Security of Wireless Communications against Eavesdropping and Attacks by Using Shannon's Theory

Bretas Alberto, Dong Wen*

School of Electrical, Electronic and Computer Engineering, The University of Western Australia,
Crawley WA 6009, Australia

Keywords:
Wiretap Attack;
Information Security;
Physical Security;
Security;
Wireless Networks

Corresponding Author Email:
don.weng@uwa.edu.au

DOI: 10.31838/IJCCTS.12.01.10

Received: 10.04.24

Revised: 19.05.24

Accepted: 26.06.24

Abstract

This research applies Shannon's information theory on improving the security of the wireless communication from eavesdropping and attacks. Most wireless networks are prone to security threats because of their nature of operation as compared to the wired network which makes it important to establish secure means of transmitting data. Another measure that gives a quantitative estimate to the problem of obtaining the maximum reliable rate of information transfer is Shannon's information theory. This paper discusses techniques like physical layer security that takes advantage of the characteristics of the channel to minimize the quantity of data that can be overheard by an attacker. Hence, we seek to find the channel condition and employ artificial noise generation, cooperative jamming and secure beamforming to reduce the capacity of the eavesdropper channel while boosting the legitimate user's date rate. Furthermore, we analyze non-symmetric pre-shared key security solutions that do not incorporate classical cryptographic keys ensuring higher levels of security against computational threats. Analyzing the results theoretically and by simulation, this study demonstrates that applying the principles which were derived from Shannon's theory can enhance security in wireless networks particularly when facing adaptive adversaries. The findings reported in this paper help in designing more secure wireless protocols, which are vital in the future M2M and IoT systems.

How to cite this article: Alberto B, Wen D (2024). Security of Wireless Communications against Eavesdropping and Attacks by Using Shannon's Theory . International Journal of communication and computer Technologies, Vol. 12, No. 1, 2024, 76-85

Introduction

Wireless networks or more commonly known as WiFi is one of the most utilized technologies in the modern world. However, having wireless connectivity as a form of relating to the network has its own security issues one of which is WiFi eavesdropping. This emerging antis has spurred numerous researchers and security specialists to look for new ideas in order to protect data in transit over WiFi networks. The Shannon's Information Theory appears to provide a viable solution to strengthen the security of WiFi network. To make WiFi eavesdropping considerably difficult, this approach integrates several highly effective ideas including signal-to-noise ratio and key generation. Focusing on WiFi channels, the article goes a step further in how Information Theory is implemented and touched on concepts like quantization and direct sequence spread spectrum. In addition, this paper discusses the applicability of orthogonal frequency division multiplexing to enhance security measures that could help researchers to analyse practical application of this technology and anticipate developments in the future.[1-4]

The Evolution of WiFi Security

In the development process of WiFi security, there are phased innovations and continuous problems. With the wireless networks admiring the society, the necessity for the most efficient security measures that would prevent such issues as wifi eavesdropping, etc., were in urgent need of rapid improvement.

WEP to WPA3

The changes in the mechanisms guarding wireless communication needs be seen only as a continuous progress in the fight between the defenders and attackers. The first significant standard that ever launched was the Wired Equivalent Privacy (WEP) in 1997 aiming on the security standard of wired network. WEP employed a 64 or 128 bit key along with a 24 bitInitialization Vector (IV) and constructed the RC4 encryption. Nonetheless, WEP has its fundamental flaws, such as the utilisation of static keys along with a fragile encryption algorithm to precede him. Because of these shortcomings, the Wi-Fi Alliance introduced, in the meantime solution, known as the Wi-Fi Protected Access (WPA) in the year 2003. WPA brought in the Temporal Key Integrity Protocol (TKIP) this more effectively in generating a new key for every packet sent across. However, WPA was not without its weakness especially in the personal mode where all users were provided with a single pre-shared key (Figure 1).[5]

