Machine Learning Based Attack Against Artificial Noise-aided Secure Communication

Yun Wen*, Makoto Yoshida*, Junqing Zhang†, Zheng Chu‡, Pei Xiao‡ and Rahim Tafazolli‡
*Wireless Research Center, Fujitsu Laboratories Ltd.
Email: yun.wen@jp.fujitsu.com
†Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom
‡5G Innovation Centre (5GIC), University of Surrey, Guildford, GU2 7XH, United Kingdom

***Abstract*—Physical layer security (PLS) technologies have attracted much attention in recent years for their potential to provide information-theoretically secure communications. Artificial Noise (AN)-aided transmission is considered as one of the most practicable PLS technologies, as it can realize secure transmission independent of the eavesdropper's channel status. In this paper, we reveal that AN transmission has the dependency of eavesdropper's channel condition by introducing our proposed attack method based on a supervised-learning algorithm which utilizes the modulation scheme, available from known packet preamble and/or header information, as supervisory signals of training data. Numerical simulation results with the comparison to conventional clustering methods show that our proposed method improves the success probability of attack from 4.8% to at most 95.8% for the QPSK modulation. It implies that the transmission to the receiver in the cell-edge with low order modulation will be cracked if the eavesdropper's channel is good enough by employing more antennas than the transmitter. This work brings new insights into the effectiveness of AN schemes and provides useful guidance for the design of robust PLS techniques for practical wireless systems.**

***Index Terms*—Physical Layer Security; Artificial Noise; Machine Learning; Supervised-learning; Blind Estimation**

I. Introduction

Wireless communications are expected to expand into mission critical services such as connected vehicles and remote medicine, which makes security one of most important concerns in future wireless systems [1]. Wireless transmissions have inherent security vulnerability due to their broadcast nature, which makes passive eavesdropping and active attacks much easier compared with their wired counterpart. Traditional cryptographic schemes protect the data by encryption, but they may be cracked in the future by the emerging quantum computing technologies [2]. On the other hand, Physical Layer Security (PLS) technologies take a new direction by exploiting the unpredictable characteristics of the wireless channel, such as fading, to achieve information-theoretically secure communication [3].

Artificial noise (AN)-aided transmission is considered as one of the most practicable methods among numerous PLS technologies [4], as it can realize a secure communication without the eavesdropper (Eve)'s channel information and independent of Eve's channel status, e.g. signal-to-noise ratio (SNR). The legitimate transmitter, Alice, equipped with multi-antenna, firstly generates AN vectors based on the unique channel impulse response between itself and the legitimate receiver, Bob. Alice will then add the AN vectors, lying in the null space of the Alice-Bob channel, to information vectors for transmission, thus the AN vectors only interfere Eve. Since the noise vector and information vector are both transmitted from the same transmitter, Eve cannot improve its receiving signal-to-interference ratio (SIR) even the wireless channel between Alice and Eve is very good. Although some other PLS technologies such as GSVD-based and ZF-based precoding [5], [6] can also provide secure communication independent of Eve's SNR, their precoding requires Eve's channel state information which is usually not available in real systems.

Most existing AN work considers that Eve has less antennas than Alice [7], [8], which is a too optimistic assumption and difficult to be guaranteed. Therefore, how to ensure secure communication when Eve has more antennas than Alice, is essential for the practical realization of AN methods. As pointed out in [9], when Eve has more antennas than Alice, it can use the channel information between Alice to Bob and Alice to Eve to cancel the noise vector completely and achieve a higher capacity than Bob. It is thus necessary for Alice and Bob to protect their channel information from Eve to ensure secure communication under such condition.

