The Challenges Facing Physical Layer Security

Wade Trappe

ABSTRACT

There has recently been significant interest in applying the principles of information-theoretical security and signal processing to secure physical layer systems. Although the community has made progress in understanding how the physical layer can support confidentiality and authentication, it is important to realize that there are many important issues that must be addressed if physical layer security is ever to be adopted by real and practical security systems. In this article, I briefly review several different flavors of physical layer security (at least for wireless systems), and then identify aspects (a.k.a. weaknesses) where the foundation for physical layer security needs to be strengthened. I then highlight that the opportunities for applying physical layer security to real systems will be quite rich if the community can overcome these challenges. In the course of the article, I note new directions for the community to investigate, with the objective of keeping physical layer security research targeted at having a practical impact on real systems.

INTRODUCTION

Physical layer security has become an emerging hot topic in wireless systems.[1] At the heart of this enthusiasm is the belief that the physical layer represents a previously untapped resource for enhancing wireless security. In particular, rather than rely solely upon generic higher-layer cryptographic mechanisms, as has been the norm, there is a belief that it is possible to design lower-layer services that support security objectives such as authentication and confidentiality. There are several good surveys and collections that explore the fundamentals of physical layer security [1–3], but briefly these services can be summarized as follows.

AUTHENTICATION/IDENTIFICATION SERVICES

Rather than employ a shared cryptographic authentication key between Alice and Bob, we instead exploit the uniqueness of the Alice-Bob channel relative to the Eve-Bob channel. The uniqueness of the channel between two locations provides a means of uniquely identifying wireless entities [4] or detecting an entity claiming multiple identities [5]. Devices may authenticate themselves based on their ability to produce an appropriate received signal at the recipient.

CONFIDENTIALITY

Confidentiality at the physical layer can generally be broken down into two different classes: dissemination methods that secretly convey information using the properties of the wireless medium, and extraction methods that seek to build secret information from the wireless channel's characteristics. Roughly speaking, for *dissemination* methods, researchers have shown that it is possible to secretly communicate if one can devise ways to ensure that the wireless channel between the correct transmitter and receiver is better than the channel to any illegitimate receiver. *Extraction* methods, which are philosophically similar to authentication methods, seek to use the unique space, time, and frequency characteristics of the wireless channel as the source of shared secret information (e.g., a key) between a transmitter and a receiver.

With all of the excitement surrounding physical layer security, I believe it is important to revisit the intent behind this research area and whether we, as a community, are on track to developing tools that will engender the trust needed for their adoption. Physical layer security is intended to secure real systems, and thus I think we should examine what we can do as a community to ensure that our methods will be warmly received by the broader security community. The purpose behind this critique is to present my opinions as a researcher and pragmatist who has conducted theoretical and systems research in physical layer security, and in doing so help steer the physical layer security community to high-impact topics that will ensure that our research will be integrated into real wireless systems.

BEING CRITICAL: WHAT ARE THE HURDLES?

When considering the hurdles facing physical layer security, it is natural to consider each type of physical layer security separately (authentication, secret dissemination, and key establishment). A quick analysis, however, will reveal that

The author is with Rutgers University.

[1] It must be recognized that there has been recent work in physical layer security for optical systems, but the focus of this discussion is on wireless systems.

0163-6804/15/$25.00 © 2015 IEEE

there will be significant overlap between the challenges that each of these different flavors of physical layer security will face. Therefore, the approach I have taken is to identify the fundamental assumptions on which these different flavors of physical layer security are built, and the potential hurdles that could prevent physical layer security from succeeding. Loosely, I would break these down into assumptions regarding the adversary and assumptions regarding the nature of the wireless channel, recognizing that weaknesses in our assumptions about the wireless channel would naturally be exploited by a clever adversary. Finally, there are practical matters that warrant investigation.

Hurdles from the Adversary Model

The adversary model used in physical layer security tends to be different than what is employed by the security and cryptography community. Consequently, bridging the gap between the different adversary models used by the different communities is perhaps the most important hurdle facing physical layer security. To many in the traditional security community, our models are perceived as weak, and below I elaborate on several aspects related to our adversary models that can be explored as a means to make our work more readily accepted by the broader security community.