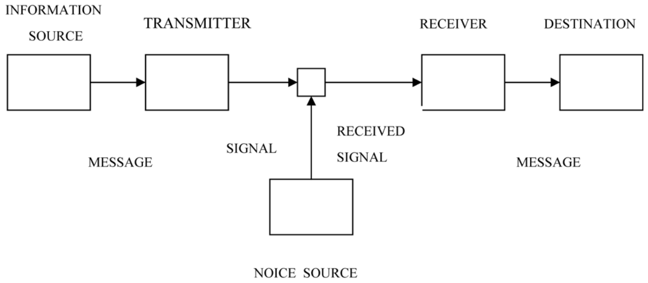

Fig. 1: Shannon's Information Theory to Prevent WiFi Eavesdropping

The optional elements of IEEE 802.11i were adopted in WPA2 in 2004 providing the mandatory features. This protocol signified a big enhancement by integrating AES through the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). WPA2 offered better encryption and improved key management and therefore became a market norm for several years. The current version is WPA3 that was released in 2018 to.of the previous versions, WPA3 came with longer security features. WPA3 is capable of protecting against attempts to guess the correct password and also offers forward secrecy in the event even the password is cracked in the future, the data will still not be intercepted. They also benefit when it comes to the security of open networks and when initializing the setup of devices which do not support graphical user interfaces.[6]

Persistent Vulnerabilities

Nonetheless, WiFi networks are not immune from security concerns even whereas the world has evolved means of developing and implementing new technologies. First one is the susceptibility to password cracking attacks a situation that is compounded by poor password selection methods. This is especially so in the WPA-Personal and WPA2-Personal modes where common passwords are easily crackable by rainbow tables. Another weakness is absence of the forward secrecy in WPA and WPA2 protocols also constrain the data protection significantly. This means that if an attacker get hold of the pre-shared key, he or she will be in a position to decrypt all past and future traffic that was encrypted with the same key. This issue shows that it is necessary to change their network passwords periodically and use different and long pass phrases. The KRACK attack demonstrated in 2017 disclosed vulnerability in WPA2 protocol that made it possible for attackers to infiltrate the encrypted traffic between devices and access points. However, in some cases patches were quickly released which showcase the ever present need for increasing WiFi security and frequency of updates. Last year, the WiFi security vulnerability known as FragAttacks (fragmentation and aggregation attacks) impacted almost all WiFi devices. These opened ways for attackers within the specified reach to pilfer information or go for devices connected to the WiFi; an indication that even current modern WiFi safety standards are not safe from certain incursions. Finally, as implemented technology generally WiFi, it is also clear tactics of potential attackers vary with the advancement of implemented technology. As the 5G networks come into the world and IoT devices rise in number, WiFi security face new problems again. So, a large number of IoT devices have poor security measures that the intruders can leverage to gain access to a network. Further, cloud services have become a norm and AI has made its way into security measures as well as the means of attack in the case of WiFi security (Table 2).[7-8]

Table 2. Shannon's Information Theory in Preventing WiFi Eavesdropping

		Application in WiFi		
Concept	**Definition**	**Security**	**Benefits**	**Challenges**
Entropy	Measure of uncertainty or randomness in data	Used to assess the unpredictability of encryption keys	Ensures strong encryption with high unpredictability	Achieving high entropy requires robust key management

Concept	Definition	Application in WiFi Security	Benefits	Challenges
Channel Capacity	Maximum rate at which information can be reliably transmitted	Ensures optimal data rates while minimizing signal leakage	Prevents data from being overheard by optimizing channel usage	Hard to maintain with multiple users or noisy environments
Redundancy	Excess bits added to ensure data integrity	Introduces error-correcting codes to detect and prevent tampering	Improves reliability and error detection	Increases bandwidth usage and complexity
Mutual Information	Measures the amount of shared information between the transmitter and receiver	Used to minimize information leakage to unauthorized parties	Helps design more secure communication protocols	Requires accurate modeling of eavesdroppers' capabilities
Perfect Secrecy	Condition where the ciphertext reveals no information about the plaintext	Theoretical foundation for encryption schemes like one-time pad	Provides maximum security in theory	Difficult to achieve practically in WiFi networks due to key distribution issues

Information Theory: A New Approach to Security

With WiFi networks experiencing new security threats emerged a new approach based on Claude Shannon's Information Theory that can help prevent wifi eavesdropping. This approach is based on the conventional concepts of information theory and presents a novel approach to protect wireless data to improve the security measures in Wi-Fi networks.