Survival tests by many attack methods are necessary to prove the robustness of security schemes [10]. Therefore, attack methods that help Eve estimate the channel between Alice and Bob for cracking AN-aided transmission, become an essential criteria to evaluate AN scheme' robustness for its practical realization. Despite its importance, there is very little work in this area. An attack method using independent component analysis (ICA) has been proposed in [11]. However, ICA can only deal with one Gaussian distributed source [12], thus may not work well to decode the AN signals which include multiple Gaussian distributed noise sources. Known plaintext attacks against PLS were proposed in [13] and [14], whose performances highly depend on the amount of available known plaintext. Since Alice will obviously not transmit known wireless header information, e.g. preamble, by using AN, which only benefit Eve by providing known information with its cipher-text, it is difficult for the above methods to work well in real system environments.

The work in [15] proposes an attack method which only uses AN-aided symbols. This method treats AN-aided modulated

symbols as points distributed in different hyperplanes, and decodes the desired information by adopting a clustering algorithm to transform them back to the correct constellation points. Although it does not need any additional information such as the known plaintext, the clustering algorithm has a high probability to converge to local optimal values due to its dependency on the initial values, especially when the modulation orders and number of antennas increase.

In this paper, we propose an efficient machine learning-based attack method. The method firstly utilizes the information of modulation scheme from an AN-aided packets' known symbols (preamble and/or header) to build the supervisory signals of training data. A supervised learning-based algorithm is then developed to search for the decode matrix, with which the received AN-aided signals can be transformed to have the smallest distance to the supervisory signals. Finally, an offline phase shift operation is adopted to remove the effect of phase-rotation thus the AN-aided signals can be recovered to those received in Bob, which means AN method is cracked. Numerical simulation results with the comparison to conventional clustering methods in [15] show that our proposed method improve the success probability of attack from 4.8% to at most 95.8% for the QPSK modulation. This implies when Eve adopts our attack method, AN transmission fails to keep its independence to Eve's channel status, and the transmission to the receiver in the cell-edge with low order modulation will be cracked if the Eve's channel is good enough.

The rest of this paper is organized as follows. In Section II, we give a brief description of AN transmissions and its problems. We present the details of our proposed method in Section III, and the simulation results with the comparison to the conventional method are shown in Section IV. We conclude the paper in Section V.

Notations: We denote conjugate, transpose, conjugate transpose, Euclidean norm and trace operations by $(\cdot)^*$, $(\cdot)^T$, $(\cdot)^H$, $||\cdot||$, and $Tr(\cdot)$, respectively. $\mathbb{C}^{m\times n}$ and $\mathbb{B}^{m\times n}$ are the set of $m \times n$ complex matrices and Boolean matrices, respectively. $\mathcal{CN}(\mu, D)$ denotes a complex Gaussian distribution with mean μ and covariance D.

II. System Model and Overview of AN

A. Preliminary of AN

We consider a system including one transmitter Alice, one legitimate receiver Bob, and one eavesdropper Eve, with numbers of antennas N_A, N_B, and N_E, respectively. As shown in Fig. 1, H and G are the uncorrelated Rayleigh-fading channels between Alice to Bob and Alice to Eve. Here, $H \in \mathbb{C}^{N_B\times N_A}$ and $G \in \mathbb{C}^{N_E\times N_A}$, and the elements of H and G are i.i.d. complex random variables. AN schemes assume $N_A > N_B$. Therefore, Alice can use its abundant antennas to generate AN vectors. Alice first operates singular value decomposition (SVD) of H as $H = U\Lambda V^H$, where V is an unitary matrix and $V \in \mathbb{C}^{N_A\times N_A}$, then derives subspaces for information vector and artificial noise from V as

$$V = [V_1, Z], \tag{1}$$

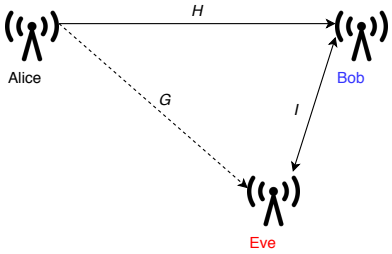

Fig. 1. System model.

