Realizing physical layer security in large wireless networks using spectrum programmability

Bouhafs, Faycal; den Hartog, Frank; Raschella, Alessandro; Mackay, Michael; Shi, Qi; Sinanovic, Sinan

Published in:
2020 IEEE Globecom Workshops (GC Wkshps)

DOI:
10.1109/GCWkshps50303.2020.9367399

Publication date:
2021

Document Version
Author accepted manuscript

Realizing Physical Layer Security in Large Wireless Networks using Spectrum Programmability

Faycal Bouhafs[1], Frank den Hartog[1], Alessandro Raschella[2], Michael Mackay[2], Qi Shi[2], Sinan Sinanovic[3]

[1]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia
[2]School of Computer Science and Mathematics, Liverpool John Moores University, Liverpool, UK
[3]School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, Scotland UK
{f.bouhafs, frank.den.hartog}@unsw.edu.au, {A.Raschella, M.I.Mackay, Q.Shi}@ljmu.ac.uk, Sinan.Sinanovic@gcu.ac.uk

***Abstract*— This paper explores a practical approach to securing large wireless networks by applying Physical Layer Security (PLS). To date, PLS has mostly been seen as an information theory concept with few practical implementations. We present an Access Point (AP) selection algorithm that uses PLS to find an AP that offers the highest secrecy capacity to a legitimate user. We then propose an implementation of this algorithm using the novel concept of spectrum programming which extends Software-Defined Networking to the physical and data-link layers and makes wireless network management and control more flexible and scalable than traditional platforms. Our Wi-Fi network evaluation results show that our approach outperforms conventional solutions in terms of security, but at the expense of communication capacity, thus identifying a trade-off between security and performance. These results encourage implementation and extension to further wireless technologies.**

Keywords*— Physical Layer Security, IEEE 802.11, Wireless Communications

I. Introduction

The rise of the Internet of Things (IoT) introduces new challenges to wireless communications as it implies the massive deployment of networked devices, all requiring access to the Internet via a range of technologies. However, the broadcast nature of wireless communications makes them vulnerable to interception by unauthorized or malicious users, which has largely been mitigated to date through cryptographic encryption [1, 2]. In addition, a significant portion of these devices also have limited resources and therefore cryptographic solutions might not be sufficient for this case.

In this context, physical layer security (PLS) [3] is emerging as a promising approach through exploiting the physical properties of the wireless channel. Specifically, PLS limits the amount of information that can be intercepted by a malicious user at the bit level by taking advantage of the imperfections of the communication channel due to its inherent randomness and the presence of noise. These properties make PLS an attractive option to add an extra layer of security [4]. However, so far there has been no contributions that propose a full approach to apply PLS in a specific Radio Access Technology (RAT). We aim to address this challenge and consider PLS in the context of IEEE 802.11 and more specifically large Wi-Fi networks. In recent years, Wi-Fi technology has become almost ubiquitous in workplaces and public spaces and is seen as an important enabling technology for the IoT. These large scale networks often represent an ideal environment for malicious users to eavesdrop and intercept sensitive information [5]. In this paper, we propose a new algorithm which connects a Wi-Fi user to the Access Point (AP) that offers the most secure connectivity according to the principles of PLS. The algorithm is based on the concept of spectrum programming which enables centralized and fine-grained management of wireless networks. This concept was first introduced as part of the EU Horizon 2020 funded Wi-5 project [6], and an open-source prototype of the architecture is available in [7].

The remainder of this paper is organized as follows. Section 2 describes the context of large Wi-Fi networks and presents our algorithm. In Section 3, we first identify the challenges of implementing our approach and then explain the concept of spectrum programming and how it could be used to facilitate our PLS implementation. In Section 4, we present the adversary model against which the proposed algorithm will be assessed. In Section 5, we describe the simulation model we used to evaluate our solution and present the obtained results. We also discuss our evaluation approach in relation to the real security threats that large wireless networks face. Finally, in Section 6 we present our conclusions and the proposed future work.