Shannon's Contributions

Claude Shannon, often referred to as the father of information theory, laid the groundwork for this new approach to security. His groundbreaking paper, "A Mathematical Theory of Communication" (1948), introduced key concepts that revolutionized our understanding of information transmission and security. Shannon's work introduced the concept of entropy in information, which measures the amount of uncertainty or randomness in a message. This idea has become crucial in evaluating the strength of encryption systems. The higher the entropy, the more resistant a cryptographic system is to brute-force attacks.

Another significant contribution was Shannon's Law, also known as the Shannon-Hartley theorem. This theorem establishes the maximum rate at which information can be transmitted over a communications channel with a specified bandwidth in the presence of noise. The formula for channel capacity (C) is expressed as:

$$C = B * \log2(1 + S/N)$$

Where:

- B is the available bandwidth (in Hertz)
- S is the power of the received signal (in Watts)
- N is the power of the received noise (in Watts)

This relationship highlights two fundamental constraints on achievable data rates: relative availability of bandwidth and signal to noise ratio between the receiver and sender's equipments.

Information-Theoretic Security Principles

In line with Shannon study, information-theoretic security has become a major framework for implementing secure wireless security systems. This approach amounts to making security stem from the properties of the communication channel alone rather than from the ability of the computer to solve complex problems. Perfect secrecy is another principle which was defined by Shannon in his paper "The communication theory of secrecy systems" in 1949. This idea remains that the given ciphertext should not pass any information about the plaintext regardless of computational power. It is tricky to form ideal models in practice, nonetheless, perfect secrecy is an ideal model for security systems.

Other principle include the use of physical layer security. This approach seeks to leverage on some general characteristics of radio waves to offer security. Thus, by operating in the field of evaluation of the characteristics of the wireless channel, for example, fading and interference, it will be possible to design a safe communication channel that, by its nature, will be protected from interception. Thus, based on channel characteristics, concept of key generation is one of the application of information theoretical security. This method involves the properties of the wireless channel between two legitimate users in the creation of keys. Since an eavesdropper undergoes a sequence of a different channel he cannot simply recreate the same key, thereby making communication secure.

Here, quantization methods have valuable functions to execute information-theoretic security. These methods enable the process of digitizing the channel measurements thus enabling important key generation or any security function. Such methods as direct sequence spread spectrum and orthogonal frequency division multiplexing can also increase robustness and physically remove signal from its intended path or subdivide it to multiple subcarriers. These technique increase chances of jamming but make it even more harder for the eavesdroppers to decode the information transmitted. Accordingly, with the implementation of such information-theoretic principles, it becomes possible to envisage WiFi security systems that are inherently more secure against eavesdropping. This approach provides a direction for designing the future Wireless Local Area Network security since it realizes that the current security vulnerabilities associated with WiFi security protocols are still prevalent [9]-[10].

Characterizing WiFi Channels

If one is to try and protect their wifi from wifi eavesdropping the following characteristics of WiFi channels should be considered. These are the channels through which the wireless signals travel, and characteristics of the media have become important factors influencing the security and quality of wireless communication.

Channel State Information

CSI is a well-known term in Wireless communication system that offers fine solution about characteristics of a certain link. It simply explains how the signal passes from the transmitter to the receiver with conditions such as scattering, fading and signal power loss with increase in distance. This information is necessary for the control of the transmissions with an aim of responding to the current channel conditions which are very important for establishing reliable communication that supports high data rates in multiantenna systems. CSI can be categorized into two levels: actual CSI and statistical CSI. Instantaneous CSI offers information regarding instantaneous state of the channel, modeled similar to impulse response of a digital filter. This makes it possible to add taps for optimising the transmitted signals for low bit error rate in data transmission or for spatial multiplexing. On the other hand, statistical CSI provides the statistical information about the channel such as spatial, temporal distributions and average channel gain of the fading distribution.