where the subspace of information vector V_1 is the first N_B column of V, and Z is the subspace for the artificial noise. Alice generates its transmission signal vector x as

$$x = V_1 u + Zv, \tag{2}$$

where $u \in \mathbb{C}^{N_B\times 1}$ and $v \in \mathbb{C}^{(N_A-N_B)\times 1}$ are the information and noise vector, respectively. The elements in u are chosen from modulation constellation points with average power of σ_u^2, and elements in v are Gaussian random variables with variance σ_v^2. Because Z in (2) lies in the null space of H, the received signal at Bob and Eve, z and y, can be given as

$$z = Hx + n_B = HV_1u + HZv + n_B = HV_1u + n_B, \tag{3}$$

$$y = Gx + n_E = GV_1u + GZv + n_E, \tag{4}$$

respectively, where $n_B \sim \mathcal{CN}(0, \sigma_B^2)$ and $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ are the additive white Gaussian noise (AWGN) at Bob and Eve, respectively. The AN vector v only interferes Eve and degrades its SIR. As the information vector and artificial noise vector received at Eve experiences the same channel G, even Eve has a better wireless channel to Alice compared to Bob, it cannot achieve a higher capacity than an upper bound as shown in [4]. As such, a secure communication can be guaranteed when Alice transmits to Bob in a rate higher than Eve's upper bound capacity.

Power ratio (Pr) of the AN vector at Alice is an important factor, which is defined as

$$Pr = \frac{P_v}{P_u + P_v} = \frac{(N_A - N_B)\sigma_v^2}{N_B\sigma_u^2 + (N_A - N_B)\sigma_v^2}, \tag{5}$$

where P_u and P_v are power allocated to the information vector and noise vector, respectively. Larger Pr at Alice results in lower SIR at Eve but also causes lower SNR in Bob for information signal. This results in a trade-off in security rate as investigated in the literature [7], [8].

B. Attacks on AN in Practical Conditions

Most existing AN work assumes Eve has less antennas than Alice ($N_A > N_E$). However, it is difficult to guarantee this assumption in real systems, because Eve is likely to increase its number of antennas to achieve a higher capacity. When Eve equips more antennas and obtains the channel information of G and H, it has the ability to cancel the artificial noise with a decode matrix $HG^\dagger$, which can be given as

$$y' = HG^\dagger y = HG^\dagger Gx + HG^\dagger n_E = HV_1u + HG^\dagger n_E, \tag{6}$$

where $G^{\dagger}$ is the left inverse matrix of G which exists only when $N_E \geq N_A$. In this case, Eve can achieve a higher capacity than Bob if it has better channel to Alice than Bob, and as a result decode any transmission from Alice to Bob.

Therefore, in order to ensure secure communication, it is necessary to prevent Eve from obtaining H and G. For this purpose, Alice can require Bob to transmit pilot signals and estimate the channel at the transmitter side. Because the wireless channel between Alice and Bob is reciprocal and the estimation offset between Alice and Bob can be emitted by pre-adjustment, the estimated channel at Alice equals to H and can be used to generate AN signals. Although Eve may also receive the pilots from Bob, it can only estimate the channel I between Bob to Eve, which is uncorrelated with H thus useless at decoding AN signals with (6).

However, performance of AN scheme in above conditions has not been well investigated. As mentioned in [10], survival tests by possible attacks at Eve will be essential to prove AN scheme's robustness to encourage its practical realization. With this motivation, we propose an efficient attack method and use it to evaluate AN scheme's security performance.

III. Proposed Attack Method

In this section, we present the details of the proposed attack method against AN-aided transmissions. We firstly derive the supervisory signals which are the outputs of training data, from the information of modulation schemes available from packet's preamble and header. With these supervisory signals, a supervised-learning based algorithm is developed to estimate the decode matrix which can transform the AN-aided symbols to the points with smallest distance to supervisory signals. Finally, we adopt an offline phase shift operation for the transformed signals, to remove the effect of phase-rotation introduced from the estimation.