The Adversary Is Passive: Many, although certainly not all, formulations assume that the adversary merely eavesdrops on communications. In classical cryptography parlance, such an adversary is a *ciphertext only* adversary. Many of the physical layer key establishment schemes assume that the adversary is merely monitoring the key establishment process and not actively injecting pilot symbols or imitating bit reconciliation messages. Furthermore, we rarely see active attacks like *replay attacks* employed against protocols involving physical layer security. Understanding the implications of an adversary being actively engaged in undermining the protocol will be paramount to getting physical layer security accepted. Modern cryptography recognizes that adversaries may cleverly set up *oracles* that support their cryptanalysis and attempt to undermine the system security. Chosen message attacks (e.g., chosen plaintext, chosen ciphertext, and adaptive versions thereof) are the well accepted starting point for analyzing security tools. As a community, we need to adopt a wider array of adversary modes in which the adversary is more active and, frankly, more clever.

The Adversary Does Not Have Many Observations: Many physical layer security approaches assume an Alice-Bob-Eve model where Eve makes a limited set of observations (e.g., at one extreme, Eve might be a single entity that exists at a single location). For secret dissemination methods, for example, the challenge is that if Eve is a distributed adversary and obtains multiple (say M) independent observations of Alice $\rightarrow$ Bob's single communication, the probability that one of these M channels is better than the Alice $\rightarrow$ Bob channels goes up. Furthermore, Eve could employ collaborative processing, and then the probability that Eve's (combined) effective channel is better than Bob's would go up quite rapidly — in fact, a collaborative adversary with merely a linear factor more observations than Bob can effectively make the secrecy rate 0. The community needs tools to counteract the challenge of adversarial resource advantages, and there has been promising work in leveraging feedback to overcome an adversary with multiple observations [6, 7]. Work needs to be done to ensure that such feedback mechanisms are themselves robust to adversarial manipulation and even impersonation attacks. I feel it is also worth mentioning two aspects of the Dolev-Yao model, which is frequently referred to in the security community: that there are adversaries anywhere they want to be in the network, and that these adversaries may eavesdrop, manipulate, inject, alter, duplicate, and reroute as befits their purpose. While the notion of an omnipresent adversary makes no sense in the context of physical layer security, we must nonetheless strive to strengthen our adversarial considerations in terms of where they are located in the system.

Beyond secrecy dissemination, one should consider how multiple adversaries would impact other forms of physical layer security. For methods that leverage the channel for authentication or key establishment, it must be recognized that the decorrelative properties of the channel are not absolute, and consequently, many observers located simultaneously near Alice and/or Bob may be able to collaboratively estimate the Alice-Bob channel. Understanding the implications of collusion or collaboration on physical layer security will be important to solidify the adversary model.

The Adversary Is Not Powerful: Often one hears a researcher say something along the lines of "physical layer security is based on information-theoretic security, and hence, no matter how much (computing) resources the adversary has, he will not be able to break our scheme." I would certainly agree that a considerable amount of research in physical layer security calls on information-theoretic tools. However, I would not agree that we are operating in the spirit behind information-theoretic security, which is a tool that has been successfully applied to many security problems outside of physical layer security, such as multicast security and key management. Information-theoretic secrecy uses impressive phrases like *perfect* secrecy, which suggest invincibility to resources employed by the adversary, and certainly in Shannon's original theory for secret communications the adversary is assumed to have unlimited computational resources. However, if I were an adversary challenging physical layer security, rather than put my money into buying computation, I would put my money elsewhere, such as buying better antennas. Modern cryptography and security is founded on the notion of an efficiency gap between legitimate users and illegitimate users, or, to put it another way, we expect the adversary to need greater than a polynomial amount of resources (computing, storage, money, or whatever) compared to legitimate parties. We often assume Eve has the same antennas and thus antenna gains as Alice and Bob, and this is worrisome. In fact, Eve's

The adversary model used in physical layer security tends to be different than what is employed by the security and cryptography community. Consequently, bridging the gap between the different adversary models used by the different communities is perhaps the most important hurdle facing physical layer security.

A slightly more sophisticated adversary might be able to employ ray-tracing methods to predict the channel, and an important question to explore is how much the secret key rate is affected by an adversary's ability to perform ray-tracing.

