Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 3592792, 9 pages
https://doi.org/10.1155/2017/3592792

Research Article

Cognitive Security of Wireless Communication Systems in the Physical Layer

Mustafa Harun Yılmaz,[1] Ertuğrul Güvenkaya,[2] Haji M. Furqan,[3] Selçuk Köse,[4] and Hüseyin Arslan[3,4]

[1]*Institute for Telecommunication Sciences, National Telecommunications & Information Administration, Boulder, CO 80305, USA*
[2]*Maxlinear Inc., Carlsbad, CA, USA*
[3]*School of Engineering and Natural Sciences, Istanbul Medipol University, Beykoz, 34810 İstanbul, Turkey*
[4]*Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA*

Correspondence should be addressed to Mustafa Harun Yılmaz; harunyilmaz62@gmail.com

Received 23 April 2017; Revised 3 October 2017; Accepted 1 November 2017; Published 18 December 2017

Academic Editor: Mohammad Shikh-Bahaei

While the wireless communication systems provide the means of connectivity nearly everywhere and all the time, communication security requires more attention. Even though current efforts provide solutions to specific problems under given circumstances, these methods are neither adaptive nor flexible enough to provide security under the dynamic conditions which make the security breaches an important concern. In this paper, a cognitive security (CS) concept for wireless communication systems in the physical layer is proposed with the aim of providing a comprehensive solution to wireless security problems. The proposed method will enable the comprehensive security to ensure a robust and reliable communication in the existence of adversaries by providing adaptive security solutions in the communication systems by exploiting the physical layer security from different perspective. The adaptiveness relies on the fact that radio adapts its propagation characteristics to satisfy secure communication based on specific conditions which are given as user density, application specific adaptation, and location within CS concept. Thus, instead of providing any type of new security mechanism, it is proposed that radio can take the necessary precautions based on these conditions before the attacks occur. Various access scenarios are investigated to enable the CS while considering these conditions.

1. Introduction

The proliferation of wireless technologies in our daily life leads to an increasing demand for these technologies. While the prevalence of wireless communication systems presents indisputable advantages to the users, due to the open broadcast nature of the wireless signals, the communication exchanges are exposed to the attacks of adversaries. As opposed to its wired counterparts, the enhanced mobility support of the wireless communication systems comes with the handicap of serious security vulnerabilities from the physical layer to the application layer. To protect the wireless signals from malicious attacks, security measures should be provided to the user. In the existing wireless communication systems, security concerns are addressed in the upper layers by means of various encryption techniques. Encryption is achieved in such a way that the message is encrypted with a key generated by using cipher, that is, an encryption algorithm, before the signal is transmitted. The receiver can decrypt the message by using the same key. However, since encryption is a way of protecting the message in the upper layers, it does not prevent the signal from being detected by adversaries in the medium. Additionally, encryption increases the infrastructural overhead and power consumption to enable the authentication, which may not be feasible in some applications such as wireless sensor networks [1]. Data security in wireless domain has to adapt itself to the new wireless communications paradigm by becoming more adaptive and flexible. To this end, implementation of communication security in the physical layer has recently become a field of interest. Existing security threats in the physical layer can be categorized into three groups: eavesdropping,

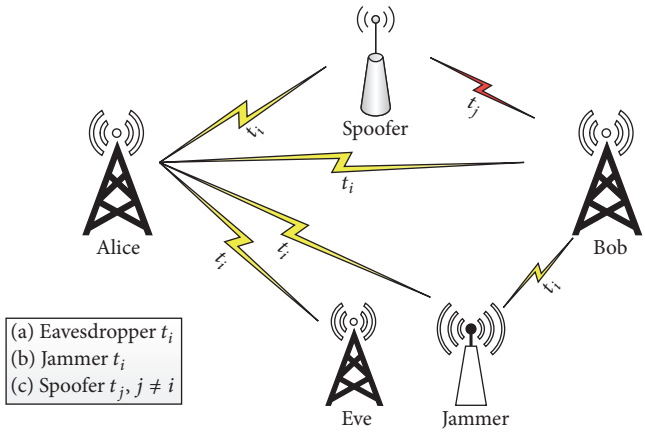

Figure 1: When Alice transmits a message to Bob at time t_i, (a) eavesdropper receives/listens the same message at time t_i, (b) jammer transmits a jamming signal to Bob at time t_i, and (c) spoofer listens to the message at time t_i and then transmits a spoofing message at time t_j where $t_j \neq t_i$.

jamming, and spoofing as depicted in Figure 1. In the physical layer security studies, legitimate transmitter, legitimate receiver, and passive attacker are symbolized, respectively, as Alice, Bob, and Eve. The attacker might be considered as either a jammer or a spoofer if attacker is active.

(1) *Eavesdropping*: when Alice transmits a message to Bob, any receiver can receive the message since the message is propagated through the whole environment. Eavesdropping refers to a situation where Eve can receive the message transmitted by Alice. The message needs to be protected against the eavesdroppers.