A. Derivation of Supervisory Signals

In practical wireless systems, each packet includes not only the data payload, but also preamble and physical layer header. Unlike the data part which is different in each packet, the format and information of the preamble and header is fixed or within a limited choice when using a specific standard. For example, for Wireless Local Area Network (WLAN) packet in IEEE 802.11ac [16], the modulation schemes are indicated in SIG-A part of the header, and can only be chosen from either BPSK, QPSK, 16QAM, 64QAM, or 256QAM. Therefore, applying AN to the preamble part which includes a lot of known information does not make sense, because it not only consumes the precious transmission power but also benefits Eve by providing known information and its cipher-text for known-plaintext attack [13], [14].

With the above practical considerations, we can derive the supervisory signals from the information of modulation schemes, for our supervised-learning algorithm. For simplicity, Bob is considered to have a single antenna ($N_B = 1$). Assuming $U = [u_1, u_2, ..., u_m]$ as the signal set of modulation, where m is the total number of signals corresponding to the constellation points. Alice maps its information bits to a symbol in U and generates AN-aided signals as shown in (2). As described in (2) and (4), the information vector is expanded by artificial noise to a vector of dimension N_A at Alice, and received by Eve as a N_E dimension vector.

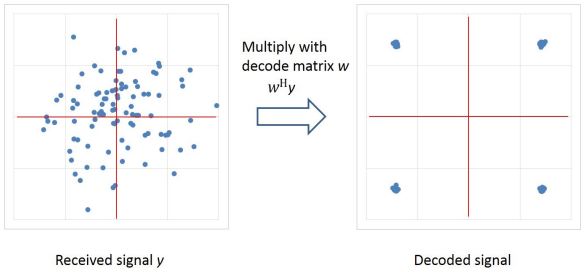

Fig. 2. Transformed AN-aided QPSK signals.

Since Eve does not know the wireless channel between Alice and Bob, it has to try to estimate a decode matrix w to transform the AN-aided signal vector y back to the transmitted information bits as

$$w^H y = b, \tag{7}$$

where $w \in \mathbb{C}^{N_E \times 1}$ is the normal vector and b is the transformed signal. Therefore, as shown in Fig. 2, when a vector $w^H = HG^{\dagger}$ is found by estimation and Eve's SNR is high enough (the noise power is ignorable), AN vector can be completely canceled and the AN-aided signals y will be transformed to either of the signal in U.

The modulation signals in U can then be used as the supervisory signals to construct training data with the inputs of AN-aided signals, for our supervised-learning algorithm. We have to point out that even in the worst scenarios to Eve, when Alice applies the AN-transmissions to the preamble part regardless of the risk of known-plaintext attack, our algorithm can still work well. Eve can simply apply our algorithm to all possible modulation schemes and identify the correct modulation schemes by comparisons, because only the results of the correct scheme will have the optimal value for the object function of the algorithm and can obtain the correct results with Cyclic Redundancy Check (CRC). The operations with different modulation schemes only introduce a linear increase in complexity which can be neglected for Eve.

B. Supervised-Learning Algorithm

In order to find a matrix w to decode the AN-aided signals, we set the following object function $J(w, \delta)$ for the supervised-learning algorithm, defined as

$$J(w, \delta) = \sum_{i=1}^{k} \sum_{j=1}^{m} \delta_{ij} d_{ij}, \tag{8}$$

where k ($0 < k \leq N_s$) is the number of sample symbols for learning and N_s is the total number of symbols in the packet. d_{ij} is the distance between the i^{th} transformed sample symbol to the j^{th} modulation signal, which is calculated as

$$d_{ij} = ||w^H y_i - u_j||^2. \tag{9}$$

$\delta \in \mathbb{B}^{k\times m}$ and its element δ_{ij} is the indicator of d_{ij} which can be calculated as

$$\delta_{ij} = \begin{cases} 1, d_{ij} = \min(d_{i1}, ..., d_{im}) \\ 0, else \end{cases} \tag{10}$$

which means only the distance between the i^{th} transformed symbol and its nearest modulation signal is counted.