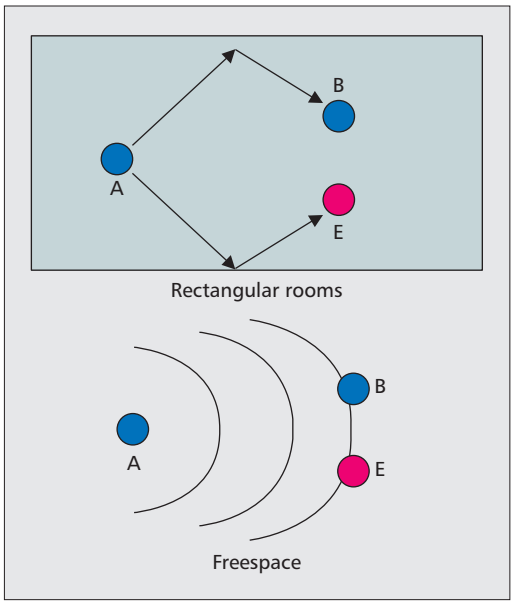

Figure 1. Symmetries inherent in the environmental geometry could pose potential weaknesses to physical layer authentication and key establishment. Two extreme examples include a rectangular room and freespace propagation.

gain is directly related to the aperture of her antenna, which is proportional to its physical aperture; hence, all Eve needs to overcome Alice-Bob is to devote more *area* to listening. Loosely speaking, this means that Eve's resources need only be quadratic in Alice-Bob's resources in order to have a competitive chance at undermining Alice-Bob's secret communication. But to put things in practical terms, a quick survey of antenna gains vs. cost finds gains ranging from 7 dBi to 20 dBi for anywhere between $25 to $200. I would thus suggest the following question: Can a non-nation-state Alice and Bob ever hope to overcome a nation-state Eve?

Hurdles from the Wireless Channel

The Channel Is Difficult for an Adversary to Predict: The security strength for both physical layer authentication and physical layer key establishment is intimately tied to the basic assumption that it is hard for an adversary to estimate or predict the channel. The literature is filled with references to the wide-sense stationary with uncorrelated scatterers (WSSUS) channel assumption and Jakes's well-known uniform scattering model to declare that a received signal rapidly decorrelates over a distance of roughly half a wavelength, and consequently that spatial separation of one to two wavelengths is sufficient for assuming independent fading paths. This decorrelative property is used as the basis to conclude that it is hard for an adversary to estimate the channel that Alice and Bob experience.[2] In actuality, there are several problems with this assumption that warrant discussion. First is quantifying when we are in a sufficiently rich scattering environment. Alice and Bob need to verifiably assess that they are in a richly scattering environment before commencing with physical layer key establishment (or authentication). It must be realized that simple environments are the bane of physical layer security. Two examples bring the severity of this problem to light: freespace and a simple rectangular room (Fig. 1). In freespace, if Bob and Eve are the same distance from Alice, they will experience the same propagation phenomena (notably, just path loss). While in a rectangular room, it is possible to construct benign scenarios where the Alice-Bob channel is the same as the Alice-Eve channel. The community is already examining questions related to the security of the propagation assumption, such as [9], and I expect that the community will continue to find cases where poor environmental scattering undermines the security of key extraction and physical layer authentication.

A slightly more sophisticated adversary might be able to employ ray-tracing methods to predict the channel, and an important question to explore is how much the secret key rate is affected by an adversary's ability to perform ray-tracing. Related to this is the interesting question of how complex the descriptive model for the environment must be in order to undermine physical layer security. I would note that ray-tracing has been used to validate physical layer authentication methods, and there is an amusing paradox here. The very tool used to validate physical layer authentication could also be employed by the adversary to undermine physical layer authentication: Eve could use the same ray-tracing to identify promising locations within a building to conduct spoofing attacks against Alice-Bob. Certainly, this is a matter of concern since many building blueprints are in the public domain, thereby facilitating ray-tracing analysis by an adversary. Developing tools that can estimate an environment's "propagation" complexity in real time will be an important practical tool for supporting physical layer security. Of course, this begs the fundamental question of what the right notion of environmental channel complexity is for physical layer security. It is quite unlikely that the notions of delay spread and the K-factor will carry the appropriate properties needed for physical layer security.