II. Applying PLS to Large wireless networks

Our aim through this research is to secure wireless networks using PLS, starting with Wi-Fi. Currently, these networks rely on encryption through WP2, and now WPA3, to protect the privacy of its users and their data but these protocols have been found to be vulnerable [31]. Wireless networks are generally prone to eavesdropping due to the broadcast nature of the medium and malicious users could therefore try to intercept communications on these networks. The problem becomes further accentuated in large Wi-Fi networks, where multiple APs are deployed to provide better coverage and offer higher capacity. Upon joining a network, a Wi-Fi user is associated to the AP that provides the best signal, often based on the Received Signal Strength Indicator (RSSI). Other metrics have been considered when selecting a suitable AP where the objective is to maximize the quality of service (QoS) for the user. These contributions can be classified as either distributed

[8] or centralized approaches [9]. Distributed solutions often apply game theory strategies, neural networks, and/or cross-layer approaches for a device to gather performance-related measurements from the network before selecting the most suitable AP according to a specific metric. Centralized approaches, on the other hand, rely on the global view obtained by a network controller to decide the most suitable AP. Although not scalable, centralized approaches tend to be more efficient, especially in large Wi-Fi networks, since the central controller is able to not only obtain a more accurate view of the state of the whole network, but also apply load balancing to avoid congesting certain APs.

To the best of our knowledge, no AP selection mechanisms have been contributed to the literature that try to optimize the security of wireless users' connectivity. We therefore propose an AP selection algorithm that exploits the principles of PLS to find the AP that could provide the best security to a Wi-Fi user in a large Wi-Fi network. To better explain the algorithm, we first provide a summary of the symbols considered in Table 1.

Notation	Description
W	Set of deployed 802.11 APs; $W = \{AP_1, AP_2, \dots, AP_N\}$
N	Number of 802.11 APs; $\|W\| = N$
S	Set of legitimate stations; $S = \{STA_1, STA_2, \dots, STA_M\}$
M	Number of legitimate stations; $\|S\| = M$
$\bar{S}$	Set of eavesdropping stations; $\bar{S}$=$\{\overline{STA_1}, \overline{STA_2}, \dots, \overline{STA_E}\}$
E	Number of eavesdropping stations; $\|\bar{S}\| = E$
B	Bandwidth offered by 8021.11 channel, expressed in Hz
$S_{i,j}$	SINR experienced by station STA_j from AP_i
$RSSI_{i,j}$	Received Signal Strength Indicator provided by AP_i to STA_j
$C_{i,j}$	Shannon capacity of the channel between AP_i and STA_j; $C_{i,j} = Blog_2(1 + S_{i,j})$

Table 1. Description of Symbols

We assume that STA_m is trying to connect to the Wi-Fi network in the presence of E eavesdropping stations. By the principles of PLS, STA_m can communicate securely with an AP AP_n in the presence of an eavesdropping station STA_e, as illustrated in Fig. 1, if $C_{n,m} > C_{n,e}$. This value considers the channel gain between the station and the AP, the AP transmit power, the additive Gaussian white noise, and the interference experienced by the station from other APs.

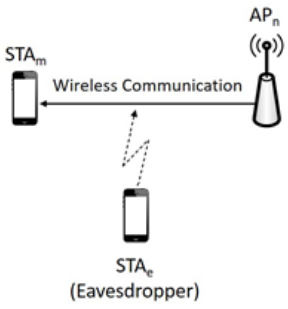

Fig. 1. Example of eavesdropping in Wi-Fi networks.

First, the algorithm determines the two APs that provide the strongest RSSI to STA_m, labelled AP_{n1} and AP_{n2}, respectively. Second, it measures the capacity of the channel between STA_m and each of AP_{n1} and AP_{n2}, labelled: $C_{n1,m}$ and $C_{n2,m}$ respectively. Third, the algorithm selects STA_e, the eavesdropping station that receives the strongest RSSI from AP_{n1}. Fourth, the algorithm measures the capacity of the channel between STA_e and AP_{n1} and AP_{n2}, labelled: $C_{n1,e}$ and $C_{n2,e}$. Note that we assume that the location of each eavesdropper is known, and that its channel capacity can be measured. This assumption is reasonable and is discussed further in section 4. Finally, the algorithm connects STA_m to the AP that could guarantee $C_{s,m} = max\{C_1, C_2\}$, as presented in **Algorithm 1** below.