(2) *Jamming*: when Alice and Bob are communicating with each other, a jammer transmits a noise type of signal to Bob with the aim of corrupting the communication. When Bob receives both signals at the same time, legitimate signal would be received as meaningless signal. Therefore, the signal would not be decoded. This type of attack is named as jamming. When the attack is held, it needs to be identified by legitimate users, and the signal needs to be protected accordingly.

(3) *Spoofing*: spoofing refers to a situation where the attacker deceives Bob. Spoofing can be carried out in two ways. (a) When Alice stops transmitting the signal, an attacker starts to transmit a deceiving signal to Bob. (b) When Alice transmits the signal, if an attacker transmits deceiving signal with higher power than Alice's signal power, Bob would receive the attacker's signal as legitimate signal while it would consider Alice's signal as interference signal. Similar to the jamming case, this attack needs to be identified and necessary precautions should be taken.

In the literature, studies on physical layer security mainly focus on spread spectrum (SS) techniques and channel and power based solutions. In SS techniques, the energy of the signal is spread over the wider spectrum by means of possessing a wider band. SS techniques are particularly useful against the jamming attacks and eavesdropping. In eavesdropping case, these techniques are used to attain the low probability of interception and detection. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are primary SS techniques used in the literature. FHSS is derived by hopping the signal with a predefined pseudorandom code in the spectrum while in DSSS the energy of the signal is spread over a wide spectrum with a pseudonoise (PN) sequence which keeps the signal power under noise level. As mentioned in [2], these techniques can be utilized to provide security against jamming attacks with certain vulnerabilities. For instance, FHSS technique may be vulnerable against spoofing attacks. To overcome this issue, an antijamming scheme that is based on transmitting a secure identity generated with cryptographic methods is proposed in [3]. Thus, the legitimate transceiver communication can be protected against jamming and spoofing attacks. The drawbacks of DSSS scheme against jammers are investigated in [4]. This drawback is defined in such a way that when PN sequence of jammer is matched with the transmitter's PN sequence, the legitimate receiver can be jammed. To address this drawback, authors propose a watermarked DSSS scheme. In this scheme, an authentication information is embedded to PN sequence to make the system more resistant against jamming attacks.

In channel based solutions, the uniqueness feature of the channel can be utilized to improve security. Since the communication channel between Alice and Bob is different from the channel between Eve and Bob, Alice can perform a secure communication by using its unique channel with Bob. The effects of artificial noise insertion in the presence of Eve are explored in [5]. The primary objective of the artificial noise insertion is to degrade Eve's channel while not affecting Bob's channel. To carry out this aim, Alice adds noise intentionally to the null spaces of Bob's channel. Since Eve does not know the intentional addition of noise, she is not able to detect the signal correctly. Thus, the secure communication would be satisfied even if Eve's channel is not known. Primarily, eavesdropping and spoofing can be prevented with channel based solutions.

In power based solutions, received signal strength (RSS) and directional antenna are used to provide security. RSS is utilized to detect the primary user (PU) emulation attack in [6]. In the cognitive radio network, there are PUs and secondary users (SUs). SUs use the licensed spectrum of PUs. If PU utilizes any bands in its spectrum, SU does not use the same band in order not to cause interference with PU. To determine which bands are utilized by PU, SU can use spectrum sensing algorithm. There might be spoofers in the environment to deceive SUs by masquerading the PU. A verification algorithm to detect the spoofers is proposed in [6] by utilizing the signal characteristics and location of the legitimate transmitter. RSS measurements are performed within a wireless sensor network. All transmitters locations can be estimated by identifying the RSS peaks. In [7], directional antennas are explored against jamming attacks instead of the more conventional omnidirectional

antennas. The connectivity is maintained under jamming attacks with directional antennas. Since there are multiple antennas in Bob, certain antennas can easily be reconfigured towards a direction other than the direction where the jamming signal is coming from. In this case, the transmitter can keep the connectivity with the legitimate receiver with higher data rate when compared to omnidirectional antenna usage case. Wyner introduces the wiretap channels, namely, eavesdropper's channel, in [8]. He aims at rendering the signal meaningless taken by wire-tapper. To achieve this, Wyner utilizes signal-to-noise ratio (SNR) differences observed at Bob and Eve. If Eve's SNR is lower than Bob's SNR, Alice can initiate a secret communication with Bob without any information leakage to Eve via encoding.

While the aforementioned studies provide a security only in the physical layer, the security in cross-layer is investigated in the following studies. The requirements and benefits of cross-layer security are presented for wireless sensor network (WSN) in [9]. As explained in [9], cross-layer design should work collaboratively to detect the adversaries while enabling the efficient power consumption. The cross-layer utilization by means of the intrusion detection is proposed in [10]. It is proved that security which is obtained by exploiting the data coming from different layers such as link and network layers is increased significantly when compared to the single layered security solutions in terms of true positive rates.