The Channel Needs to Be Dynamic: A similar concern arises when one considers the radio environment temporally; a completely static environment where the scatterers do not move also poses several concerns. Temporal decorrelation of the channel plays a significant role in the non-reciprocity of the channel observations between Alice and Bob, and thus has an important role in how a key establishment algorithm must process a sequence of bidirectional channel probes. In the first case, it is necessary to complete bidirectional probing (Alice $\rightarrow$ Bob and Bob $\rightarrow$ Alice) before the channel decorrelates in order to ensure that Alice and Bob are observing highly correlated observations of the same phenomena. In the second case, temporal coherence plays a role in subsequent Alice-to-Bob probing: either the algorithm must explicitly utilize the correlation to ensure that Alice and Bob arrive at the same decisions (e.g., the Radio Telepathy algorithm of [8]), or else the algorithm must explicitly ensure that subsequent rounds of channel probing have decorrelated to ensure independence in the secret bits that are

[2] I will be the first to admit that I have leveraged this argument myself, c.f. [8]!

established (e.g., as exists in the JRNSO quantization algorithm [10]). If the channel is completely static (coherence time is infinite), there is no "renewal" process, which leads to several problems in key establishment: Alice and Bob might not establish enough bits from a single channel usage; and a key formed at one instance might be the same as a key formed at a later time, and hence Eve can run her own measurements later to estimate Alice's and Bob's shared key. If the channel is somewhat dynamic, the key extraction algorithm must cope with correlated measurements. For example, in a level crossing algorithm, the correlation between subsequent Alice and Bob measurements is the basis for key extraction protocol, while in a quantization-based algorithm, subsequent measurements by Alice and Bob must be independent (e.g., either delayed measurements or by a whitening procedure).

The Channel Is Gaussian (or Symmetric): We often assume that our channels are Gaussian, but how Gaussian is "Gaussian" really when we consider fading? Without symmetry in the fading distribution, physical layer key establishment schemes may suffer from poor distillation if not properly considered. Gaussianity arises in fading from the sum of many independent non-resolvable multipaths. However, as bandwidth increases, resolvability sets in, and the standard application of the central limit theorem begins to fail. Hence, there is a potential problem as we take physical layer key establishment to the wideband regime. Even in non-wideband regimes, we need an assurance that the distribution of key bits coming out of physical layer key establishment is unbiased, which necessitates an assurance that the underlying channel is symmetric. This is a strong requirement, and merely saying that ideal fading is Gaussian and hence symmetric is not sufficient. Being able to reliably quantify and ensure that the channel Alice and Bob are experiencing is close to having a symmetric distribution and quantify the proper amount of privacy amplification is an important problem facing physical layer key establishment, which will necessitate connecting empirical channel estimation to statistical tests that can strongly verify the symmetric nature of the channel. Of course, there is the fundamental question: How close is close enough to symmetric?

The Adversary Cannot Control the Channel: The notion of an active or passive adversary typically has to do with whether the adversary is merely listening or actively injecting communications into the environment. In the context of physical layer methods, we should also consider that the adversary may attempt to manipulate the environment to its advantage. Although unlikely, a powerful attacker would be one that is able to manipulate the amplitude and phases of the signals being exchanged between Alice and Bob in a controlled manner by manipulating the environment. In particular, by manipulating the environment, it is possible to bias the resulting bits in the key establishment process. Such an attack was illustrated in [11] where naïve key establishment that merely uses received signal strength was shown to be able to be manipulated. An interesting question that remains is whether key establishment schemes that are based on complex channel characterizations can be similarly affected and controlled by an adversary.

Integrating Channel Knowledge into Practical Secrecy Dissemination: In secret dissemination, the approach taken to convey secret information depends on the amount of channel state information that is known to the various benign and adversarial participants. There is a considerable amount of work that characterizes secrecy under varying amounts of statistical information available regarding the Alice-Bob and Alice-Eve channel state [3]. A natural next step is to make the explicit connection between how Alice can assess what information she has and how she can adjust her secret communication methods appropriately in an online manner.

