COMPARISON OF DIFFERENT TYPES OF PHYSICAL LAYER SECURITY TECHNIQUES IN WIRELESS COMMUNICATION SYSTEMS: A REVIEW

Muhammad Imran Khan
University of Lahore
Islamabad Campus
PAKISTAN

Muhammad Riaz
University of Lahore
Islamabad Campus
PAKISTAN

ABSTRACT

The physical data transportation methods are different in wireless communication as compare to wired communication networks. The main difference between these communication is how to secure the channel during the broadcasting from the at- tacks such as interference, eavesdropping and jamming. Previous traditionally proposed techniques are not suitable to secure the physical layer of wireless communication system. In this paper we identified the different types of threats that attack the physical layer when the channel is open and broadcasting a message signal. Then we give the comprehensive overview off different types of security techniques that are used to secure the physical layer, these techniques are categorized in three types: time domain, spatial domain and frequency domain based. Furthermore, we analyze the pros and cons of currently using technologies in each category.

Keywords: Wireless Sensor Networks (WSNs),Direct Sequence Spread Spectrum (DSSS),Single-Input Multiple- Output (SIMO), Multiple-Input Multiple-Output (MIMO), low probability of interception (LPI),Coordinate Interleaved Orthogonal Designs (CIOD), Orthogonal Frequency Divi- sion Multiplexing(OFDM),Frequency Hopping Spread Spec- trum(FHSS).

INTRODUCTION

Wireless Communication system means to transfer information from one system to another system using different mediums of communication such as optical fiber, wireless link, hard disk drive of computers these mediums is known as communication system. Fig 1.1 sows the Wireless Communication system. There are two types of communication channels wired and wireless communication channels. [1] If transmitter and receives is connected through wire is calls wired channel and if transmitter and receiver is connected without wire is called wireless channel. The main difference between wired and wireless channel depends on their reliability and data transfer rate. Wired channel is more reliable then wireless channel because wireless channel behavior changed frequently due to less time spam and low rate transmission to the high capacity networks. Hybrid network is designed in which devices are connected using wired and wireless technology. Our focus on wireless communication system in which data transfer from transmitter to receiver through electromagnetic waves. The first wireless communication system experiment is performed by Guglielmo Marconi in 1897 between a fixed-station and a ship. For increase in capacity of wireless channels has experience for better growth of wireless communication system. After establishment of voice services in wireless communication wired-line services are replaced with wireless services. There are various field s of wiles communication channels. WLAN (Wireless Local Area Network) used in different residential areas, Schools and office buildings.PAN (Personal area network) is a connection between two user devices such as Bluetooth, Mobile portable hotspot etc[2].The aim of this research to provide a complete overview, how to secure the

physical layer in wireless communication system.However, because of broadcast nature these systems are unreliable and face security issues such as interface, tampering, Denial of Service, leakage, counterfeiting, eavesdropping, network flooding etc[3].Furthermore, these