Besides the studies focusing on the specific security issue, in a few studies, the physical layer security literature is surveyed. In each of these papers, authors examine the security studies from different perspectives. In [11, 12], and from a bigger picture in [13, 14], authors investigate the security in cognitive networks. While authors in [15] explain the security issues in health care domain, authors in [16] look at these issues in smart grid applications.

2. Motivation

Although existing efforts satisfy the security needs of the users under certain conditions and for specific wireless communications systems, they might fail in others. For instance, since channel based solutions have complete dependency on channel conditions, while these solutions would work when legitimate transceiver is static and has reciprocal channel, these solutions would fail when the legitimate transceiver is either mobile or performs communication based on frequency division duplexing. Alternatively, SS techniques can be employed to protect data against jamming attacks and eavesdropping. When there is a spoofer in the environment, if an additional protection algorithm as given in [3] is not proposed, SS technique would fail. Moreover, using an additional algorithm would increase the complexity of the legitimate transceiver. Another issue with SS techniques is related to PN or hopping sequence sharing. When a legitimate transmitter sends PN or a hopping sequence to a legitimate receiver, if the sequence is not protected, an illegitimate node can capture this secret information. Therefore, illegitimate node can easily eavesdrop, jam, or spoof the legitimate receiver. As explained in Section 1, localization can be performed with power based solutions. In RSS based localization, it is assumed that illegitimate node uses omnidirectional antennas and multiple receivers measure the RSS of this node to be able to perform true localization. If illegitimate node employs the directional antenna, localization would fail [17]. On the other hand, since the location of eavesdropper is unknown, power based solutions cannot provide security against eavesdroppers either.

All of these weaknesses of the existing solutions indicate the necessity that the security threats need to be investigated with more comprehensive solutions in the physical layer. In this study, we propose cognitive security (CS) concept which provides adaptive security solutions in the communication systems by exploiting the physical layer security from different perspective. The adaptiveness relies on the fact that radio adapts its propagation characteristics to satisfy secure communication based on specific conditions. In this paper, the conditions are defined as the user density, application specific adaptation, and location. Please note that, in the existing efforts, security is provided when the legitimate transceiver is under attack(s). However, the security is performed in CS concept before the attack occurs. In other words, CS proposes that the necessary precautions are required to be taken before the attack takes place based on the conditions which are explained in detail in the subsequent sections. Thus, the systems would adjust the propagation parameters of the radio against possible threats. With the given conditions, CS should

(i) Increase the reliability in the wireless communication systems: since transceiver would be able to adjust the security level, increasing the security adaptively will increase the overall reliability of the communication system automatically. Especially, when a receiver is under jamming attack, one of the most important problems is to satisfy reliable communication to guarantee the quality of service requirement. CS would play an important role in this situation.

(ii) Decrease the system complexity: the active attackers need to be detected in current security mechanisms. This requires additional algorithms to be implemented in the systems. Since, in CS concept, detecting the attackers is not necessitated, this would reduce the complexity caused by the usage of the additional algorithms.

Along with these advantages, CS should also

(i) Increase the data rate: the radio resources allocated for providing secure communication can be reduced for the cases which do not necessitate high level of security due to low probability of threat. For instance, if the security is based on the location, let us say, in rural areas, security level is lowered when compared to urban areas. Since some resources which are allocated to provide security would remain empty, these resources will be used for data communication. Thus, the users who live in rural areas would have higher data rates.

(ii) Decrease the energy consumption: it is important to lower the consumed energy in the systems during the communication, for example, in mobile devices. If

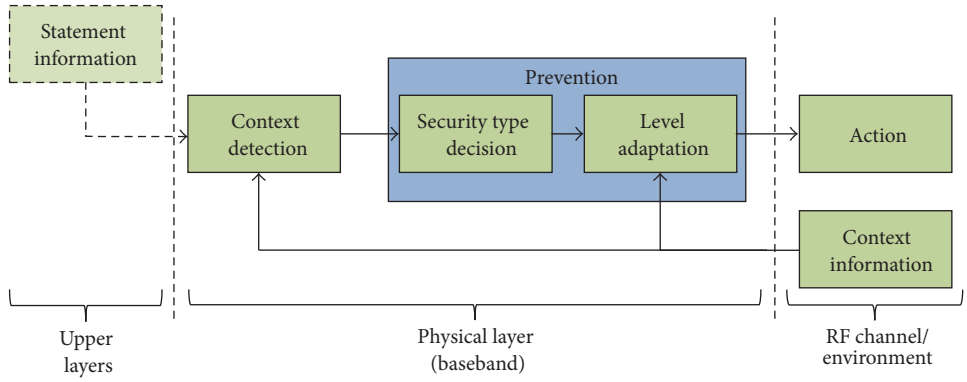

Figure 2: System model for cognitive security.

security level is lowered in uplink, the mobile device would be able to transmit the same amount of data in less duration since the data rate would be higher.