The rate of change that actually constrains the acquisition or CSI is found to have a significant relationship with the rate of change of channel conditions. In slower fading systems, since the channel conditions change during the time required to transmit a single information symbol, statistical CSI is feasible. But in slow fading systems, since the rate of change in CSI's is relatively slow it can be accurately estimated and used for transmission adaptation for sometime before they become out dated. CSI is commonly described as magnetic vector that consists of numbers that show the amplitude and phases of the subcarrier in a wireless channel. This information can be obtained from commercial off-the-shelf (COTS) WiFi network interface controllers (NICs), which makes it available for multiple wireless sensing approaches which encompasses WiFi sensing and LTE sensing.

Reciprocity and Randomness

CSI is a well-known term in Wireless communication system that offers fine solution about characteristics of a certain link. It simply explains how the signal passes from the transmitter to the receiver with conditions such as scattering, fading and signal power loss with increase in distance. This information is necessary for the control of the transmissions with an aim of responding to the current channel conditions which are very important for establishing reliable communication that supports high data rates in multiantenna systems. CSI can be categorized into two levels: actual CSI and statistical CSI. Instantaneous CSI offers information regarding instantaneous state of the channel, modeled similar to impulse response of a digital filter. This makes it possible to add taps for optimising the transmitted signals for low bit error rate in data transmission or for spatial multiplexing. On the other hand, statistical CSI provides the statistical information about the channel such as

spatial, temporal distributions and average channel gain of the fading distribution.

The rate of change that actually constrains the acquisition or CSI is found to have a significant relationship with the rate of change of channel conditions. In slower fading systems, since the channel conditions change during the time required to transmit a single information symbol, statistical CSI is feasible. But in slow fading systems, since the rate of change in CSI's is relatively slow it can be accurately estimated and used for transmission adaptation for sometime before they become out dated. CSI is commonly described as magnetic vector that consists of numbers that show the amplitude and phases of the subcarrier in a wireless channel. This information can be obtained from commercial off-the-shelf (COTS) WiFi network interface controllers (NICs), which makes it available for multiple wireless sensing approaches which encompasses WiFi sensing and LTE sensing.[11]

Exploiting Channel Characteristics for Security

Consequently, the peculiarities of the wireless channels enable the novel approaches to boost up the security from wifi eavesdropping. Using these characteristics, researchers have fashioned new approaches in guarding wireless communication.

Secret Key Generation

One of the most critical uses of the channel characteristics is for secret key generation in security systems. This approach presents an alternative to the conventional technique of public key cryptography provides information theoretic security uses the randomness in wireless channel. The process relies on three fundamental principles: temporal change, symmetry of the communication channels and spatial diversification. This is as a result of the mobility of transmitters, receivers or objects in a given environment to affect channel paths by reflected, refracted, and scattered. importance, this behavior brings in random aspects that can be utilized for the purpose of key generation (Figure 2).

The essence of this technique is based on channel reciprocity. It means that the multipath and fading behavior observed at both the transmitter and receiver sides of a wireless link are same up to the time scale of channel coherence. It enables other users especially those with legal permissions to come up with the same key on their own. Spatial decorrelation means that if any lawful intercept is beyond half a wavelength distance from both the users, the fading patterns will be mutually independent. It greatly improves the keys' security that are produced by means of this principle.

Several channel parameters can be used for key generation, each with its own advantages:

1. Channel State Information (CSI): This fine-grained parameter affords explicit channel information to be included, thus allowing high KGR and resistance to predictable channel attacks.
2. Received Signal Strength (RSS): Presently the most popular parameter owing to the increased availability of its uses in practical applications.
3. Channel Impulse Response (CIR): Is utilized exclusively as the internal random source for CSI-based and RSS-based key generation systems.