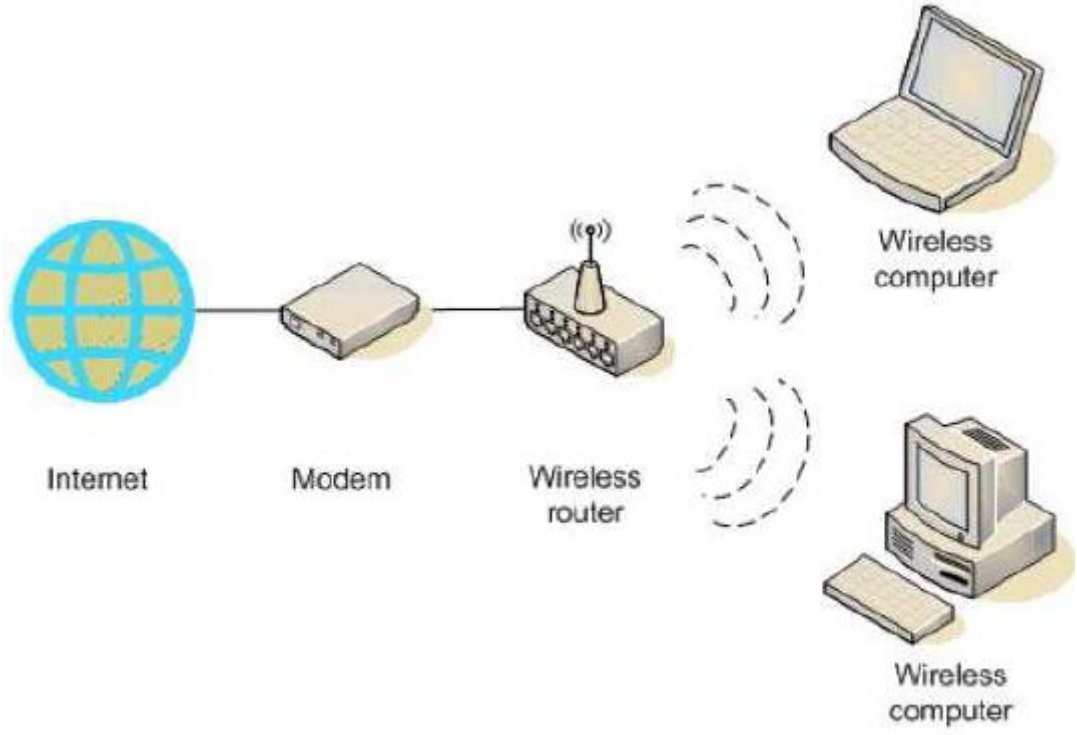

Fig. 1. Wireless Communication system.

security issues are key challenge in the evolution of wireless communication. To overcome these issues most of the researchers focused on encryption /decryption, authentication and trust management [4]. Encryption /decryption method is not enough to ensure the security of complex wireless structure. Such as issues related to interface and eavesdropping in physical layer cannot be solved by this technique [5, 6]. Furthermore, structured signaling scheme and cooperative techniques are most emerging technologies that are used to overcome the drawback of physical layer [7]. These techniques use different characteristics of wireless communication system to reduce the complexity and eliminate the risks of interference and attach such as random parameter, spread spectrum etc [8].In this paper we identified the different types of threats in physical layer of wireless communication systems and then compare the different types of techniques used to overcome these threats in physical layer.

TYPES OF ATTACKS IN PHYSICAL LAYER

In wireless communication systems physical layer is at the bottom and responsible for carrier frequency generation, frequency section, modulation and signal detection. Wire- less communication systems receive the information signals through the physical layer and then send this data stream to the upper layers for demodulation. Different types of physical attacks disturb the transmission characteristics of physical layer.in general attacks are categorized in two categories such as active and passive attacks.

Active Attacks

Jamming and interference are including in active attacks. these two types of attacks effected the broadcasting signal in some specific frequency bands.Jamming attack is occurring due to transmitter failure and interference attach is occurs when the receiver is unable to receive the signal signal due to interference. Malicious attacks are also known as jamming attack and interference is not only caused by the hostile attackers but it's also effected by the users who are using same channel.For Example, a large number of nodes are uniformly distributed in WSNs and multihop transmission is used for communication, signal transmission from one node to another node is easily effected in this scenario.In [9] authors describe the different types of jamming attacks such as barrage jamming, spot jamming, deceptive jamming and sweep jamming.