Algorithm 1

```
Determine AP_n1 and AP_n2 from W
Measure C_n1,m and C_n2,m
RSSI_n1 := 0
For each STA_j ∈ S̄
    Measure RSSI_n1,j
If (RSSI_n1,j > RSSI_n1)
    RSSI_n1,j → RSSI_n1
    STA_j → STA_e
End If
End For
Measure C_n1,e and C_n2,e
C_1 := 0
C_2 := 0
If (S_n1,m > S_n1,e)
    C_n1,m − C_n1,e → C_1
End If
If (S_n2,m > S_n2,e)
    C_n2,m − C_n2,e → C_2
End If
If (C_1 > C_2)
Connect STA_m to AP_n1
Else
Connect STA_m to AP_n2
End If
```

Therefore, the central idea behind the algorithm is that an STA can always find an AP to connect to, such that its channel capacity is larger than the channel capacity of the closest eavesdropper, and thus secrecy can be achieved. This is a reasonable assumption as eavesdroppers in this use case operate at the periphery of the Wi-Fi network and thus have lower channel capacity than legitimate users. We also assume that there is no other adversary station $STA_{e'}$ with its capacity $C_{n2,e'} > C_{n2,e}$.

III. Designing an SDN-based PLS System

A. Design Considerations to Realize PLS

Applying our PLS algorithm necessitates implementation as part of a real-time network control platform which requires certain design considerations that are not addressed in previous PLS-related work. More specifically, a platform to enable the application of PLS to large Wi-Fi networks should be able to:

1. **Frequently measure channel capacity**: The PLS algorithm relies on frequent measurements of the channel's capacity between each STA and AP in the network, typically in the order of a measurement every few seconds.
2. **Dynamically apply the PLS algorithm**: The platform should be able to gather all the measurements and calculate

the channel that provides the best secrecy to a legitimate STA according to the proposed algorithm.

3. **Ability to rapidly manage connections**: Once the system determines the AP to provide the most secure connectivity, it should be able to quickly associate the STA to the AP. This should happen within milliseconds, as another handover may be needed seconds later, and minimal capacity should be lost in the process.

As mentioned previously, centralized solutions are more efficient in managing large Wi-Fi networks. However, existing centralized platforms are either vendor specific or are unable to support the capabilities identified above. Vendor-specific solutions are usually applicable to single domain networks such as enterprise networks but cannot be used in multi-domain networks such as apartment blocks [10]. Moreover, vendors typically do not provide security solutions that go beyond the currently accepted standards. Therefore, in order to implement the proposed algorithm, it will be necessary to deploy a management platform that provides open interfaces for third-party applications, as is the case with programmable networks such as Software-Defined Networking (SDN) [11]. Wi-5 is a programmable architecture that extends the concept of SDN to manage Wi-Fi networks including radio resources and connection management, both of which are necessary to realize PLS. Next, we will highlight the main differences between SDN and spectrum programming and how Wi-5 could be used to realize PLS for large Wi-Fi networks.

B. How to Realize PLS With Spectrum Programming

SDN has emerged as an open, efficient and flexible approach to manage large networks by decoupling the control plane from the data plane and centralizing the network management operations in a single entity, referred to as a controller. This concept has now been extended to wireless networks management through what is referred to as Software-Defined Wireless Networking (SDWN) [12]. Several SDWN solutions have been proposed to manage different types of wireless networks, including Wi-Fi. However, these solutions fall short of supporting radio resource management and do not offer the monitoring capabilities required to implement the proposed algorithm. Moreover, these solutions, although open, do not offer the necessary primitives to make radio resources programmable and accessible to third parties. On the other hand, research in the area of Software Defined Radio (SDR) has resulted in programming platforms for radio communications [13, 14]. Nevertheless, these platforms only offer limited programmability on the communications level, and thus are unsuitable for fine-grained wireless network management.

Spectrum programming platforms such as Wi-5 address these limitations by introducing the spectrum plane to the data plane and control plane as defined in SDN. The spectrum plane extends the programmability of the network down to the radio spectrum. In Wi-5, as illustrated in Fig. 2, APs expose the main radio primitives to the Wi-5 central controller which in turn exposes a northbound API, enabling third parties to develop various applications for programming the wireless network as desired. We believe that such architectures are ideal to implement the proposed algorithm. In its current form [7], however, Wi-5 is implemented with only Wi-Fi, and SDR is left for future work.