3. Cognitive Security Concepts

The system model for cognitive physical layer security is illustrated in Figure 2. The radio combines the relevant information obtained from the radio channel and environment. Based on the available knowledge, the context is detected. To improve the detection performance, the statement information can be attained from the upper layers. After an associated security mechanism is determined by the radio, the level of the security can be adjusted as a function of the intensity of threat.

In this study, we define three the CS concepts: user density, application specific adaptation, and location.

3.1. User Density. User density refers to a number of users per unit area. If the number of users is high in a given area when compared to a predetermined normal, for example, schools and hospitals, it can be stated that the area has high density in terms of the number of users and named as high user density through the rest of the paper. From the security perspective, high user density is an important parameter, especially for CS concept. As mentioned in Section 1, there are three threat groups in physical layer security studies. The radio can act intelligently to provide secure communication in spite of the fact that these three groups are probable to occur related to the user density. For specific places such as hospitals, office blocks, and airports, security is highly important. Jammers, eavesdroppers, or spoofers are expected to exist in such places as shown in Figure 3. In [18], authors define the probability of eavesdropping (or attacking) in a given area A.

$$P(e) = 1 - e^{-\rho A}, \tag{1}$$

where ρ is the node density. For a given area, when the node density increases, probability of eavesdropping increases as well.

Density is the detectable data by the radio. In a high user dense area, since most of the resources would be occupied by the users, the detection of the density can be achieved by observing the total number of allocated resources at a time. When high density is detected, attackers would aim to affect the communication in between legitimate users, for instance, between a patient and a doctor in the hospital. Implantable medical devices (IMDs) such as defibrillators and peacemakers are implanted within the patient's body and are monitored and controlled by the physician with the help of external unit wirelessly. This wireless nature will make the IMDs vulnerable to attacks which might disrupt the communication by jamming or sending wrong information to the legitimate receiver by spoofing. In both cases, if the patient is in a critical condition and needs an emergent treatment, since the doctor will not be able to know the patient's situation because of jamming or spoofing, s/he will not treat his/her patient. The result might therefore be fatal for the patient. In this case, to be immune to attacks, the radio might increase the security. If the high user density stems from the office block, legitimate users might be eavesdropped on. The aim of the eavesdropper is to capture the company's critical information. Another important issue is that there might be many jammers, eavesdroppers, or spoofers who work collaboratively in high user dense areas. The security can possibly be improved significantly by adaptively adjusting the propagation parameters of the radio.

There might be various reasons for users to gather in a given area such as stadium, hospital, school, or airport. Since it is not possible for a radio to detect the reason of users' gathering, the necessary information can be obtained from the upper layers. For instance, if the users in the high dense area send important documents, this can be detected by the upper layers and this information is provided to radio. Based on this notice, radio can consider that the density stems from the employees who work in an office block. This type of security approach is named as cross-layer security in the literature [9]. As defined in Section 2, one of the key advantages of CS is to increase the data rate. If a holistic approach is not considered, data rate might be decreased unnecessarily in some cases. For instance, assume that the security should be higher in office blocks than the security in stadiums. Since radio does not have the reason of users' gathering, it would increase the security to the same level in all high user dense areas. This may not be desirable for