- ***Deceptive Jamming:*** In this type of jamming attackers send the effected data packets to the users through the network and make sure that these packets are received by the users as a normal data packets. This type of jamming is very difficult to detect and its very damaging.
- ***Barrage Jamming:*** Large number of frequencies is at- tacked at a same time and its effected the whole com- munication between the users under the barrage jamming coverage area. Transmission power limit factor is effected on the wide range frequencies. Wide range frequencies are attacked by the attackers and weak frequencies are jammed.
- ***Spot jamming*** is very simple and widely used technology in which high power signal is transmitted to cover the original signal. Spot jamming mainly focus on individual frequency jamming. *Sweep jamming:* Multihop technology is used by at- tacker in sweep jamming because wide range frequencies are easily covered and its directly attack on frequency-hopping technology.

There are two types of interference which are active and passive interference [10]. Furthermore, active interference also categorized in two sub types on-demand interference and random interference [11].

- ***On-Demand Interference:*** Hiding techniques are imple- mented in this type when the interference interrupted the transmitted signal. Direct-sequence spread spectrum have spectrum density with low power to transmit a signal. The spectrum of transmitted signal is similar to the noise single power so that it's time to enhance the information hiding techniques performance effectively.
- ***Sustained interference:*** In this type of interference at- tackers effect the normal communication through sending the interference signal to occupy the channel for long time for delay the communication. It's also effect the data transmission time and effect the transmitted message.
- ***Random Interference:*** Randomly users are effected from this interference because the interference cycles and time are ambiguous as compare to sustained interference its effected the energy consumption and effect the multihop WSN.

Furthermore, interference and jamming signal bandwidth can also be categorized as narrowband and wideband. In narrow band attacks the narrow range frequency range is usually used. However, advancement in technology is increased time to time and 3g and 4g jamming and interference bandwidth could be up to MHz.

Passive Attacks

There are Two types of passive attacks traffic analysis and eavesdropping. These attacks are caused due to the characteristics of some fundamental issues of wireless medium, broadcast message and name [11]. Wireless communication is difficulty to secure from the unwanted intruders due to its broadcast nature, illegal or legal user within the coverage area get access to

utilize and analyze the wireless signal [12]. Information of the users are easily accessed by the intruders due to open access of wireless communication channels in Eavesdropping communication information systems. The attackers are analysis the traffic flow and changes in the networks and extract the information from the current ongoing communication. Such as in wireless sensor network an intruder easily check he position of base station and changes in networks traffic. In other words, attackers hack the base station and paralyze the entire communication network [13].

PHYSICAL LAYER SECURITY TECHNIQUES

In 1949 theoretical concept of physical layer information security transmission was built with the help of Shannon's notation [13] by wyner [14]. Furthermore, Csisx'ar and korner extend this technology [12].In [13] author find that the existing codes for channel security are use full if the length of the secret

