to alleviate security and reliability trade-offs (SRT). Because of satellite and terrestrial system integration, interference/jamming is introduced between the two networks, which are classically regarded as detrimental. New research has recently shown that these interferences may be employed as green jamming to improve the safety and reliability of physical layers in IFINs[2]. In this connection, a possible problem is a new interference management technique.

Coordinating communications between the satellite and airborne platform. 5G is still a difficulty to overcome in the network coverage of wide isolated locations with a small population. Given the constraints of direct satellite connectivity as well as the high costs of installing many ground stations in remote locations, it is impracticable for poorer nations to use terrestrial relays. The recently introduced new satellite-aerial and terrestrial network architecture[50] has been employed as an aid to satellite transmission. This new architecture is able to give access to the Internet to a wide range of disconnected persons worldwide. However, this architecture is more subject to security attacks and physical layer security remains an unresolved topic because of the inherent property of vast coverage by satellites and aerial networks. The use of new resources for the spectrum. Spectrum resources are quite limited. in recent years develop into the main impediment for communication at high data rates. Free space optical communication (FSO), because of its exceptionally high bandwidth, unlicensed frequency allotment, In comparison to RF, it has low power consumption and strong channel security, As a result, it is a feasible technique for both inter-satellite and ground-to-space communications. First, an inter-satellite FSO-based data relay connection is already run by the European data relay satellite (EDRS). To increase the downloading of Earth observation data and photos between LEO and GEO satellites. In satellite communications that can realize the notion of terabits satellite system and increase the overall capacity of a satellite network, on the other hand, free-space optical (FSO) technology for ground and aerial satellite connectors is seen as the next big thing. Therefore, in future integrated satellite systems, the combined FSO/RF satellite air-terrestrial network will have a crucial function. They function by assigning all users confidence or reputation values and updating them in advance according to attack detection reports after each round for techniques based on trust, reputation, and secrecy criteria. These settings can also be altered to users and hence misleading measurements cannot be trusted. More working time is needed for assigning, calculating, and updating these safety measures each time. In addition to the technological hurdles, the effectiveness of existing security solutions is limited by time-variable wireless channels.

In future works, there are still many fascinating open-ended issues to be studied. Current protection mechanisms, for example, have been built to resist one of the known social layer attacks[51][52]. Therefore, frameworks are needed to identify all conceivable threats and to deal with them. A combination of physical layer mitigation strategies and the MAC layer might provide future guidance for research to overcome each layer's safety constraints. MAC layer techniques can feed SU trustworthy data to assist SUs to understand and reason about their neighbors via cryptographic protocols [53]. This enables SUs to gather and construct a network database that can assess how dependable neighbors are. In comparison to the physical layer, higher levels are less vulnerable to assault [54]. This notion can be an excellent effort for the future for finding a way of distributing the greater degree of safety across the many layers of the open system model [46].

Location-based approaches depend on PU information, which in real settings can't be obtained[55]. Therefore, improved strategies need to be developed that do not require PU location knowledge. Cooperative systems employ the laws of fusion to determine the existence of PU in the spectrum. In order to amend the final decision, the attackers might use OR and AND also voting provisions in both centralized and decentralized schemes [44]. More improved fusion centers that can make the sensing choice efficiently are needed.

Moreover, it is highly necessary to build real-time detection and protection tactics to tackle assaults with the lowest delays in order to successfully neutralize any form of assault[56].

In addition, prior research assumes basic scenarios in which a single PU and cell are taken into account. One of the study issues to be explored is the detection of In multi-cell and multi-user systems, there is a persistent danger. Existing detection algorithms cannot separate attackers from various PUs with multi-cell and multi-user systems. In order to examine effectively how to meet current difficulties, genuine implementation is essential to evaluate detection and defensive approaches.

VI. Conclusion

Security issues in communications networks emerged and became important scope due to the escalated types of services in the networks. In special cases, the security in the physical layer of the TCP/IP model considered a critical matter and worthily merit more important because that this layer is responsible for establishing communication due to the physical channel and at the same time is vulnerable to attacks. At the onset of this paper, various types of active and passive attackers that may threaten the network in the physical layer have been classified and declared. Then an analytical survey has presented for various types of security aspects in the physical layer, these types classified according to the detection and defense security methods taken from different domains points of view, which are time, frequency, and special domain. Each of those domains has many proposed defending techniques in the kinds of literature. As investigated from the researches, time and frequency domains have less implementation complexity and energy consumption than spatial domain, but on the other side, they need larger storage spaces and more capabilities of computational power in addition to additional hardware units. At last, security challenges and future directions have been presented. In fact, security techniques of physical will still be in the theoretical stage research phase and there are interesting directions and hotspots for future researches and practical applications.