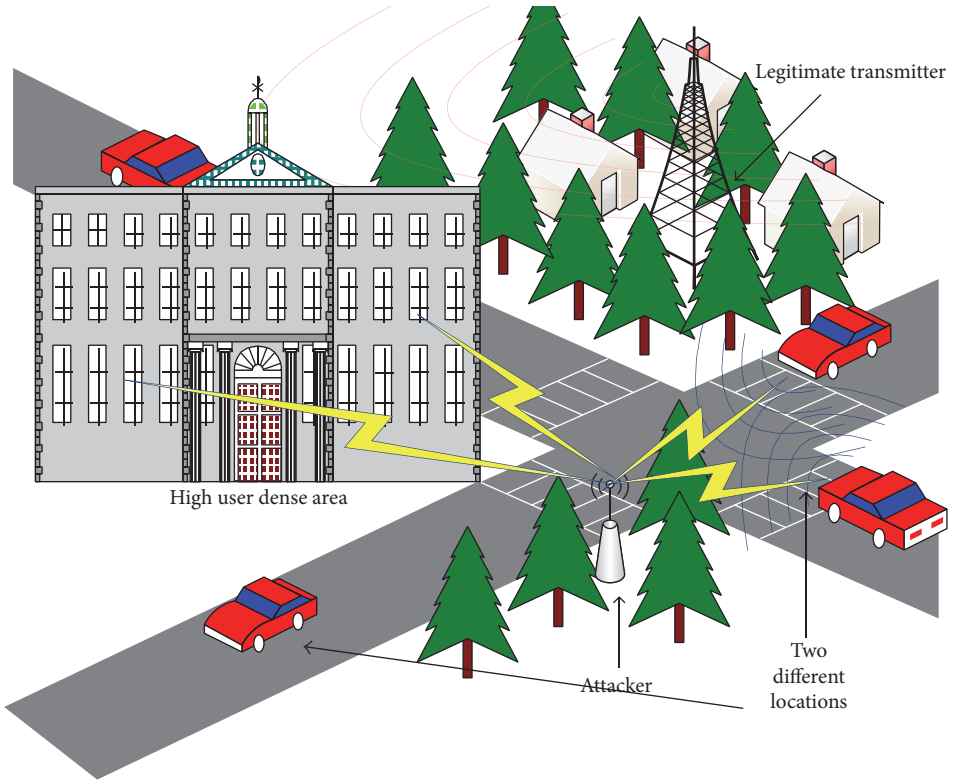

Figure 3: Attackers would appear in the user dense areas. Also, they are more likely to jam or spoof the vehicular communication in the intersections.

every situation. For the same amount of user data, high secure communication might necessitate more resources to be allocated than less secure communication. Therefore, data rate in the relevant dense area would decrease. When the density in question occurs in the stadiums, data rate would become more critical. The security level in the stadium should not be the same as the one in the office blocks. This situation can be considered as the probability of error in the increment level of security.

3.2. Application Specific Adaptation. Application specific refers to different fields such as military, commercial, and health monitoring in which the radio is used. Communication is typically held wirelessly in these fields. To minimize or alleviate the interference, different frequency bands are allocated for each field. These different bands carry significant context information for the radio. This helps the radio to detect the type of application for which the communication is being fulfilled.

Each application has different security requirement. While it is high for military communication, it might be low for commercial applications, such as for cellular communication. Ensuring secure communication requires more resources to be allocated and a higher data rate is vital for commercial sector. Allocating as many resources as in military communication for security reasons to carry out the communication may therefore not be feasible in commercial domain. In any case, communication needs to be provided securely when the transceiver is under attacks. Existing security threats would differ based on time and place where the communication is being held for each application. For instance, when the country is in peace, passive attacks like eavesdropping would be significant for military communication. But, if there is an emergency situation such as a battle, jamming and spoofing are going to be very serious issues as well. In these types of situations, security needs to be adjusted accordingly. The existing algorithms which are proposed to protect the data from eavesdroppers may not provide the security in jamming or spoofing scenarios as mentioned in Section 2. This indicates that securing the communication against each type of attacks necessitates different solutions. In any emergency situation, military may need to reach out to the public across the country or may need additional resources for the communication. To meet this demand, military has to utilize certain ubiquitous structures such as cellular base stations and broadcasting antennas. Although security level might be lower in cellular communication when compared to military, when the emergency situations occur, radio should be able to detect it and adapt itself to new situations. Since the cellular or broadcasting structure is not suitable to implement the same security methods, the radio should provide more secure communication via the physical layer security mechanisms. Herein, military would protect its communication against jamming or spoofing attacks. If

the security level depends on the application, it needs to be adaptively managed.

Another important application is the Internet of things (IoT) for future wireless networks. Various types of technologies such as implantable medical devices (IMDs), WSN, and autonomous vehicles will share the bands in IoT. These different technologies may require different level of security. For instance, while it is critical to provide high security for IMD, it may need less security in smart home applications such as controlling the refrigerator over the Internet. Therefore, CS will play an important role in 5G and beyond networks in terms of providing and adjusting necessary security and data rate needs for each application.

3.3. Location. Specific location or social environment where the communication is fulfilled is an important parameter for CS concept. For some devices such as unmanned aerial vehicles (UAVs), the location information is required to find their geographical position. Therefore, it is important to provide security against attacks based on the location information. It can be said that there is a high correlation between the type of the security threats and the location. For instance, for vehicle-to-vehicle (V2V) communication, location determines the type of the communication between vehicles. When two vehicles go back-to-back on the road, the communication is performed to maintain a minimum distance between vehicles, namely, space cushion, through the sensors at all times to not cause an accident. Alternatively, when two vehicles encounter an intersection where there is a significant decision-making process, the type of the communication would be different. One issue is the order of the vehicles to cross the intersection [19]. While this example highlights the importance of the location in terms of the type of the V2V communication, this location information is also critical to satisfy the secure communication between vehicles. The two vehicles at the intersection point need to talk to each other while simultaneously monitoring the measurement of the sensors to detect any possible rear vehicle. This may lead to some security gaps to attack the vehicles that are at the intersection point as depicted in Figure 3. In this situation, there are two possible security issues: jamming and spoofing. An attacker may destroy the communication of the vehicles or may send the same message to two vehicles such as the priority of who would pass first. Both situations would eventually cause an accident. The security level can be significantly increased if the radio is able to detect the location. Thus, the accident may be precluded.