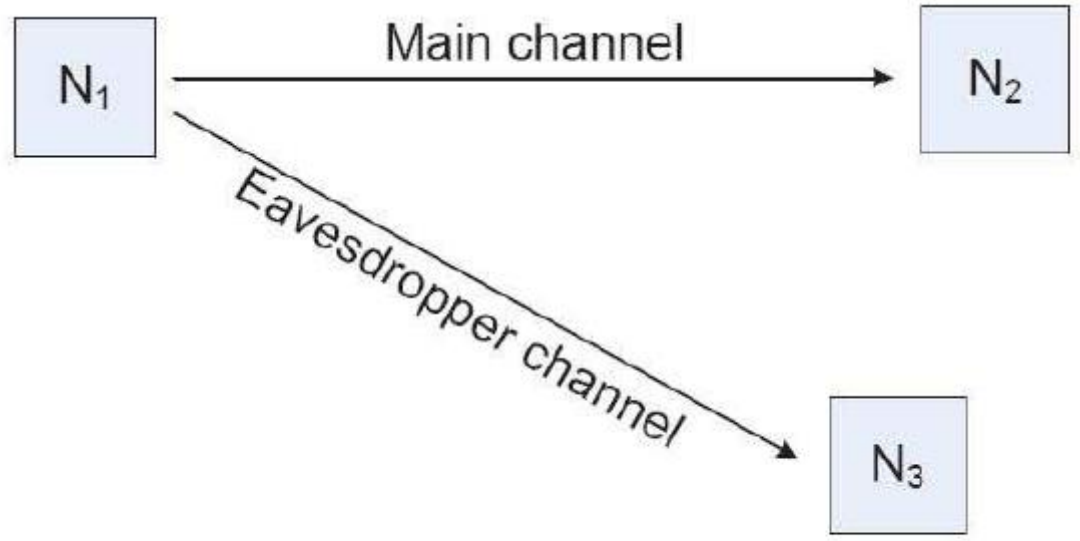

Fig. 2. Eavesdropping Scenario.

key is longer than the transmitted information. Nowadays there are lot of emerging technologies and security methods such as MIMO, SIMO and relay channels are used to secure the physical layer in wireless communication systems[15].Later on wireless communication systems enhance the physical layer security by combining the different security techniques .In [16] authors proposed amplify-and-forward compressed sensing (AF-CS) frame work to enhance the physical layer security in which different eavesdropping nodes are in listen- ing state.In[17] different physical layer security technologies with respect to spatial domain, time domain and frequency domain are presented and conclude the results on the bases of these technologies.

Spatial Domain Technologies

Spatial domain technologies consist of beamforming, di- rectional antennas. Antenna technologies are used to avoid the realization or signal interference with the random channel parameters, with these technologies system become wiretap resistant, anti-interference and anti-jamming.

1) ***Directional Antenna and Beamforming Techniques:*** *Di- rectional antenna* transmit signal in more than one directions with high transmission power and cover wide geographical coverage and cover long transmission distance. When signals are received at directional

antenna, its categorized the main beam in beam and nulling align. In beam align locate the original message signal and null align deals with the interfer- ence signal. With this techniques directional antenna eliminate or reduce the interference. Furthermore, it's also degrade the interference and reduce the performance for anti-jamming and anti-interference[17].Directional antenna enhances the ant jamming performance of antenna as compare to unidirectional antenna [18]. Energy consumption of directional and uni directional antennas are same, but in low transmission power and equal iso tropical radiated-power at the receiver end reduce the probability of detecting the interference [19].Gain performance and muni atomization is improved with the directional antenna and its used in adhoc networks, wireless mesh networks to enhance the performance of communication system[19]. Directional antenna is best choice to overcome network connectivity and interference issues. *Beamforming* also used as an alternate of directional antenna which is a combination of multiple array antennas. Antenna bean direction can be se through the number of configure antennas, geometry and element spacing. To avoid the interference, the direction of antenna set towards the legitimate receiver[20].Transmitted signal is concentrated and intense, due to these factors the ability to resist the eaves- dropping, cross talk and jamming will be increased among the multiple users[21].Beamforming is not suitable for low power networks because its power consumption is much higher than the directional antennas.in [22] jamming beamforming and joint beamforming antennas are designed to protect the communication between the sender and receiver for a full duplex BS.In[23] authors proposed a multi antenna secure relay technology to secure the physical layer of wireless communication system. They proposed the large scale MIMO technology which is used to solve the problems in short dis- tance interference.Nowadays smart antennas are widely used in 3G and 4G communication technologies. It also improves the communication rate while solve the interference in multi user communication issue. Multiple antennas are not widely used in beamforming but it used cooperative array antennas for multimode cooperative networks[23].

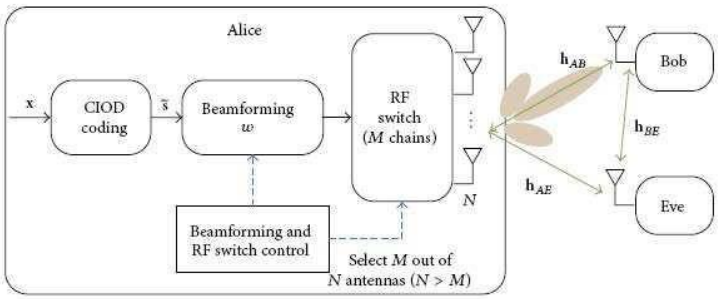

Fig. 3. Proposed System model of ASM with CIOD in [24].