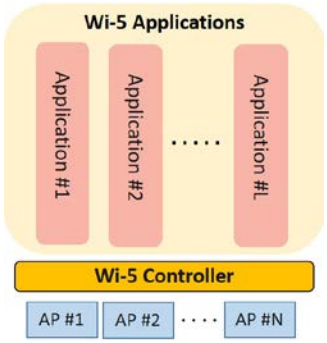

Fig. 2. High-level depiction of the Wi-5 architecture

As shown in Fig. 3, our algorithm will operate on the Wi-5 controller and obtains measurements from the APs using the monitoring primitives offered by the platform, for the computation of the secrecy capacity. Once the AP that offers the highest secrecy capacity is found, the controller will use the AP-STA association functionality to connect the STA to the selected AP. We rely on a spectrum programming architecture such as Wi-5 to do this quickly by utilizing the concept of Lightweight Virtual Access Points (LVAP), which enable handovers within milliseconds [15].

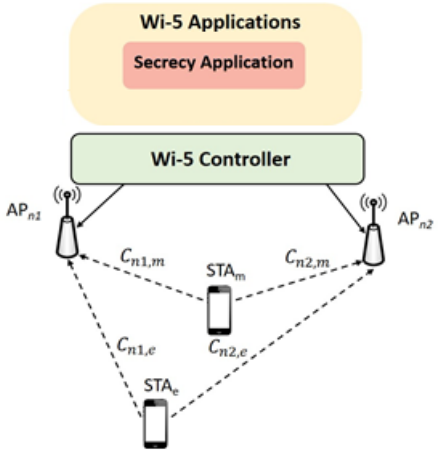

Fig. 3. Implementation of the secrecy algorithm using the Wi-5 architecture

IV. ADVERSARY MODEL

Our aim is to apply the principles of PLS to secure large Wi-Fi networks against adversaries that fit the following model:

Passiveness: The adversary is a passive wiretapper and does not try to actively affect the quality of communication of a legitimate user. It simply tries to eavesdrop on it.

Malicious: The adversary aims to steal sensitive information from legitimate users through interception of the data communicated over their Wi-Fi connection.

Location: The adversary deploys several STAs as close as possible to the Wi-Fi network such that these stations can eavesdrop on legitimate users. In a typical use case, for example an enterprise network in a private environment, we expect this would be somewhere along the perimeter of the network. The

location of the eavesdropping stations are, however, known to the Wi-Fi APs of the network. This is a reasonable assumption as previous work proves APs can detect eavesdropping stations [16]. Their location may change over time, but not faster than what can be expected from a typical nomadic user.

Eavesdropping Capabilities: The capabilities of the adversary do not allow it to receive a noiseless signal when eavesdropping on legitimate users. This means that the channel of each eavesdropping station STA_e is a noisy version of the legitimate user's channel. In addition, we assume that knowledge of the gains of all channels is available to the APs.

V. PERFORMANCE EVALUATION

To evaluate the performance of the proposed PLS algorithm, we conducted a range of experiments while applying two different AP selection models: the secrecy-based model as described in section 3, and a reference model in which the AP offering the best RSSI is always selected. We assume that all APs operate according to IEEE 802.11, are homogeneous, and managed via a Wi-5 controller.

A. Algorithm Implementation

We used MATLAB to simulate a large Wi-Fi network consisting of 25 fixed APs randomly deployed in an outdoor area of 300m × 300m at a minimum distance of 50m from each other, which serve 200 STAs. The STAs are uniformly distributed within the same area and have different bit rate requirements that vary between 100 kbps and 10 Mbps, which will be considered for the computation of the throughput. In these simulations, we adopted a common free-space large-scale path loss model with the path loss exponent set to 2. Moreover, the bandwidth of the AP channels, the transmit powers, and the noise power are 20 MHz, 20 dBm and -92 dBm, respectively. To assess the performance of our algorithm in the presence of eavesdropping terminals, we simulate three scenarios in which the number of STA_e E varies between 10, 20, and 40. These stations are randomly deployed and uniformly distributed at the edge of the 300m × 300m area, and follow the adversary model described in section 4. Every simulation run is repeated 10 times, taking a different uniform distribution of the APs and stations each time, and the results are averaged.