As mentioned before, key generation usually has low complexity, mainly using operations that consist of sample and store data at the stage of channel probing. This makes it particularly applicable in constrained IoT devices due to the efficient use of the limited resources available.

Channel-Based Authentication

Another strong authentication method is physical layer authentication (PLA) which leverage channel characteristics to achieve secured and low complexity authentication. This method ensures wireless transmitters through employing wrist physical layer characteristics such as RF sign fingerprints, WI state data, RSS, and CIR. The major strength of PLA is its capability to employ the feature and the location of the transmitter for decision making hence eradicating the upper layering hence taking less time in computations. It is especially useful in situations where application of some standard methods of authentication can be highly inefficient in terms of resources or network topology.

Channel-based authentication techniques can identify legitimate and illegal nodes by examining various channel characteristics:

1. Received Signal Strength (RSS): Defines the signal strength of the received signal and can serve as an identification number.
2. Channel Impulse Response (CIR): Gives information on the manner in which the waveform modifies as it moves through the surrounding.

3. Channel State Information (CSI): Explains the impacts of scattering, fading and power decay on transmitted signals in given carrier frequencies.

These characteristics present a kind of one-to-one relation between various places and spatial and temporal environment al properties, which are hard for the attackers to mimic. An extra layer of security is established for channel-based authentication in MIMO systems. Multiple antennas also yield additional dimensions of channel estimation data, resulting in what is known as the 'security gain' relative to single-input single-output (SISO) systems. This approach compares channel frequency responses at subsequent frames for the identification of spoofing attacks and present better performance in different settings. Thus, utilization of such channel characteristics opens a lot of opportunities for the improvement of wireless network security from wifi snooping and other risks, and serves as the solid groundwork for ensuring safe communication in the modern world with ceaseless advancements of wireless technology.

Countering Eavesdroppers with Information Theory

The information theory offers a strong foundation on which one can design effective countermeasures that would help fight wifi eavesdropping. Hence by applying the characteristics of communication channel and signal processing, researcher has developed new way to secure the wireless communication.

Secrecy Capacity Maximization

Physical layer security, which forms the basis for this work, stems from the secrecy capacity which means the maximum rate that information can be transmitted securely from a source to a destination. Optimization of this capacity is essential in avoiding cases of wifi eavesdropping and preserving the wireless confidentiality. Certain steps that can be employed in an effort to achieve the best arrangements of secrecy capacity include; positioning of network elements and sharing of resources. For instance, in UAV-enabled relay communication systems, the authors have posed optimization problems to allocate both the power and bandwidth for trajectory planning of the UAV. These parameters are optimized such that the legitimate channel capacity is much greater than the eavesdropping channel capacity thus increasing the security of the envisaged system (Table 2).

Such optimization process uses often complex equations as the successive convex approximation-alternative iterative optimization (SCA-AIO) algorithm. This method contributes to finding solutions of the highly coupled non-convex optimization problems arising in the secrecy capacity maximization including

Table 2. Techniques for WiFi Security Based on Shannon's Information Theory

Security Technique	Based on Shannon's Concept	Description	Advantages	Limitations
Encryption (AES, WPA3)	Entropy, Perfect Secrecy	Encrypts data to make it unreadable to eavesdroppers	High level of confidentiality	Key management and complexity
Error Correction Coding	Redundancy	Detects and corrects errors introduced by noise or interference	Ensures data integrity and tamper detection	Adds overhead to data transmission
Rate Adaptation	Channel Capacity	Dynamically adjusts the data rate based on channel conditions	Optimizes data transmission, minimizing vulnerabilities	Complex to implement, especially with varying network conditions
Secret Key Agreement via Channel	Mutual Information	Generates secret keys based on the shared channel characteristics between devices	Limits eavesdropper's ability to learn the key	Dependent on accurate modeling of the environment
Physical Layer Security	Information-Theoretic Security	Leverages physical properties of the wireless channel to secure communication	Can provide security even without traditional cryptography	Still in development, complex deployment in real-world networks

information causality constraints, LoS for reliable transfer, and quality of service for mobility users.