We then adopt a supervised-learning algorithm to search for the decode matrix w which can minimize the $J(w, \delta)$, as shown in Algorithm 1. N in Step 1 is the maximum number of iterative calculation before terminating the algorithm. T_d in Step 2 is the threshold of distance for $J(w, \delta)$ to prevent the algorithm from converging to the local optimal value. T_d is calculated by $T_d = k\alpha\sigma_E^2$, where α is the margin factor considering the variance of noise power. ϵ_c in Step 4 is the threshold to check if $w(n)$ has been changed from previous value. Here we use the iterative calculation in our algorithm because the derivative of Boolean-valued function δ_{ij} to w is difficult to be derived directly. The details of derivative calculation in Step 3 is presented in the Appendix.

After the convergence of the algorithm, we demodulated the constellation point for each symbol to u_j where the index j is calculated by $\underset{j=1,...,m}{\operatorname{argmin}} ||w^H y_i - u_j||$, and thus decode each symbol to its information bits.

C. Offline Phase Shifting

After searching for the decode matrix and demodulation, an offline phase shifting operation is adopted to remove the effect of phase rotation which may be introduced in the supervised-learning algorithm. Phase rotation is an inherent problem in blind estimation without channel information [17]. When the modulation methods adopt phase values of constellation points to express different information bits (such as that in PSK and QAM), the phase rotation in estimation will cause a 100% Symbol Error Rate (SER) at the receiver. Taking BPSK modulation as an example and omit the noise in Eve, both the decode matrix $w^H = HG^\dagger$ and $(w')^H = e^{-j\pi}HG^\dagger$ will achieve the same minimum value of the target function in (8). However, the latter one will cause a 180 degrees phase rotation thus all symbols of bit 1 will be demodulated as 0, and vice versa, which results in a 100% SER. Since the initial value of w is random and Eve has no pre-knowledge of the channel H and G, the probability of converging to w and w' is equal, which will result in a 50% Packet Error Rate (PER) for BPSK even when there is no artificial noise.

As shown in Algorithm 2, an offline phase shifting operation is designed for all symbols in the decoded packets to remove the effect of phase rotation. CRC=1 indicates that the packet has passed the CRC check, which means all bits in the packet are the same as those transmitted from Alice. N_p is the number of candidate phases in the modulation signals (e.g. $N_p = 4$ in QPSK). We adopt a phase shift function $f(2\pi/N_p, b_j)$, which converts the bit information in the j^{th} symbol, b_j, to the shifted ones. The output of phase shift function has fixed values for a certain modulation schemes, e.g. for QPSK $f(\pi/2, 00)$=01, $f(\pi/2, 01)$=11, $f(\pi/2, 11)$=10 and $f(\pi/2, 10)$=00. The above phase shifting is performed until the correct phase which leads to the correct CRC. This operation may increase the computational complexity to a maximum of N_p times, which is an affordable linear increase to Eve, and results in a much higher success probability of attack.

Algorithm 1 Supervised learning algorithm

Initialization:
    (1) Set $n = 0$ as the calculation number
    (2) Set $c_1 = 0$ and $c_2 = 0$ as convergence indicators
    (3) Generate initial $w(n)$ randomly and normalize as $w(n) = w(n)/||w(n)||$
Step 1:
if $n > N$ **then**
    $w = w(n)$ and terminate the algorithm
else
    Calculate d_{ij} and δ_{ij} from (9) and (10)
    Calculate $J(w, \delta)$ from (8), increase $n = n + 1$
end if
Step 2:
if $J(w, \delta) < T_d$ **then**
    $c_1 = 1$
end if
Step 3: Re-calculate $w(n)$ to minimize $J(w, \delta)$ by

$$\frac{\partial J(w, \delta)}{\partial w} = 0$$

and get $w(n)$ as

$$w(n) = \left(\sum_{i=1}^{k} \sum_{j=1}^{m} \delta_{ij} y_i y_i^H \right)^{-1} \left(-\sum_{i=1}^{k} \sum_{j=1}^{m} \delta_{ij} b_j^* y_i \right),$$