In terms of social environment, three types of environments can be considered: rural, suburban, and urban areas. The main difference between the environment types is the population density. At this point, it is important to emphasize that the social environment should not be confused with user density in terms of the detectability. As mentioned above, user density definition covers a small area such as stadiums and schools, and it can be within urban, suburban, and rural areas. However, environment covers the whole urban, suburban, or rural area by definition.

In wireless communication, environment information is important in terms of the capacity. For instance, to increase the capacity, various deployment strategies of the base stations (BSs) are applied. While the BSs whose coverage area is as high as 1-2 km might be sufficient to serve for the users in rural areas, the small BSs whose coverage area is around 10–200 m would need to be deployed in urban areas to meet the users' demands. To provide a secure communication, environment is a significant parameter. Based on the environment type, security need would differ, especially in the public safety context. The crime rates are much higher in urban areas. For example, 39 crimes are recorded per 1,000 residents in rural areas while 79 crimes are reported in urban areas in England [20]. To decrease the crime rate, governments need to take necessary preventions. When a crime or an emergency situation occurs, each unit of the system, for example, mobile devices and networks, should work coordinately and securely so that the relevant government agent can act promptly. If the system is under jamming or spoofing attacks, the communication might be disrupted. Therefore, a high security level should be provided for each unit. Since, most of the time, this is the case for the urban areas, radio should adaptively increase the security based on the environmental information for the wireless systems. In conclusion, the type of environment also determines the level of security rather than just the security itself.

Figure 4 shows the relation between security needs and type of environment in terms of probability of attacks. This figure is drawn, that is, not based on simulation, to only help readers to visualize this relation. The probability of attack increases in the urban areas when compared to rural areas. It is also visualized that the increasing probability of attack increases the usage of resources for security reasons, which also leads to decreasing data rate.

Another importance of the location information is related to the devices which have dependency on accurate geographical position such as UAVs. While UAVs can be controlled from a ground station, they can also have preinstalled location and mission information and perform duty automatically. In both cases, UAVs necessitate location information obtained from global positioning system (GPS) satellites. Attackers would intend to disrupt the communication between UAV and GPS satellite.

Please note that UAVs are used for different purposes in different areas. While they are used for policing in public safety, they are also utilized in scientific researches, for disaster relief, and in armed attacks. Each type of usage may require the security in different levels in terms of localization. While the low level of security might be enough to provide communication in disastrous relief cases with the aim of obtaining high data rate, high level of security would be necessary in armed attacks. On the other hand, when the country is in battle, UAVs used for other purposes such as for commercial usage can also be utilized to defend the country against the enemies. Since the enemies' aim would be to disrupt or spoof the communication between UAVs and GPS satellites, UAVs would need to increase the security accordingly to not be harmed or controlled by the enemies.

As highlighted above, the aim in this study is to take the necessary precautions based on some conditions; any type of

Table 1: Advantages of cognitive security concept against security threats.

Security threats	Explanation of cognitive security conditions	Benefits
Eavesdropping	(i) Increase the secrecy rate (versus information rate) in scenarios of high user dense areas such as office blocks and airports or locations such as urban areas or specific applications such as military and public safety (ii) Relax the secrecy constraints, that is, increase the information rate, for conditions such as rural areas, WiFi, and cellular communication	Data rate Latency Energy consumption
Jamming	The level of security against jamming, for example, processing gain in spread spectrum, is adaptively increased in locations such as intersections of roads or specific applications such as military and public safety	Reliability Complexity Latency
Spoofing	Enable the spoofing detection mechanism when the condition exists, and disable the algorithm, or use a simpler method, in high user dense areas such as office blocks, stadiums, or locations such as intersections of roads and location dependent UAV devices, or specific applications such as military and in vivo communication	Complexity Reliability