Artificial Noise Design

This makes artificial noise (AN) as an effective weapon against wifi eavesdropping. This technique involves deliberately inserting unwanted signals known as noise to make thetraffic appear random while at the same time frustrating those who seek to eavesdrop while having minimal effects on theactual communication. It is obvious that the design of artificial noise is one of the keys to improving physical layer security. One of them is to send AN into the null space of the legitimate user's channel to minimize the interference level. This approach is effective in receiving that the AN should cause an appreciable decline in the quality of signals to the eavesdroppers while not impacting the signal-to-noise ratio of the intended receiver. Lingoes that are more elaborate than simple null-space projection of AN have been employed in the development of advanced AN design techniques. For example, some approaches optimise AN to be not perfectly aligned with the null space of the legitimate channel. This strategy can offer further security advantages especially where both the LUE and the potential eavesdropper CSI are obtainable at the transmit end.

As for practicable application, AN can also be created and forwarded by helper nodes in the network. For example, in UAV assisted IoT systems, non-Occupied IoT Sensors and Tags can start emitting predesigned artificial noise signals. This shared security approach can assist in safeguarding the dissemination of especially incoming or outgoing secret key from the UAV gateway to appropriate IoT device. It was previously determined that how well AN can mitigate wifi eavesdropping relies on power splits between the information-carrying signal and the artificial noise. Different optimization techniques have been designed to find the suitable strategy for power splitting in order to meet requirements such as the probability of eavesdropping and security rate. In this perspective, wireless networks can greatly improve their resistance to eavesdropping attacks through the adoption of secrecy capacity maximization strategies associated with the appropriate design of artificial noise. These approaches grounded on the information theory give an excellent starting point of establishing secure communication systems that would be resistive to the new threats that are likely to prevail in the wireless environment.

Advanced Techniques for Enhanced Security

With the increased war against wifi eavesdropping, researchers have come up with new strategies to enhance wireless network security. These intrusive techniques encode data using the state of the art technology to ensure the development of the impregnable barriers to any eavesdroppers.

MIMO and Beamforming

MIMO in association with beamforming has been found to be a potent weapon against unlawful invasion of wireless communication. MIMO systems employ simultaneous use of multiple antennas at the transmitter and receiver side to carry multiple streams of data. It also improves the total security of the network at the same time as boosting data through put. Beamforming a technique used to direct the wireless signal in certain directions complements MIMO in enhancing the security of a network. Through the focus of the signal in the direction of the receiver, beamforming Sunday reduces the signal in other directions thus making it difficult for the attackers to jam the transmission. This spatial focusing of energy enhances the quality of the channels for the legitimate users but degrades the quality for the attacker.

Combining beamforming with multiple input multiple output has led to drastic evolution of wireless communication systems with more developed networks being 4G LTE, Wi-Fi and the upcoming 5G networks. These techniques are used in cellular networks for capacity, coverage and user quality improvement especially in developed urban areas and indoors where there is likely to be wire tapping. This is conceptually extended further by the adaptive beamforming algorithms which use feedback from the radio channel to adjust antenna weights and parameters associated with beamforming. This enables the system to have real time optimal transmission and reception while at the same time responding proactively to the menace of eavesdroppers.

Cooperative Jamming Strategies

Cooperative jamming has turned out as a creative strategy in the improvement of physical layer security in wireless systems. In this method, interference signals are purposely injected into the communications channel so as to complicate the operation of unauthorized listeners without at the same time affecting genuine users severely. In a cooperative jamming scenario or in fact genuine jammers, the interferers or the other idle network components put in jamming signals to increase the secrecy capacity of the transmitter-receiver channel. This approach is most suitable in multi- channel wireless communication systems where the power of the jamming signal can be judiciously distributed to the various channels in existence (Figure 3).