Random Parameters and Random Antenna Technology: Random Parameter development is based on beamforming concept. Randomization is caused due to weight of the trans- mission antenna, and user received eavesdropper's signals but the legitimate user's communication not effected by chan- nel.Redundancy of transmitted antenna arrays are exploit for signal randomization. Furthermore, the channel multiplication, parameters multiplication and random coefficient have fixe value and it's not affect the demodulation [25].Low power probability interception is used by randomized transmission array to indeterminacy of wireless communication for eaves- dropper's blind deconvolution. Random parameter is also sim- ilar to random antennas. Main difference between the random parameter and random antenna is that the random parameter is executed by the random weighting coefficient and random antennas are receive the random signals. Furthermore, the ran- dom antenna mostly used MIMO systems. The signal transmits from the transmitter randomly and continuously, to realize that the transmission between the randomization between the illegal or legal user with the transmitter[26].In [27] authors proposed a secure MIMO wireless communication scheme that is totally based on the combine Proposed model shown in fig 3 is working with both array gains and diversity to potential eavesdropping

against them. Authors used the ASM scheme to get better results for the mm wave frequencies using the antenna arrays[24].ation of Antenna Subnet Modulation and Coordinate Interleaved Orthogonal Designs.Direction of dependent transmission data is retrieve from the symbol rate of modulated radiation pattern.ASM introduce the additional functions in the conste-llation to provide more security to the desired receiver. Furthermore, the random parameters for the appropriate users are use the training channel for smooth communication and signal demodulation and performance can be enhancing by add more antennas in the system. Signal uti- lization is the weak point of this technology because multiple antennas are used for transmission[15].

Artificial Noise Technology

Artificial noise required the highest capacity from the ap- propriate channel that is connected with the eavesdropping channel when the channel state information is better than the eavesdropping channel security increase for the appropriate channel[12].Artificial noise is produced by the transmitter when the available power is used by transmitter, and degrade the eavesdropping channel. Beamforming is used to aided the artificial noise from the channel.Beamforming method was proposed in [28] in which authors used multiple antennas for the development of zero space. Furthermore, they introduce the noise signal for zero space for the appropriate channel which made the receiver more efficient to extract the real information from the signal using noise filtering, but illegal user are affected by these noise signals.From the last years many researcher work on the optimization based techniques [29, 30]. Such as in [31] QoS is ensured and they use limited indicator for the SINR to assist the artificial-noise and save energy for the communication system and improve the security capacity .In[32] artificial noise techniques was extended from the zero space to the signal space and get much batter results. Analog coding systems is proposed in [33] which is based on the artificial noise which is used to increase the physical layer security in wireless communication system.In this proposed technology the selected parts of antenna received the reference signals from the broadcast phase and these antenna parts are selected by the relay node, beamforming matrix is derived when the reference signal is received at the different parts of the antenna and this matrix is equal to the noise vector channel fading matrix. Furthermore, in [34] authors extend this tech- nology to MIMO orthogonal frequency division multiplexing and also introduce the spatio temporal selective artificial noise approach calculate the estimation of errors for eavesdropping channel. However, this technology is still impractical and there are many issue still persist that can be solved.