Hurdles from Practical Matters

Complementing the above hurdles is an array of practical matters that need to be addressed when moving to a system implementation. Although my intent is to highlight fundamental hurdles that we need to address, I would be remiss if I were not to mention my list of practical hurdles. There are several practical aspects of a transceiver's design that make utilizing channel reciprocity challenging when conducting physical layer key establishment. Beyond the issue of channel coherence time identified earlier, there are other matters that impact the validity of the reciprocity assumption, including properly quantizing channel estimates and non-isotropic noise conditions. Furthermore, there are matters related to calibration and associated amplifier discrepancies, transceiver burn-in, and frequency drift. We must have the appropriate tools in our toolbox to address these challenges, and although I am certain we may borrow methods from conventional communications engineering, I expect the security aspect of the problem will necessitate some new tricks when implementing in real systems. Turning to physical layer authentication, if Alice and Bob have lost their connection for a period of time, the channel no longer supports Bob's verification as the Alice $\rightarrow$Bob channel will have significantly changed. Thus, an important challenge is how to keep authentication going following communication outages. Lastly, in regard to secret dissemination, much of the literature focuses on results under assumptions of Gaussian signaling. This is unrealistic — no practical communication system employs Gaussian signaling, but instead actual transmissions involve discrete constellations, like quadrature amplitude modulation (QAM). For secret communication, discrete signaling behaves quite differently from Gaussian signaling. As an example, in a fast fading scenario, QAM can perform better than Gaussian schemes when Bob's channel is on average worse than Eve's channel as the discrete nature of the signaling effectively limits the information leakage when Eve's channel is better [12–14]. I think we should realize that if discrete signaling gives different conclusions than Gaussian signaling, and discrete constellations are practical, we ought to explore them more in our community's work. Furthermore, I believe that

The notion of an active or passive adversary typically has to do with whether the adversary is merely listening or actively injecting communications into the environment. In the context of physical layer methods, we should also consider that the adversary may attempt to manipulate the environment to its advantage.

Investigating approaches such as ciphers or encoding for physical layer confidentiality that are efficient and have little to no message expansion is a promising direction for investigation that would greatly benefit IoT devices. As a researcher and participant in physical layer security, I am excited to see how these challenges will be addressed in the years ahead.

not only will we learn valuable lessons when going to practical implementations, but we might also find characteristics beneficial in overcoming some of the other hurdles outlined earlier.

Discussion: There Is Light at the End of the Tunnel

I do not want the reader to think that there is only bad news. I do not believe this to be the case. The above discussion has identified hurdles we need to address, and for which I believe the community has more than ample ingenuity to overcome. By comparison, a survey of classical security research will reveal a long list of encryption algorithms and security protocols that have undergone refinement over the years, and this is as natural to security engineering as it is to communications engineering or any other form of research. Furthermore, as I have noted earlier, we must bridge the language gap between our community and the classical security community in order to have the security community adopt our methods. Toward this end, we can revisit many of our approaches, and explore them in the context of semantic security and indistinguishability — this is a relatively low-hanging fruit as some of the formulations we have devised share many of the same properties as desired by the modern cryptography community. As an example, there is a remarkable similarity between probabilistic encryption [15] and codes developed for secret dissemination.

I would also like to offer to the community my belief that physical layer security is the best approach to securing many emerging wireless systems that are not well suited for conventional cryptographic approaches. In particular, we have all heard the rumblings of the Internet of Things (IoT) as a new area of research. I would point out that a significant portion of the IoT will be low-end, low-energy, and lightweight computing devices that will come with real restrictions on how one designs their functions. For these low-end devices, most of the available energy and computation must be devoted to executing core application functionality, and there may be little left over for supporting security. This is where I feel that the physical layer security community can have a notable impact as an ideal approach to securing the low end of the IoT is to dual-use existing radio communication functions for security. For example, physical layer signal processing can be applied at a gateway receiver to authenticate whether a transmission came from the expected IoT transmitter in the expected location. Similarly, one might explore using the physical layer for confidentiality, and along these lines I would note that physical layer secrecy has its own costs; perhaps the most obvious is the message expansion needed for confidentiality. Similar to the message expansion problems associated with probabilistic encryption, a source coding approach to physical layer secrecy typically involves a coded ciphertext that is larger than the plaintext. Since the message is larger, there will be more strain on the energy needed by the system. Investigating approaches such as ciphers or encoding for physical layer confidentiality that are efficient and have little to no message expansion is a promising direction for investigation that would greatly benefit IoT devices. As a researcher and participant in physical layer security, I am excited to see how these challenges will be addressed in the years ahead.