We simulate the secrecy-based algorithm, assuming it runs as an application in the platform described in Section 3. The algorithm uses the monitoring functionality of the architecture to measure the capacity of the channel between each AP and the STAs. Since our adversary model assumes that the location of eavesdropping stations is known to the APs, the controller is therefore able to measure the capacity of the channel between each AP and any eavesdropping station. The algorithm then associates each station to the AP that offers the best security, as defined in section 2, and executes the association using LVAPs. For the sake of comparison, we implement another AP selection algorithm based on RSSI, where a station is always associated to the AP that offers the highest signal strength. We assess both algorithms according to the following performance metrics while varying the number of eavesdropping stations E:

1. **Secrecy rate $C_{s,n,m}$**: This represents the transmission rate at which the selected AP_n communicates with a legitimate STA_m without being intercepted by the closest eavesdropper. The maximum achievable secrecy rate is known as the secrecy capacity.
2. **Shannon rate $C_{n,m}$**: This represents the communication capacity of the channel that AP_n offers to a legitimate connected station STA_m.
3. **Throughput**: This represents the amount of data per second passing through the connection offered by the selected AP_n to a legitimate STA_m, taking into account all the STAs that are sharing AP_n's available data rate. The upper bound of the throughput for STA_m corresponds to its bit rate requirement.

The secrecy rate in the case of the RSSI-based algorithm considers the possible presence of the detected STA_e that receives the strongest RSSI from the selected AP, based on step 4 of the algorithm.

B. Secrecy rates

Fig. 4, Fig. 5, and Fig. 6 show the Cumulative Distribution Function (CDF) of the Secrecy rate and Shannon rate under both AP selection algorithms in the three simulated scenarios, i.e. for E=10, E=20, and E=40, respectively. The x-axis is in units of 100 Mbps. For each scenario, the CDF includes the rates obtained for all the legitimate STAs over all the independent simulations. From Fig. 4 we can observe that the probability of achieving a secrecy rate below 10 Mbps where E=10 is quite low for both algorithms, with the CDF for the RSSI-based algorithm and secrecy-based algorithm at 15% and 5% respectively. This means that both algorithms can find an AP that could offer a secure connection with a secrecy rate at 10 Mbps or higher, but the secrecy-based algorithm has a higher chance of achieving this. Fig. 4 also shows that the probability of achieving a specific secrecy rate below the required value increases with the required secrecy rate. This means that the probability of finding an AP that could offer a secrecy rate at or above this value shrinks. This behavior is expected, because the presence of eavesdropping stations makes it difficult to achieve high secrecy rates. More specifically, we can observe that the secrecy-based algorithm leads to significantly higher chances to achieve secrecy rates of 10-60 Mbps than the RSSI-based algorithm. This is an effect of connecting STAs to APs based on whichever provides the highest secrecy rather than signal strength. Both algorithms produce almost the same results for the probability to find an AP that can achieve a secrecy rate of >60 Mbps or lower. Apparently, it is very challenging to find such high secrecy capacities either way. Fig. 5, and Fig. 6 show that the probability of finding an AP that achieves a secrecy rate above a specific value drops as the number of eavesdropping stations increases. For instance, when E=20 (Fig. 5), the probability for both algorithms to achieve a secrecy rate below 10Mbps is higher than when E=10, with the CDF for the RSSI-based algorithm and secrecy-based algorithm at 35% and 12%.