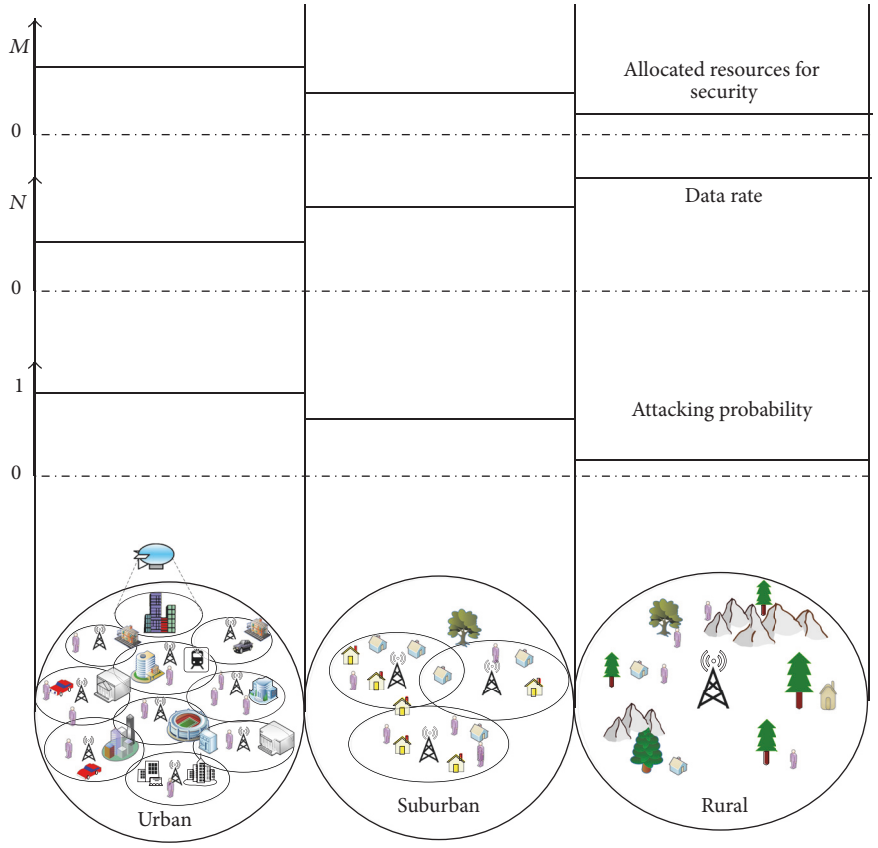

Figure 4: Based on the environment information, security needs can change. While the probability of attack might be higher in urban areas, it might be low in rural areas. The increased probability of attack increases also the resource usage to provide higher security, which also leads to decreased data rate.

new security mechanism is therefore not proposed within CS concept. Instead, three different conditions are given to help radio to determine if the security is a need or not. In Table 1, the benefits of the CS concept related to security threats are enlisted. After the security need occurs, any current security solution can be utilized. At this point, it is worth mentioning that the CS should not be confused with context-aware security concept. In context-aware security, the information is mainly obtained by different sensors. Based on the these information, the system in upper layers tries to detect if there is an attack. If so, then, the necessary security algorithm is placed. In other words, the focus in context-aware security is

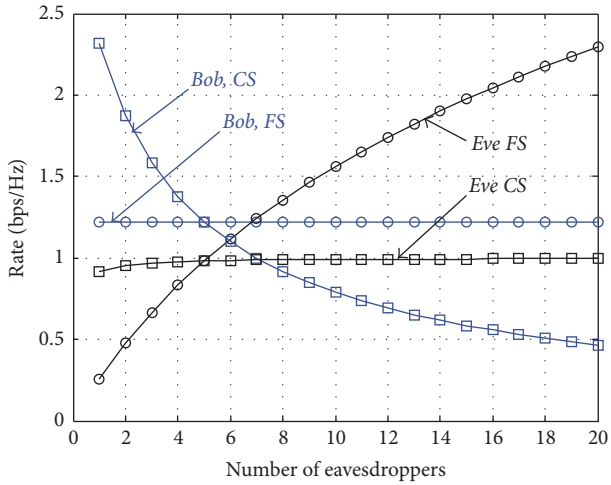

Figure 5: When the number of eavesdroppers increases in a given area, while the rate of Bob remains constant in the FS case, it is decreasing in CS. However, in terms of the security, CS provides higher security than FS case.

on providing the necessary security when it is a need based on the context information like temperature, speed, and so on [21] as in conventional approaches in the security studies [13, 14]. In CS, the security need is determined based on the conditions regardless of the attack that occurs.

In Figure 5, we compare the CS with fixed security (FS), in which the security level is the same for any conditions, for the user density case in terms of rate versus the number of eavesdropper. The rate is computed as Rate $= \sum_i \log_2(1 + \mathrm{SNR}_i)$, where i is the antenna index. As given in (1), when the user density increases in a given area, the probability of eavesdropping also increases. Based on (1), we realize this increment as the increasing number of eavesdroppers in the figure. We assume that Alice transmits the signal to Bob from multiple antennas and there are multiple eavesdroppers working collaboratively. We assume that the transmitter utilizes multiple antennas with artificial noise to provide security during communication with Bob. Invoking that the signal transmitted by multiple antennas can be considered as multidimensional signal, one of these dimensions is allocated for the data transmission to Bob while the remaining ones are used for the artificial noise transmission. In FS case, we assume that the number of transmit antennas of Alice is fixed. In this case, when the number of eavesdroppers increases, Eve's rate will also increase. Since only fixed number of antennas is used to send artificial noise signal, the desired security will be achieved only for the cases where the number of eavesdroppers is less than the number of dimensions allocated for the artificial noise at the transmitter. Therefore, the sum rate of the eavesdroppers will increase by increasing the number of collaborating malicious nodes. For this case, the rate of Bob will remain constant. In CS case, the number of transmit dimensions for the artificial noise of Alice changes with the number of eavesdroppers in the environment. While the security level of eavesdropper stays the same because of having constant rate, Alice's rate decreases. It is because the total transmit power of Alice is fixed and shared between the data and artificial noise signals.