Step 4:
if $||w(n) - w(n-1)|| < \epsilon_c$ **then**
    $c_2 = 1$
else
    Return to Step 1
end if
Step 5: Convergence check
if ($c_1 == 1$ and $c_2 == 1$) **then**
    $w = w(n)$ and terminate the algorithm
else
    Start from Initialization (2)
end if

IV. Simulation Results

A. Simulation Parameters

This section presented various simulation results to evaluate the performance of our proposed method, in comparison to those of the conventional one proposed in [15].

We set $N_A = N_E = 4$ and $N_B = 1$. A block fading channel was assumed where the channel gains remain the same during the transmission of one packet. Channel matrix G and H were generated randomly for each packet, and the performance of the attack method is evaluated using the average value of one thousand packets. Each packet included 100 modulated

Algorithm 2 Phase shifting algorithm

if CRC = 1 **then**
  Terminate
else
  for $i \leftarrow 1, N_p - 1$ **do**
    for $j \leftarrow 1, N_s$ **do**
      $b_j = f(\frac{2\pi}{N_p}, b_j)$
    end for
    if CRC = 1 **then**
      Terminate
    end if
  end for
end if

symbols. We set N = 1000, $\epsilon_c = 10^{-6}$ and $\alpha = 10$ for the searching algorithm in Algorithm 1. The signal power was normalized and the SNR was defined as $1/\sigma_E^2$. A packet would be received correctly only when all symbols in the packet were demodulated correctly.

B. Numerical Results

Fig. 3 compares the success probability of attack between the proposed method and the conventional clustering method, represented by dash and solid lines, respectively. The information bits were transmitted using the QPSK modulation. SNR in Eve was 40 dB and the number of sample symbols k was 50. Success probability of attack is calculated as (1 - PER) of received packets in Eve. For the fair comparisons, we also show the results when conventional method applies the offline phase shifting. As shown in Fig. 3, our proposed method largely improves success probability of attack compared to the conventional one, from 4.8% to 95.8% in Pr=0.1, and from 4.3% to 72.2% in Pr=0.5, which is usually considered as the optimal power ratio of AN [8].

We also show the comparison of the proposed method and the conventional one with different modulation schemes in Fig. 4. From the results in Figs. 3 and 4, we can see that when Eve adopts our attack method, the AN transmission with low order modulation such as BPSK and QPSK can be cracked in a high probability. This means AN fails to keep its independence to the Eve's channel status, and the transmission to the receiver in the cell-edge with low order modulation will be cracked if the Eve's channel is good enough. Therefore, in order to guarantee secure communication, the transmitter needs to increase artificial noise power as well as adopting higher order modulation for the information vector. This will largely decrease the coverage area compared to the traditional wireless services which do not consider security in physical layer, thus become an essential problem towards AN's realization.

Fig. 5 shows the dependence on the number of Eve's antennas. One can see that increasing the number of Eve's antennas causes degradation in conventional method's attack performance. This is probably because the increase in N_E also increases the dimensions of received signals, which in turn increases the probability of achieving the local optimal values in conventional clustering method, thus fails to find the

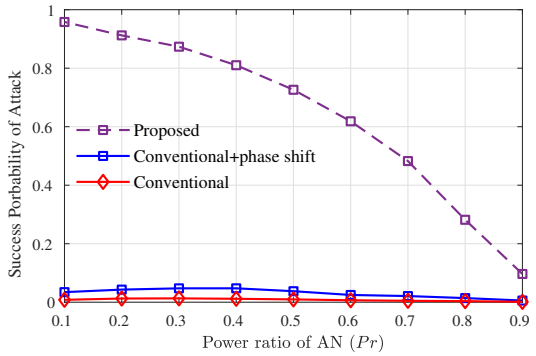

Fig. 3. Comparison of success probability of attack (QPSK).