The results obtained from this scenario (E=20) also show that achieving secrecy rates between 10Mbps and 60Mbps becomes more difficult than with *E=10*. Nevertheless, our

algorithm still provides a better chance to find an AP with the required secrecy rate than the RSSI-based algorithm. The results also show that achieving a better secrecy rate affects the capacity offered by the AP to the STA. For instance, in Fig. 4 (E=10), when the required capacity is 20Mbps, both the secrecy-based and RSSI-based algorithms yield the same probability of finding an AP that could not achieve the same Shannon rate or higher, with the CDF at 5%. As the Shannon rate increases, the probability of the selected AP to achieve a lower rate becomes higher. However, when the Shannon rate is between 20Mbps and 110Mpbs, the AP selected by the secrecy-based algorithm has a higher probability of achieving a rate below these values than the one selected by the RSSI-based algorithm. A similar pattern is observed when E=20 and E=40, presented in Fig. 5 and Fig. 6, respectively. These results show that the improvement of the secrecy rate offered by our algorithm comes at a price as it affects the Shannon rate offered by the channel. The performance difference increases as the number of eavesdropping stations increases.

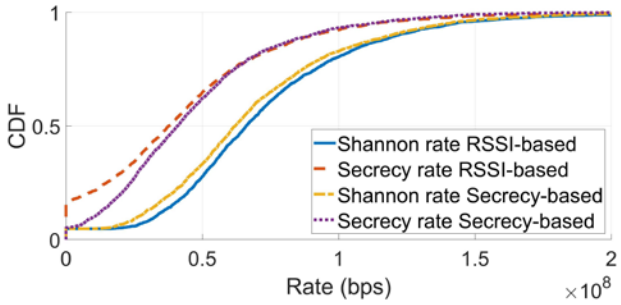

Fig. 4. CDF of secrecy and Shannon rate with 10 eavesdropping stations.

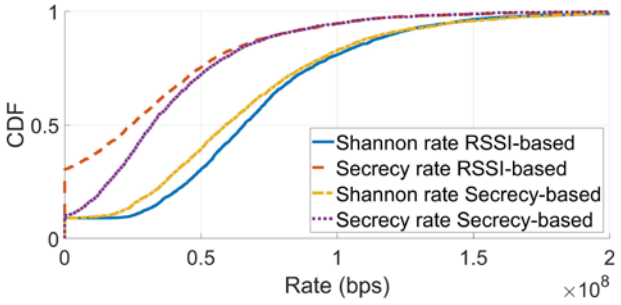

Fig. 5. CDF of secrecy and Shannon rate with 20 eavesdropping stations.

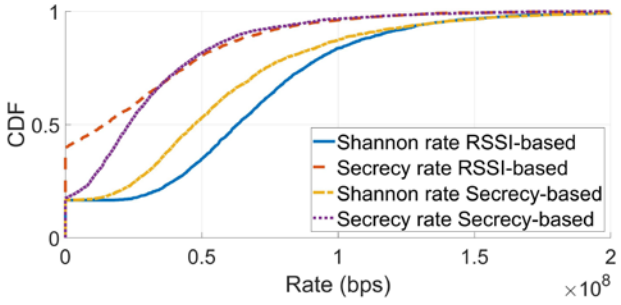

Fig. 6. CDF of secrecy and Shannon rate with 40 eavesdropping stations.

C. *Throughputs*

Fig. 7, Fig. 8 and Fig. 9 show the performance in terms of throughput for E=10, E=20 and E=40, respectively. In these figures, the upper and lower edges of the plotted boxes represent the 25th and 75th percentiles of the throughput distribution spread for all the STAs in the simulated area. Their median values are indicated by the central red lines. The values that we considered as outliers are indicated by red dots.

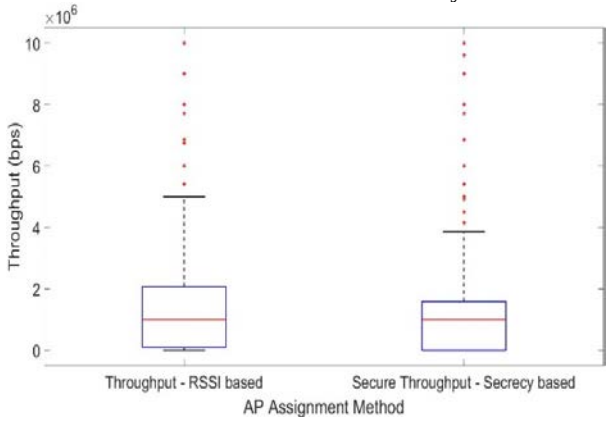

Fig. 7. Throughputs with 10 eavesdropping stations.