References

1. [1] W. Fang et al., “Information security of PHY layer in wireless networks,” J. Sensors, vol. 2016, 2016, doi: 10.1155/2016/1230387.
2. [2] B. Li, Z. Fei, C. Zhou, and Y. Zhang, “Physical-layer security in space information networks: A survey,” IEEE Internet things J., vol. 7, no. 1, pp. 33–52, 2019.
3. [3] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” IEEE Commun. Surv. Tutorials, vol. 11, no. 4, pp. 42–56, 2009, doi: 10.1109/SURV.2009.090404.
4. [4] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, “Physical layer security in wireless networks: A tutorial,” IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, 2011, doi: 10.1109/MWC.2011.5751298.
5. [5] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, “Profiling the Strength of Physical-Layer Security,” no. 2, pp. 21–30, 2016, doi: 10.1145/2939918.2939933.
6. [6] Ludovic Pietre-Cambacedes, and Marc Bouiss, “ Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes) ” IEEE 2010 , doi : 10.1109/ICSMC.2010.5641922
7. [7] S. Pfennig, E. Franz, S. Engelmann, and A. Wolf, “End-to-end key establishment with physical layer key generation and specific attacker models,” in Physical and Data-Link Security Techniques for Future Communication Systems, Springer, 2016, pp. 93–110.
8. [8] M. A. Magzoub, A. A. Aziz, M. A. Salem, H. A. Ghani, A. A. Aziz, and A. Mahmud, “Physical layer security and energy efficiency over different error correcting codes in wireless sensor networks,” Int. J. Electr. Comput. Eng., vol. 10, no. 6, pp. 6673–6681, 2020, doi: 10.11591/IJECE.V10I6.PP6673-6681.
9. [9] W. Guo et al., “Analysis of Cooperative Jamming Cancellation with Imperfect Time Synchronization in Physical Layer Security,” IEEE Wirel. Commun. Lett., vol. 10, no. 2, pp. 335–338, 2021, doi: 10.1109/LWC.2020.3030075.
10. [10] Y. Gao et al., “Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges,” IEEE Access, vol. 6, no. c, pp. 26350–26357, 2018, doi: 10.1109/ACCESS.2018.2832839.
11. [11] K. An, T. Liang, X. Yan, and G. Zheng, “On the Secrecy Performance of Land Mobile Satellite Communication Systems,” IEEE Access, vol. 6, pp. 39606–39620, 2018, doi: 10.1109/ACCESS.2018.2854233.
12. [12] A. Compagno, M. Conti, and M. Hassan, “An ICN-based authentication protocol for a simplified LTE architecture,” in International Worskhop on Communication Security, 2017, pp. 125–140.
13. [13] S. Mathur et al., “Exploiting the physical layer for enhanced security,” IEEE Wirel. Commun., vol. 17, no. 5, pp. 63–70, 2010, doi: 10.1109/MWC.2010.5601960.
14. [14] D. K. Petraki, M. P. Anastasopoulos, and S. Papavassiliou, “Secrecy capacity for satellite networks under rain fading,” IEEE Trans. Dependable Secur. Comput., vol. 8, no. 5, pp. 777–782, 2011, doi: 10.1109/TDSC.2010.34.
15. [15] D. Ta et al., “Attacks in Cognitive Radio Networks To cite this version :,” 2018.