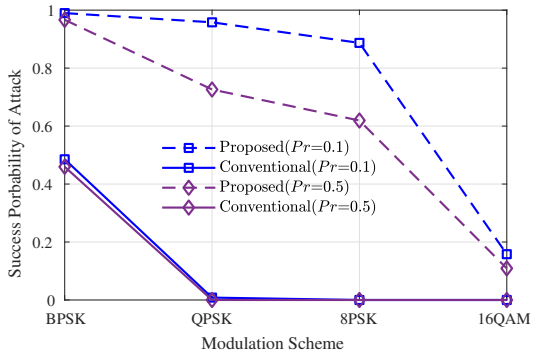

Fig. 4. Success probability of attack with different modulation schemes.

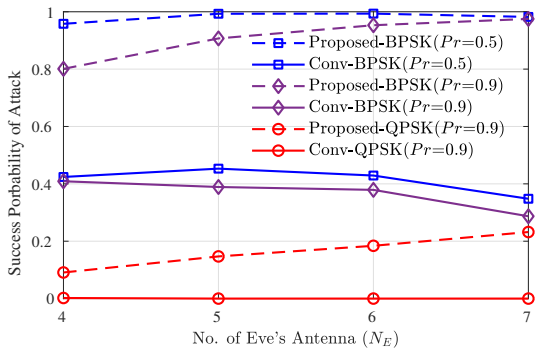

Fig. 5. Success probability of attack vs number of Eve's antennas

decode matrix. While in our proposed method, the increase in N_E results in an improvement of success probability of attack. It indicates our proposed method can utilize the resource in Eve more efficiently thus achieve higher attack performance.

The results with different number of sample symbols k are shown in Fig. 6. Our proposed method outperforms the conventional one on all accounts. Since the performances of both the proposed method and the conventional method show dependence on the number of sample symbols, which can be considered as an inherent nature of machine learning algorithm, AN transmission can only provide secure communication under certain conditions if the transmitted packet is sufficiently short.

V. Conclusion

This paper proposes a machine learning-based attack method against AN-aided transmissions. Our method utilizes the modulation scheme information from the packet preamble

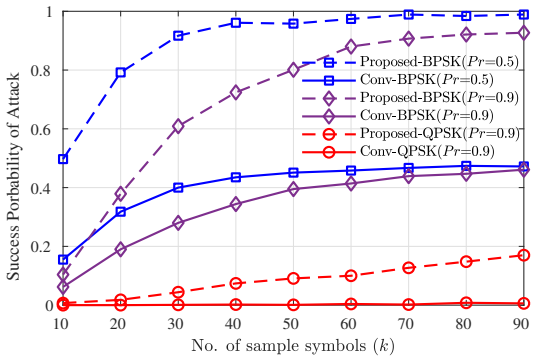

Fig. 6. Success probability of attack with different number of sample symbols.

and header to build the supervisory signals, with which a supervised-learning algorithm is developed for eavesdropper to estimate the channel between transmitter and receiver for decoding the AN-aided packets, followed by a phase shift operation to remove the effect of phase rotation. Numerous simulation results show that our method can improve success probability of attack from 4.8% to at most 95.8% for QPSK modulation. This implies that if the eavesdropper adopts our attack method, AN transmission fails to keep its independence to the eavesdropper's channel status, and the transmission to the receiver in the cell-edge with low order modulation will be cracked if the eavesdropper employs more antennas than the transmitter. Our attack method can bring a fresh view on the evaluation of AN schemes and motivate researchers to design more robust PLS approaches. Our future work will conduct experimental evaluation of the proposed attack method. We also intend to develop a novel AN scheme which is robust against the machine learning attacks.

ACKNOWLEDGMENT

The authors would like to acknowledge the immense support of the University of Surrey 5GIC. We also acknowledge members in Department of Electrical Engineering and Electronics of the University of Liverpool for their constructive advices and comments.