Time Domain Technologies

Time domain is the most popular technology used in channel coding introduced by Shannon [13]. Shannon channel model prove that the encoded information signal can be send in the presence of noise and realize that the capacity of secure transmission channel arbitrary rate is low. Further- more, channel codding plays an important role to correct the transmitting information using some check codes. There are many channel codding schemes are used now a days such as LDPC, BCH, Turbo, and soft decode-compress-forward schemes.Binary numerical systems was introduced by kwat et al[35] ,it's also called yarg codes .These codes are used as a QAM mapping scheme to create a sequence of multiple binary bits for the QAM constellation symbols.QAM symbol mapping gray codes have different characteristics as compare to Yarg codes. Due to these effects the gray codes are minimize to get the required SNR to get the required BER ,use of Yarg codes minimize the security gap[36].In[37] authors estimate the security issues over the AGWN wiretap channel that can be used to measure the effectiveness of the different transmission techniques.AGWN wiretap channel scheme can be used to cover the security gap between the unauthorized and authorized channels. This security

gap can be reducing while send the scramble information bit and non-systematics codes with the transmitted information code word.LDPC code are the most popular and efficient channel coding scheme after Turbo channel codding schemes and its used widely by army, civil, commercial and other areas due to its better error cor- rection ratio. In [38] authors proposed a physical layer coding scheme that is totally based on RC-LDPC codes to secure the communication for the Gaussian wiretap channel.Yang et al [39] proposed a channel coding scheme in which artificial nose can be add with the wiretap channel to increase the security of the physical layer. In this channel coding scheme artificial noise cover the null space at the side of appropriate receiver but it acts like a ransom interference at the eavesdropper receiver side and transmit information signal using precoding technique.

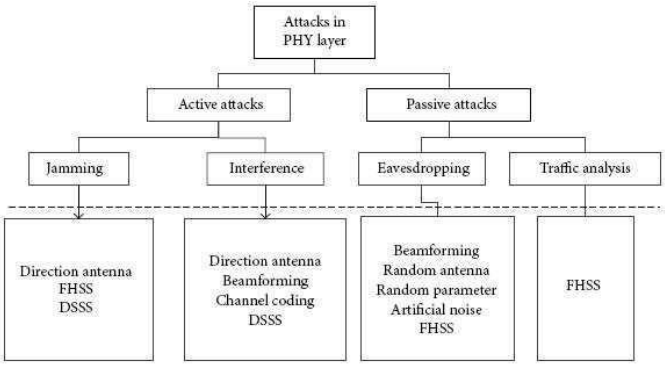

Fig. 4. Categories of Physical layer attack and defense techniques.

Frequency Domain Technologies

Frequency domain technology is used for the security of physical layer. Its use the wide range and change able carrier frequency to reduce the interference. Nicola Tesla firstly intro- duced the spread spectrum, it was used by the U. S military. Due to its anti-jamming characteristics this technology was applied by U.S military in their field operation areas and civil areas in 1980s [40].Spread Spectrum used to modulate the original signal and transmit the signal in the pseudo random sequence, and the receiver demodulate the signal using the same technique and sequence to get the original information signal. SNR is increased in this process but interference reduced.Spread spectrum is divided in different categories ac- cording to the method used to extend the narrow band signals. Spread spectrum categories are FHSS,DSSS,THSS,CSS and the consolidation of these techniques.

TABLE I
COMPARISON OF PHYSICAL LAYERS SECURITY TECHNIQUE IN WIRELESS NETWORKS

Secure technique	Beamforming	FHSS	Channel coding	Artificial noise	DSSS	Random parameters	Random antennas	Direction alantenna
Type	Spatial domain	Frequency domain	Time domain	Spatial domain	Frequency domain	-	Spatial domain	Spatial domain
Technical characteristics	Super imposed multi antenna signal	Fast hopping of carrier frequency	Powerful error correc- tion capability	Increased channel diversity	Increased band width	Increased signal random- ness	Increased channel randomness	Increased receive gainin particular direction of space
Ability to defend against jamming attacks	-	High	-	-	Higher	-	-	Medium
Ability to defend against eavesdropping attacks	Medium	Higher	-	High	-	Higher	Higher	Low
Complexity	High	Medium	Low	High	Medium	High	High	High
Ability to defend against interference attacks	Low	-	High	-	Medium	-	-	Low