16. [16] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," IEEE Netw., vol. 30, no. 6, pp. 62–69, 2016, doi: 10.1109/MNET.2016.1200149NM.
17. [17] Y. Wang, X. Xu, W. Wu, and J. Bao, "A primary user emulation attack countermeasure strategy and energy-efficiency analysis in cognitive radio networks," J. Commun., vol. 12, no. 1, pp. 1–7, 2017, doi: 10.12720/jcm.12.1.1-7.
18. [18] F. Salahdine, N. Kaabouch, H. El, and G. Matched, "cognitive radio networks To cite this version : HAL Id : hal-01371162 Matched Filter Detection with Dynamic Threshold for Cognitive Radio Networks," 2016.
19. [19] Z. Yuan, D. Niyato, H. Li, J. Bin Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 30, no. 10, pp. 1850–1860, 2012, doi: 10.1109/JSAC.2012.121102.
20. [20] C. S. Xin and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," IEEE Trans. Mob. Comput., vol. 13, no. 5, pp. 1022–1034, 2014, doi: 10.1109/TMC.2013.121.
21. [21] Y. Zou, J. Zhu, and B. Zheng, "Defending against eavesdropping attack leveraging multiple antennas in wireless networks," 2013 8th Int. ICST Conf. Commun. Netw. China, CHINACOM 2013 - Proc., pp. 699–703, 2013, doi: 10.1109/ChinaCom.2013.6694683.
22. [22] J. E. Barceló-Lladó, A. Morell, and G. Seco-Granados, "Amplify-and-forward compressed sensing as a PHY-layer secrecy solution in wireless sensor networks," Proc. IEEE Sens. Array Multichannel Signal Process. Work., vol. 9, no. 5, pp. 113–116, 2012, doi: 10.1109/SAM.2012.6250442.
23. [23] F. Yu, C. C. Chang, J. Shu, I. Ahmad, J. Zhang, and J. M. De Fuentes, "Recent advances in security and privacy for wireless sensor networks," J. Sensors, vol. 2015, 2015, doi: 10.1155/2015/169305.
24. [24] D. Steinmetzer, M. Schulz, and M. Hollick, "Lockpicking physical layer key exchange: Weak adversary models invite the thief," Proc. 8th ACM Conf. Secur. Priv. Wirel. Mob. Networks, WiSec 2015, 2015, doi: 10.1145/2766498.2766514.
25. [25] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," IEEE Trans. Wirel. Commun., vol. 11, no. 7, pp. 2564–2573, 2012, doi: 10.1109/TWC.2012.051512.111481.
26. [26] E. Tebekaemi, "Designing An IEC 61850 Based Power Distribution Substation Simulation / Emulation Testbed for Cyber-Physical Security Studies," CYBER 2016 First Int. Conf. Cyber-Technologies Cyber-Systems, no. c, pp. 41–49, 2016.
27. [27] V. Desnitsky, D. Levshun, A. Chechulin, and I. Kotenko, "Design technique for secure embedded devices: Application for creation of integrated cyber-physical security system," J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl., vol. 7, no. 2, pp. 60–80, 2016, doi: 10.22667/JOWUA.2016.06.31.060.
28. [28] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," IEEE Commun. Mag., vol. 54, no. 6, pp. 152–158, 2016, doi: 10.1109/MCOM.2016.7498103.
29. [29] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey," Futur. Internet, vol. 12, no. 4, p. 65, 2020.
30. [30] M. Lin et al., "Integrated 5G-Satellite Networks: A Perspective on Physical Layer Reliability and Security," IEEE Wirel. Commun., vol. 27, no. 6, pp. 152–159, 2020, doi: 10.1109/MWC.001.2000143.
31. [31] Y. Wan, K. Xu, G. Xue, and F. Wang, "IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes," Proc. - IEEE INFOCOM,

vol. 2020-July, pp. 874–883, 2020, doi: 10.1109/INFOCOM41043.2020.9155424.