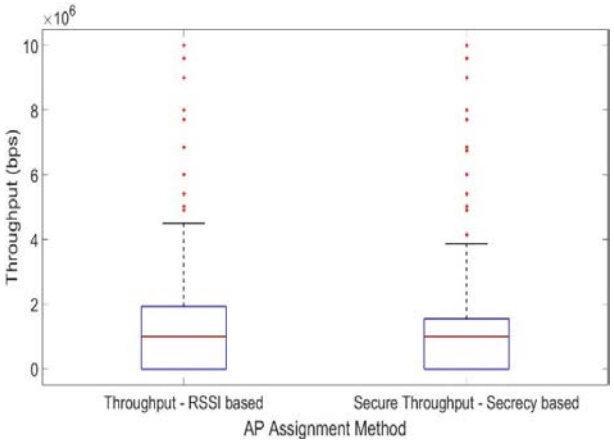

Fig. 8. Throughputs with 20 eavesdropping stations.

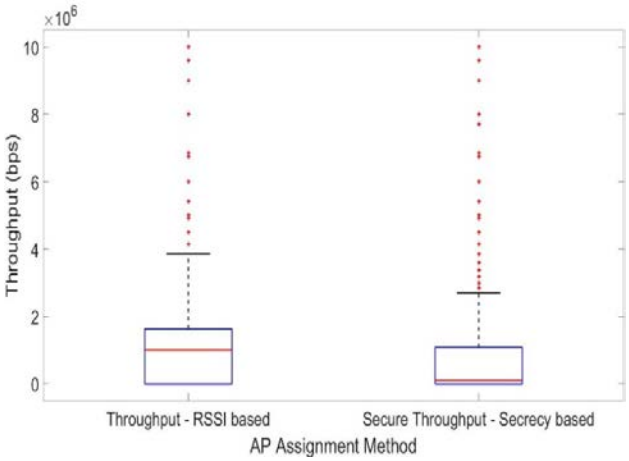

Fig. 9. Throughputs with 40 eavesdropping stations.

From Figures 4-9 we can conclude that the difference in terms of Shannon capacity illustrated in Figures 4-6 affects the throughput that could be achieved using each algorithm, which is shown in Figures 7-9. Note that an adversary would like to minimize the number of eavesdropping stations deployed, as more stations increase the likelihood of detection. However, in this work we consider a worst case scenario where the network

is operating in a very hostile environment with many adversaries trying to steal information. In addition to the relevance of this scenario to today's cyber security concerns, our work also helps to achieve the following objectives:

1. Assess the performance of the network in the presence of eavesdroppers when using PLS optimization under the wiretap channel model in [17].
2. Identify tradeoffs between the different performance metrics wherever possible, i.e. determine the cost of a secure communication on other performance aspects of the network.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we presented a new AP selection algorithm to secure large wireless networks against eavesdropping using PLS. The algorithm is implementable today, using the concept of spectrum programming. The proposed approach is the first of its kind to apply PLS to secure a complete wireless network. Our evaluation results showed that the proposed secrecy-based algorithm offers a better secrecy rate than conventional solutions, thus providing better security to the users. These improvements come, however, at the expense of a lower capacity rate offered by the communication channel and therefore represents a trade-off between security and performance, where certain users could favor an improvement in terms of the secrecy rate at the expense of performance or the opposite. We believe that our results strongly encourage further research and implementation, along with extension to other wireless and mobile networking technologies and architectures such as beamforming. Other research questions that we will consider going forward include: 1) the role of indoor vs outdoor environments and the inclusion of reflections; and 2) the estimation of latency and overhead introduced by using the Wi-5 spectrum programming platform.

REFERENCES

[1] M. Stamp, *Information security: principles and practice*. Wiley Online Library, 2011.

[2] M. E. Whitman and H. J. Mattord, *Principles of information security*. Cengage Learning, 2011.

[3] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[4] H. Rahbari and M. Krunz, "Secrecy beyond encryption: obfuscating transmission signatures in wireless communications," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 54-60, 2015.

[5] W. A. Arbaugh, "Wireless security is different," *Computer*, vol. 36, no. 8, pp. 99-101, 2003.