4. Conclusion and Open Issues

Providing security in wireless communication is a critical task. In this paper, we focused on the security in physical layer where we proposed CS concept. Radio can adapt its security level in CS by considering three different conditions which are defined as user density, application specific adaptation, and location. These conditions come along with certain challenges which can be listed as follows.

4.1. How to Detect If the Condition Exists? To make the security adaptive, ensuring the detectability of context information is critical. While some of the context information such as user density is easy to detect via available spectrum sensing techniques [22], for some of them such as application specific, it is a hard task. As explained in Section 3.2, when the country is in battle and the military needs to use the cellular stations and frequencies for the communication, radio should have the capability to increase the security. Here, the question arises as to how the radio realizes that condition. If there is a need to obtain some parameters from the upper layers to detect the context information, how should radio collaborate with those layers? Collaboration between the layers is also a subject of cross-layer techniques [9].

4.2. How to Identify the Correct Statement about the Context? As mentioned in Section 3.1, detailed knowledge might be needed to adapt the security level after detecting the existence of context information. For instance, the reason of users' gathering can be an entertainment event which might not necessitate a high security level while it can be required in business environments. How one can differentiate the statement of the context emerges as a hot topic.

4.3. What Type of Security Mechanism Can Be Used and How Many Resources Should Radio Allocate? There are many studies to secure the communication in physical layer most of which focus on specific circumstances. Especially, after detecting the context information and identifying the correct statement, the third step is: "Other than current efforts, what type of security mechanisms should be performed depending on the information captured from the environment and upper layers?" Will this new method provide higher security than the existing efforts? For which context will it be a remedy? Regardless of whether a new method is proposed or any existing solution is used, how is the security level adjusted? For instance, based on the security threat, the waveform can be determined in the physical layer. If there is a jamming attack, spread spectrum waveform can be utilized. In this case, the security level can be considered as the processing gain, that is, the amount of spreading. As a final note, the adaptation ability of a specific technique to change the security needs should also be considered. For instance, transmit power can be a limiting factor for some users which might restrict the flexibility of the security level in artificial noise insertion based techniques. Alternatively, in SS, total

available bandwidth needs to be considered while performing the adaptation.

In this study, we provided different conditions which necessitate CS. However, it is highlighted that various new context information can be integrated into CS concept by taking the dynamic nature of the wireless communication systems.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This paper is partially supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant no. 114E244.

References

[1] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in *Proceedings of the 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON*, pp. 193–202, San Diego, Calif, USA, June 2007.

[2] 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 Magazine*, vol. 18, no. 2, pp. 66–74, 2011.

[3] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping. Part I. System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, 2013.

[4] X. Li, C. Yu, M. Hizlan, W.-T. Kim, and S. Park, "Physical layer watermarking of direct sequence spread spectrum signals," in *Proceedings of the 2013 IEEE Military Communications Conference, MILCOM 2013*, pp. 476–481, San Diego, Calif, USA, November 2013.

[5] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of the 62nd Vehicular Technology Conference, VTC 2005*, pp. 1906–1910, Dallas, Tex, USA, September 2005.

[6] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[7] G. Noubir, "On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility," in *Wired/Wireless Internet Communications*, vol. 2957 of *Lecture Notes in Computer Science*, pp. 186–200, Springer Berlin Heidelberg, Berlin, Germany, 2004.

[8] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] M. Xiao, X. Wang, and G. Yang, "Cross-layer design for the security of wireless sensor networks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation, WCICA 2006*, pp. 104–108, China, June 2006.

[10] G. Thamilarasu and R. Sridhar, "Exploring cross-layer techniques for security: Challenges and opportunities in wireless networks," in *Proceedings of the Military Communications Conference, MILCOM 2007*, Orlando, Fla, USA, October 2007.

[11] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, 2013.

[12] J. L. Burbank, "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008*, Singapore, May 2008.

[13] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1691–1708, 2012.

[14] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Gódor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2012.

[15] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: a survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[16] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 46–52, 2012.

[17] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *Proceedings of the 32nd IEEE Conference on Computer Communications, IEEE INFOCOM 2013*, pp. 2778–2786, Italy, April 2013.

[18] H.-N. Dai, Q. Wang, D. Li, and R. C.-W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 760834, 13 pages, 2013.

[19] V. Milanés, J. Pérez, E. Onieva, and C. González, "Controller for Urban intersections based on wireless communications and fuzzy logic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 11, no. 1, pp. 243–248, 2010.

[20] T. Pateman, "Rural and urban areas: comparing lives using rural/urban classifications," *Regional Trends*, vol. 43, no. 1, pp. 11–86, 2011.

[21] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 212–226, 2014.

[22] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.