APPENDIX

The detailed expression of the $\frac{\partial J(w,\delta)}{\partial w}$ in Step 3 of our Algorithm 1 is given as

$$\frac{\partial J(w,\delta)}{\partial w} = \frac{\sum_{i=1}^{k}\sum_{j=1}^{m}\partial(\delta_{ij}d_{ij})}{\partial w}. \tag{11}$$

As δ_{ij} is a Boolean-valued function which depends on the comparison between different d_{ij}, it is difficult to directly derive its derivative to w. Therefore, we consider it to be a constant number to w so as to simplify the (11) using only $\frac{\partial d_{ij}}{\partial w}$, which can be calculated as

$$\begin{aligned}\frac{\partial d_{ij}}{\partial w} =& \frac{\partial(Tr\{(w^H y+b_j)^H(w^H y+b_j)\})}{\partial w}\\ =& \frac{\partial(Tr\{y^H w w^H w\})}{\partial w}+\frac{\partial(Tr\{y^H w b_j\})}{\partial w}+\\ & \frac{\partial(Tr\{b_j^H w^H y\})}{\partial w}+\frac{\partial(Tr\{b_j^H b_j\})}{\partial w}\\ =&(yy^H)^T w^* + (b_j y^H)^T + 0 + 0. \end{aligned}\tag{12}$$

With (11) and (12), we can calculate $\frac{\partial J(w,\delta)}{\partial w}=0$ as follows:

$$\sum_{i=1}^{k}\sum_{j=1}^{m}\delta_{ij}(yy^H)^T w^* + \sum_{i=1}^{k}\sum_{j=1}^{m}\delta_{ij}(b_j y^H)^T = 0. \tag{13}$$

By moving the second term in (13) to the right side of the equation and performing conjugate operation on both sides, we can derive w which can minimize the $J(w,\delta)$ as

$$w(n) = \left(\sum_{i=1}^{k}\sum_{j=1}^{m}\delta_{ij}y_i y_i^H\right)^{-1}\left(-\sum_{i=1}^{k}\sum_{j=1}^{m}\delta_{ij}b_j^* y_i\right), \tag{14}$$

which is the expression shown in Step 3 of the Algorithm 1.

REFERENCES

[1] G. Liu and D. Jiang, "5G: Vision and requirements for mobile communication system towards year 2020," *Chinese Journal of Engineering*, vol. 2016, 2016.

[2] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, 2017.

[3] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 2017.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, 2008.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—part ii: The mimome wiretap channel," *IEEE Trans. Inf. Theory*, vol. 11, no. 56, pp. 5515–5532, 2010.

[6] H. Reboredo, J. Xavier, and M. R. Rodrigues, "Filter design with secrecy constraints: The mimo gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, 2013.

[7] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, 2010.

[8] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, 2016.

[9] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, 2015.

[10] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, 2015.

[11] F. Wu, W. Wang, B. Yao, and Q. Yin, "Effective eavesdropping in the artificial noise aided security scheme," in *Proc. IEEE/CIC Int. Conf. Communications in China (ICCC)*, 2013, pp. 214–218.

[12] A. Hyvärinen, "Independent component analysis: recent advances," *Phil. Trans. R. Soc. A*, vol. 371, no. 1984, p. 20110534, 2013.

[13] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless mimo systems." in *Proc. NDSS*, 2014.

[14] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 34–37, 2015.

[15] L. Liu, J. Liang, and K. Huang, "Eavesdropping against artificial noise: hyperplane clustering," in *Proc. Int. Conf. Information Science and Technology (ICIST)*, 2013, pp. 1571–1575.

[16] "IEEE standard for information technology–telecommunications and information exchange between systems–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments," Tech. Rep., 2013.

[17] P. Campisi, G. Panci, S. Colonnese, and G. Scarano, "Blind phase recovery for qam communication systems," *IEEE Trans. Signal Process.*, vol. 53, no. 4, pp. 1348–1358, 2005.