[6] F. Bouhafs *et al.*, "Wi-5: A programming architecture for unlicensed frequency bands," *IEEE Communications Magazine*, vol. 56, no. 12, pp. 178-185, 2018.

[7] *Wi-5 GitHub*. Available: https://github.com/Wi5

[8] K. Sundaresan and K. Papagiannaki, "The need for cross-layer information in access point selection algorithms," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, 2006, pp. 257-262.

[9] H. Lee, S. Kim, O. Lee, S. Choi, and S.-J. Lee, "Available bandwidth-based association in IEEE 802.11 Wireless LANs," in *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems*, 2008, pp. 132-139.

[10] Y. S. Chen, W. H. Hsiao, and K. L. Chiu, "A cross-layer partner-based fast handoff mechanism for IEEE 802.11 wireless networks," *International Journal of Communication Systems*, vol. 22, no. 12, pp. 1515-1541, 2009.

[11] L. Chen, "A distributed access point selection algorithm based on no-regret learning for wireless access networks," in *2010 IEEE 71st Vehicular Technology Conference*, 2010, pp. 1-5.

[12] L.-H. Yen, J.-J. Li, and C.-M. Lin, "Stability and fairness of AP selection games in IEEE 802.11 access networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 3, pp. 1150-1160, 2011.

[13] B. Bojovic, N. Baldo, and P. Dini, "A neural network based cognitive engine for ieee 802.11 wlan access point selection," in *2012 IEEE Consumer Communications and Networking Conference (CCNC)*, 2012, pp. 864-868.

[14] X. Chen, W. Yuan, W. Cheng, W. Liu, and H. Leung, "Access point selection under QoS requirements in variable channel-width WLANs," *IEEE Wireless Communications Letters*, vol. 2, no. 1, pp. 114-117, 2012.

[15] I. Malanchini, M. Cesana, and N. Gatti, "Network selection and resource allocation games for wireless access networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 12, pp. 2427-2440, 2012.

[16] J. B. Ernst, S. Kremer, and J. J. Rodrigues, "A utility based access point selection method for IEEE 802.11 wireless networks with enhanced quality of experience," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 2363-2368.

[17] M. Liyanage, J. Chirkova, and A. Gurtov, "Access Point selection game for mobile wireless users," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, 2014, pp. 1-6.

[18] A. Raschellà *et al.*, "A dynamic access point allocation algorithm for dense wireless LANs using potential game," *Computer Networks*, vol. 167, p. 106991, 2020.

[19] K. Sood, S. Liu, S. Yu, and Y. Xiang, "Dynamic access point association using software defined networking," presented at the International Telecommunication Networks and Applications Conference (ITNAC), 2015.

[20] L.-H. Yen, T.-T. Yeh, and K.-H. Chi, "Load balancing in IEEE 802.11 networks," *IEEE Internet Computing*, vol. 13, no. 1, pp. 56-64, 2009.

[21] F. den Hartog, A. Raschella, F. Bouhafs, P. Kempker, B. Boltjes, and M. Seyedebrahimi, "A pathway to solving the Wi-Fi Tragedy of the Commons in apartment blocks," in *2017 27th International elecommunication Networks and Applications Conference (ITNAC)*, 2017, pp. 1-6: IEEE.

[22] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2014.

[23] I. T. Haque and N. Abu-Ghazaleh, "Wireless software defined networking: A survey and taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2713-2737, 2016.

[24] *Ettus research*. Available: https://www.ettus.com/

[25] *GNU Radio*. Available: https://www.gnuradio.org/

[26] J. Saldana *et al.*, "Unsticking the Wi-Fi client: Smarter decisions using a software defined wireless solution," *IEEE Access*, vol. 6, pp. 30917-30931, 2018.

[27] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," arXiv preprint arXiv:1504.07154, 2015.

[28] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in 2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2012, pp. 2809-2812.

[29] D. Kapetanovic, A. Al-Nahari, A. Stojanovic, and F. Rusek, "Detection of active eavesdroppers in massive MIMO," in 2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC), 2014, pp. 585-589.

[30] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[31] M. Vanhoef and F. Piessens, "Release the Kraken: New KRACKs in the 802.11 Standard", in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 299-314.