FHSS and DSSS give better results for anti jamming than the other techniques.In DSSS sender modulate the signal using the pesudinoise se- quence on a wide band. The noise sequence and the modulated signal spectrum are same, this similarity enhance the conceal- ment of modulated signal and decrease the interference effects. At the receiver end same sequence used to demodulate the received signal and the spectrum density will be decreased for the interference signal but at the other end spectrum density of useful signal will be increased. Original signal finally received and most of the noise signal filtered. Narrowband interference is limited in this process due to limited wide band bandwidth. We can get better performance by using the hybrid DS/FH DSSS technologies for multiuser interference, jamming and channel fading scenarios [41].In [42] FHSS acknowledge that the set of pseudorandom sequence codes are used by the sender for frequency fast hopping and different frequencies are used the different hopping frequencies this code is only know by the sender and the receiver.At the other hand FHSS security is depends on the frequency hopping pattern complexity.In [[43] authors proposed a new way to construct a CDMA pattern that sets the linear complexity of the appropriate sequence and new frequency hopping sequence will be formed. The different categories of Physical layer attack and defence techniques are listed in Figure 4.

COMPARISON

In this section we compares the different security tech- nologies in physical layer .As discussed above the security techniques are used to defensed the channel from interference, eavesdropping and jamming attacks. We compare the previous discussed techniques with respect to their technical character- istics, complexity and ability to defend the attacks, Table 1 shows the comparison of these techniques, (-) shows that the no significance considered or weak significance.

CONCLUSION

We observe that there are few researchers who are working on the security of physical layer in wireless communication systems. In this paper we studied the different types of articles related to physical layer security threats and techniques used to enhance security.Three basic aspects involved in physical security frequency domains, spatial domain, time domain are described. Furthermore, security techniques are also described and compare with respect to their technical aspects. Physical layer security need a wide storage space and power full computing capacity and additional powerful hardware units to overcome security issues.Now a days most of the security techniques are used to defend the jamming and interference at- tacks. Secure channel from eavesdropping attacks are depends in the encryption technology that is used to encrypt the data at upper level. Most of the security techniques are at theoretical stage and not applied to any wireless communication system to secure the physical layer.

REFERENCES

[1] A. Paulraj, R. Nabar, and D. Gore, *Introduction to space-time wireless communications*. Cambridge university press, 2003.
[2] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.
[3] 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," *Journal of Sensors*, vol. 2015, 2015.
[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.
[5] Z. Chen, M. He, W. Liang, and K. Chen, "Trust-aware and low energy consumption security topology protocol of wireless sensor network," *Journal of Sensors*, vol. 2015, 2015.
[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.
[7] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, 2013.
[8] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via coopera- tion: Signal design and optimization," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 47–53, 2015.
[9] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, 2009.
[10] 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 wireless Communications*, vol. 18, no. 2, 2011.
[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005, pp. 46–57.
[12] I. Csiszár and J. Korner, "Broadcast channels with confidential mes- sages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.
[13] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[14] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[15] Y. Zou, J. Zhu, and B. Zheng, "Defending against eavesdropping attack leveraging multiple antennas in wireless networks," in *Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on*. IEEE, 2013, pp. 699–703.

[16] J. E. Barcelo-Llado, A. Morell, and G. Seco-Granados, "Amplify-and- forward compressed sensing as a physical-layer secrecy solution in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 839–850, 2014.

[17] W. Fang, F. Li, Y. Sun, L. Shan, S. Chen, C. Chen, and M. Li, "Information security of phy layer in wireless networks," *Journal of Sensors*, vol. 2016, 2016.

[18] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *International Conference on Wired/Wireless Internet Communications*. Springer, 2004, pp. 186–200.

[19] X. Lu, F. D. Wicker, D. Towsley, Z. Xiong, *et al.*, "Detection proba- bility estimation of directional antennas and omni-directional antennas," *Wireless personal communications*, vol. 55, no. 1, pp. 51–63, 2010.