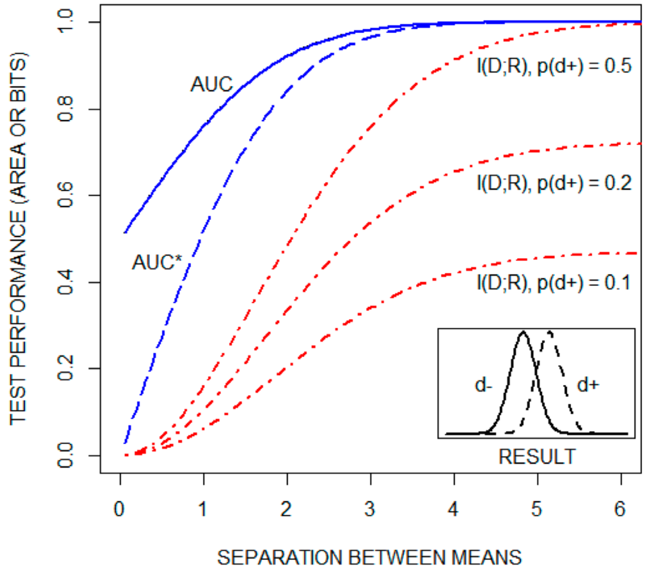

Fig. 3: Cooperative Jamming Strategies

The performance of cooperative jamming is highly sensitive to CSI and the potential eavesdroppers' actions. Consequently, whereas, complete CSI has been used in many works to study the efficient solutions for power control, the recent works admit that perfect estimation of CSI especially for the eavesdropping channels is almost impossible. In order to clarify this, game-theoretic models have been introduced to explain the conflict between friendly interferers and cognitive eavesdroppers. These models assume that the eavesdroppers have the capability of chosing certain channels to attack and hence the defense strategy is not as straightforward as suggested by earlier models.

One such approach uses a non-zero sum Nash game where the friendly interferer (defender) chooses the jamming power allocation plan and the strategic eavesdropper (attacker) chooses the channels to target. This makes it possible to make further improvements in the creation of heuristic and further defended measures against wifi eavesdropping in the frame of game theoretical solutions. It is worth noticing that cooperative jamming strategies are typically used with some degree of trade off between network security and network performance gain. Scholars have deployed mathematical models to identify the proper proportion of the power between intended signals and artificial noise with reference to eavesdropping probability limits and required security levels. Thus, using MIMO; beamforming and cooperative jamming strategies collectively can improve the interference tolerance of wireless networks to eavesdropping attacks substantially. These information theory-based approaches are quite useful in creating the grounds for designing the secure communication systems which could effectively prevent all the changes in the existing threats in the wireless environment and guarantee the private and secure content information transmission.

Real-World Implementation Challenges

Despite the fact that the theoretical concepts to counter wifi eavesdropping based on Shannon's Information Theory are favorable, their implementation faces a number of major challenges. These problems result from several factors like the constraints imposed by the respective hardware, computational problems and weaknesses, and the necessity for unification.

Hardware Limitations

One of the main challenges with the effective application of the anti-wifi eavesdropping security features is the challenge posed by hardware limitations. A lot of devices, especially in the IoT have constrained processing power and/or restricted memory. This makes it rather difficult to apply complicated techniques of protecting information with the help of encryption, or to generate keys using certain standards of information theory. Furthermore, the increase in the number of devices in today's networks including smartphones and smart appliances these devices bring heterogeneity on the level of security measures they can support. General hardware inconsistency may affect the total security of the network by presenting entry points which eavesdroppers can take advantage of.

Computational Complexity

Information theory-based security measures require many computations when being put into use. For instance, quantization for key generation or direct sequence spread spectrum techniques avail much computation power. This can cause higher latency in the transmission of data as is unwelcome in applications where time is of the essence like in disaster recovery management or other real-time applications.

Moreover, some of these enhanced security features require a lot of computations and hence; reducing battery power in mobile & IoT gadgets; thus reduces their feasibility in real-life usage. Balancing security and energy efficiency has therefore been identified as a major research challenge based on the reviewed literature in this area.