References

[1] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, Springer, 2010.
[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge, 2011.
[3] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*, NOW, 2009.
[4] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Trans. Wireless Commun.*, vol. 7, 2008, pp. 2571–79.
[5] L. Xiao *et al.*, "Channel-Based Detection of Sybil Attacks in Wireless Networks," *IEEE Trans. Info. Forensics Security*, vol. 4, 2009, pp. 492–503.
[6] X. He and A. Yener, "Providing Secrecy When the Eavesdropper Channel is Arbitrarily Varying: A Case for Multiple Antennas," *Proc. 2010 48th Annual Allerton Conf. Commun., Control, and Computing*, Sept. 2010, pp. 1228–35.
[7] X. He and A. Yener, "On the Role of Feedback in Two-Way Secure Communication," *Proc. 2008 42nd Asilomar Conf. Signals, Sys. and Computers*, Oct. 2008, pp. 1093–97.
[8] S. Mathur *et al.*, "Radio-Telepathy: Extracting a Cryptographic Key from an Un-Authenticated Wireless Channel," *Proc. 14th ACM Annual Int'l. Conf. Mobile Computing and Networking*, 2008.
[9] X. He *et al.*, "Is Link Signature Dependable for Wireless Security?" *Proc. IEEE INFOCOM*, 2013, April 2013, pp. 200–04.
[10] C. Ye *et al.*, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *IEEE Trans. Info. Forensics Security*, vol. 5, 2010, pp. 240–54.
[11] S. Jana *et al.*, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," *Proc. 15th ACM Annual Int'l. Conf. Mobile Computing and Networking*, 2009, pp. 321–32.
[12] S. Bashar, D. Zhi, and Chengshan Xiao, "On the Secrecy Rate of Multi-Antenna Wiretap Channel Under Finite-Alphabet Input," *IEEE Commun. Lett.*, vol. 15, no. 5, May 2011, pp. 527–29.
[13] S. Basharand, D. Zhi, and Chengshan Xiao, "On Secrecy Rate Analysis of MIMO Wiretap Channels Driven by Finite-Alphabet Input," *IEEE Trans. Commun.*, vol. 60, no. 12, Dec. 2012, pp. 3816–25.
[14] Z. Li, R. Yates, and W. Trappe, "Achieving Secret Communication for Fast Rayleigh Fading Channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, Sept. 2010, pp. 2792–99.
[15] S. Goldwasser and S. Micali, "Probabilistic Encryption," *J. Computer and Sys. Sci.*, vol. 28, 1984, pp. 270–99.

Biographies

Wade Trappe [F] (trappe@winlab.rutgers.edu) is a professor in the Electrical and Computer Engineering Department at Rutgers University, and associate director of the Wireless Information Network Laboratory (WINLAB), where he directs WINLAB's research in wireless security. He has led several federally funded projects in the area of cybersecurity and communication systems, projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources (the ORBIT testbed, www.orbit-lab.org), and new RFID technologies. His experience in network security and wireless spans over 15 years, and he has co-authored a popular textbook in security, *Introduction to Cryptography with Coding Theory*, as well as several monographs on wireless security, including *Securing Wireless Communications at the Physical Layer and Securing Emerging Wireless Systems: Lower-layer Approaches*. He has served as an Editor for *IEEE Transactions on Information Forensics and Security*, *IEEE Signal Processing Magazine*, and *IEEE Transactions on Mobile Computing*. He served as the lead Guest Editor for the September 2011 Special Issue of *Transactions on Information Forensics and Security* on Using the Physical Layer for Securing the Next Generation of Communication Systems and served as the IEEE Signal Processing Society representative to the governing board of IEEE TMC. He is currently IEEE SPS Regional Director for Regions 1-6.