[20] O. Bazan and M. Jaseemuddin, "A survey on mac protocols for wireless adhoc networks with beamforming antennas," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 216–239, 2012.

[21] C. Walsh, D. Hakkarinen, and T. Camp, "Distributed decode and forward beamforming," in *Local Computer Networks (LCN), 2012 IEEE 37th Conference on*. IEEE, 2012, pp. 436–444.

[22] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information-and jamming- beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, 2014.

[23] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Communications Maga- zine*, vol. 53, no. 12, pp. 40–46, 2015.

[24] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, 2013.

[25] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions." *JCM*, vol. 2, no. 3, pp. 24–32, 2007.

[26] G. Zhao, "Secure transmission in phy layer of wireless communications based on random antenna array," *China CIO News*, vol. 5, p. 96, 2013.

[27] Y. Hong, S. Im, and J. Ha, "Secure antenna subset modulation with co- ordinate interleaved orthogonal designs," in *Information and Communi- cation Technology Convergence (ICTC), 2014 International Conference on*. IEEE, 2014, pp. 97–98.

[28] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, 2008.

[29] S. H. Chae, W. Choi, J. H. Lee, and T. Q. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.

[30] A. Bilal, M. Riaz, and M. Y. Wani, "Mobile-to-mobile gaussian scatter- ing channel model." *Science International*, vol. 28, no. 4, 2016.

[31] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial- noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.

[32] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.

[33] D. Deng, Z.-l. Yang, and M. Zhao, "Phy security enhancement in analog network coding based on artificial noise," in *Wireless Communications and Signal Processing (WCSP), 2014 Sixth International Conference on*. IEEE, 2014, pp. 1–6.

[34] Ö . Cepheli and G. K. Kurt, "Efficient phy layer security in mimo-ofdm: Spatiotemporal selective artificial noise," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*. IEEE, 2013, pp. 1–6.

[35] B.-J. Kwak, N.-O. Song, B. Park, D. Klinc, and S. W. McLaughlin, "Physical layer security with yarg code," in *Emerging Network Intelli- gence, 2009 First International Conference on*. IEEE, 2009, pp. 43–48.

[36] F. Gray, "Pulse code communication, us patent 2,632,058," 1953.

[37] M. Baldi, M. Bianchi, and F. Chiaraluce, "Non-systematic codes for physical layer security," in *Information Theory Workshop (ITW), 2010 IEEE*. IEEE, 2010, pp. 1–5.

[38] M. H. Taieb and J.-Y. Chouinard, "Enhancing secrecy of the gaussian wiretap channel using rate compatible ldpc codes with error ampli- fication," in *Information Theory (CWIT), 2015 IEEE 14th Canadian Workshop on*. IEEE, 2015, pp. 41–45.

[39] Z. Yang, Y. Fan, and A. Wang, "Artificial noise and ldpc code aided physical layer security enhancement," 2014.

[40] W. Xu, "Jamming attack defense," in *Encyclopedia of cryptography and security*. Springer, 2011, pp. 655–661.

[41] M. Olama, S. Smith, T. Kuruganti, and X. Ma, "Performance study of hybrid ds/ffh spread-spectrum systems in the presence of frequency- selective fading and multiple-access interference," in *Communications Quality and Reliability (CQR), 2012 IEEE International Workshop Technical Committee on*. IEEE, 2012, pp. 1–5.

[42] M. Darnell and H. Yung, "Security considerations in frequency hopping radio systems," in *Security and Cryptography Applications to Radio Systems, IEE Colloquium on*. IET, 1994, pp. 11–1.

[43] A. Leukhin, O. Moreno, and A. Tirkel, "Secure cdma and frequency hop sequences," in *Wireless Communication Systems (ISWCS 2013), Proceedings of the Tenth International Symposium on*. VDE, 2013, pp. 1–5.