Standardization Efforts

The absence of specific best practices for the enforcement of information theory based security measures is also another challenge. The more sophisticated new approaches embedded with Shannon's Information Theory standards are still at their early stages of standardization while the conventional forms of secure internet access protocols such as the WPA3 are already set up. It is worried that it does not have one common model which will enable the devices made by these companies to discuss securely using these methods. It also makes upgrading on existing networks to contain these new security measures slightly more challenging.

However, wireless networks are dynamic, where packet topologies and associations continue to change within the environment of ad hoc and other types of deployments, this leads to some difficulties of standardization and development of security protocols. Further complicating this challenge is the effort to deal with heterogeneous traffic patterns and differing levels of security needed depending on the nature of the associated application and users. As a result, the development of such platforms requires extensive efforts from both hardware manufacturers, software developers and standards organization. This should be done in collaboration with the purpose of providing easily implementable, efficient and generic solutions based on information theory that can be integrated to devices of all types and to various networks.

Conclusion

Using Shannon's Information Theory, there is a new way of addressing the solution to wifi eavesdropping, with the help of the properties of ISM channels. These concepts such as channel state information, reciprocity and randomness of the channel portray the prospect of turning WiFi security all round by this method. This, along with other techniques such as secret key generation and channel based authentication are good starting points to erect a more secure wireless framework. However, when it comes to real-life application, these sophisticated security solutions have their own sets of challenges such as constraints posed by the hardware, high levels of computations involved and the absence of standard formats. To overcome these challenges, regular interaction between the producers of hardware and software, as well as standards bodies is imperative. In future research of this field, WiFi security protocols could be enhanced by the addition of principles in Information Theory to improve the functioning and protection of wireless networks from current and future threats.

References

1. Zhong, Xiaofeng, Chenchen Fan, and Shidong Zhou. "Eavesdropping area for evaluating the security of wireless communications." China Communications 19, no. 3 (2022): 145-157.
2. Zou, Y., Zhu, J., Wang, X. and Leung, V.C., 2015. Improving physical-layer security in wireless communications using diversity techniques. IEEE Network, 29(1), pp.42-48.
3. Zou, Y., Zhu, J., Li, X. and Hanzo, L., 2016. Relay selection for wireless communications against eavesdropping: A security-reliability trade-off perspective. IEEE Network, 30(5), pp.74-79.
4. Zhang, P., Jiang, Y., Lin, C., Fan, Y. and Shen, X., 2010, March. P-coding: secure network coding against eavesdropping attacks. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.
5. Zhang, P., Jiang, Y., Lin, C., Fan, Y. and Shen, X., 2010, March. P-coding: secure network coding against eavesdropping attacks. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.
6. Zhou, H. and El Gamal, A., 2021. Network information theoretic security with omnipresent eavesdropping. IEEE Transactions on Information Theory, 67(12), pp.8280-8299.
7. Xiong, T., Lou, W., Zhang, J. and Tan, H., 2015. MIO: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation. IEEE transactions on information forensics and security, 10(8), pp.1678-1691.
8. Zhang, X. and Wu, W., 2021. Wireless Communication Physical Layer Sensing Antenna Array Construction and Information Security Analysis. Journal of Sensors, 2021(1), p.9007071.
9. Liu, Y., Chen, H.H. and Wang, L., 2016. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. IEEE Communications Surveys & Tutorials, 19(1), pp.347-376.

10. Mukherjee, Amitav, S. Ali A. Fakoorian, Jing Huang, and A. Lee Swindlehurst. "Principles of physical layer security in multiuser wireless networks: A survey." IEEE Communications Surveys & Tutorials 16, no. 3 (2014): 1550-1573.

11. Anjos, G., Castanheira, D., Silva, A., Gameiro, A., Gomes, M. and Vilela, J.P., 2018. Exploiting the reciprocal channel for discrete jamming to secure wireless communications against multiple-antenna eavesdropper. IEEE Access, 6, pp.33410-33420.