32. [32] H. Lei, M. Xu, I. S. Ansari, G. Pan, K. A. Qaraqe, and M. S. Alouini, “On secure underlay MIMO cognitive radio networks with energy harvesting and transmit antenna selection,” IEEE Trans. Green Commun. Netw., vol. 1, no. 2, pp. 192–203, 2017, doi: 10.1109/TGCN.2017.2684827.
33. [33] G. Kavallieratos, S. Katsikas, and V. Gkioulos, “Cybersecurity and safety co-engineering of cyberphysical systems - A comprehensive survey,” Futur. Internet, vol. 12, no. 4, 2020, doi: 10.3390/FI12040065.
34. [34] L. Pietre-Cambacedes and M. Bouissou, “Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes),” Conf. Proc. - IEEE Int. Conf. Syst. Man Cybern., pp. 2852–2861, 2010, doi: 10.1109/ICSMC.2010.5641922.
35. [35] L. Pietre-Cambacedes and M. Bouissou, “Cross-fertilization between safety and security engineering,” Reliab. Eng. Syst. Saf., vol. 110, pp. 110–126, 2013, doi: 10.1016/j.ress.2012.09.011.
36. [36] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, “A survey of approaches combining safety and security for industrial control systems,” Reliab. Eng. Syst. Saf., vol. 139, pp. 156–178, 2015, doi: 10.1016/j.ress.2015.02.008.
37. [37] S. Chockalingam, D. Hadžiosmanović, W. Pieters, A. Teixeira, and P. van Gelder, “Integrated safety and security risk assessment methods: a survey of key characteristics and applications,” in International Conference on Critical Information Infrastructures Security, 2016, pp. 50–62.
38. [38] M. F. H. Abulamddi, “A Survey of Approaches Reconciling between Safety and Security Requirements Engineering for Cyber-Physical Systems,” J. Comput. Commun., vol. 05, no. 01, pp. 94–100, 2017, doi: 10.4236/jcc.2017.51008.
39. [39] E. Lisova, I. Šljivo, and A. Čaušević, “Safety and Security Co-Analyses: A Systematic Literature Review,” IEEE Syst. J., vol. 13, no. 3, pp. 2189–2200, 2019, doi: 10.1109/JSYST.2018.2881017.
40. [40] X. Lyu, Y. Ding, and S.-H. Yang, “Safety and security risk assessment in cyber-physical systems,” IET Cyber-Physical Syst. Theory Appl., vol. 4, no. 3, pp. 221–232, 2019.
41. [41] H. dan C. O’Donnell, “Scholar (22),” Solar energy research, vol. 3, no. 1. pp. 204–208, 2004.
42. [42] J. P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, and P. Urien, “SarA: Security automotive risk analysis method,” CPSS 2018 - Proc. 4th ACM Work. Cyber-Physical Syst. Secur. Co-located with ASIA CCS 2018, no. May, pp. 3–14, 2018, doi: 10.1145/3198458.3198465.
43. [43] D. P. Eames and J. Moffett, “The integration of safety and security requirements,” in International Conference on Computer Safety, Reliability, and Security, 1999, pp. 468–480.
44. [44] K. Mona and Y. Dubey, “Advanced technique for cooperative spectrum sensing optimization in cognitive radio network,” Int. J. Eng. Tech. Res., vol. 8, no. 5, 2019.
45. [45] N. T. Nguyen, R. Zheng, and Z. Han, “On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification,” IEEE Trans. Signal Process., vol. 60, no. 3, pp. 1432–1445, 2012, doi: 10.1109/TSP.2011.2178407.
46. [46] Y. Yu, L. Hu, H. Li, Y. Zhang, F. Wu, and J. Chu, “The security of physical layer in cognitive radio networks,” J Commun, vol. 9, no. 12, pp. 28–33, 2014.
47. [47] Y. Zou et al., “Detection of PUE attacks in cognitive radio networks based on signal activity pattern,” 2013 8th Int. ICST Conf. Commun. Netw. China, CHINACOM 2013 - Proc., vol. 30, no. 10, pp. 699–703, 2013, doi: 10.1109/JSAC.2012.121102.
48. [48] E. Altman, K. Avrachenkov, and A. Garnaev, “Jamming in wireless networks under uncertainty,” Mob. Networks Appl., vol. 16, no. 2, pp. 246–254, 2011.

49. [49] R. Cao and Y. Lu, “On Study of physical-layer attack detection for large volumes of data,” in 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), 2017, pp. 30–34.
50. [50] Q. Huang, M. Lin, J. B. Wang, T. A. Tsiftsis, and J. Wang, “Energy Efficient Beamforming Schemes for Satellite-Aerial-Terrestrial Networks,” IEEE Trans. Commun., vol. 68, no. 6, pp. 3863–3875, 2020, doi: 10.1109/TCOMM.2020.2978044.
51. [51] M. Yasin, B. Mazumdar, J. Rajendran, and O. Sinanoglu, “Hardware security and trust: Logic locking as a design-for-trust solution,” in The IoT Physical Layer, Springer, 2019, pp. 353–373.
52. [52] D. Das and S. Das, “Primary user emulation attack in cognitive radio networks: A survey,” IRACST-International J. Comput. Networks Wirel. Commun., vol. 3, no. 3, pp. 312–318, 2013.
53. [53] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. Bin Song, and H. Li, “A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids,” IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 2659–2668, 2014.
54. [54] K. Andersson, “Mapping out dependencies in network components in critical infrastructure.” 2018.
55. [55] X. He and H. Dai, Adversary Detection For Cognitive Radio Networks. Springer, 2018.
56. [56] W. Sibanda and P. Pretorius, “Novel application of Multi-Layer Perceptrons (MLP) neural networks to model HIV in South Africa using Seroprevalence data from antenatal clinics,” Int. J. Comput. Appl., vol. 35, no. 5, pp. 26–31, 2011.