Deep Learning-Based Proactive Eavesdropping for Wireless Surveillance

Jihwan Moon, Sang Hyun Lee, *Member*, *IEEE*, †Hoon Lee, *Member*, *IEEE*,
Seunghwan Baek and Inkyu Lee, *Fellow*, *IEEE*
School of Electrical Eng., Korea University, Seoul, Korea
†Department of Information and Communications Engineering, Pukyong National University, Busan, Korea
Email: {anschino, sanghyunlee, s_baek, inkyu}@korea.ac.kr, †hlee@pknu.ac.kr

***Abstract*—In this work, we investigate a proactive eavesdropping system where a central monitor covertly wiretaps the communications between a pair of suspicious users via multiple intermediate nodes. For successful eavesdropping, it is required that the eavesdropping channel capacity is higher than the data rate of the suspicious users so that the central monitor can reliably decode the intercepted information. Hence, the intermediate nodes operate in two different modes, namely eavesdropping mode and jamming mode, to facilitate eavesdropping. Specifically, the eavesdropping nodes forward the intercepted data from the suspicious users to the central monitor, while the jamming nodes transmit jamming signals to proactively control the data rate of the suspicious users. We propose an efficient deep learning-based approach to identify the optimal mode selection for the intermediate nodes and the optimal transmit power for the jamming nodes. Numerical results confirm the significant performance gain of our proposed method both in terms of performance and time complexity over conventional schemes.**

***Index Terms*—Deep learning, deep neural network, physical layer security, proactive eavesdropping, wireless surveillance, cooperative jamming.**

I. Introduction

Recently, *proactive eavesdropping* has started to draw interest as a new paradigm in wireless surveillance [1]. In this framework, legitimate monitors attempt to eavesdrop on suspicious users who are deemed to misuse communication infrastructures for illegal activities. It is worth noting that conventional works in physical layer security have often treated eavesdroppers as illegitimate users and have put great efforts on preventing information leaks [2]–[8]. In contrast, proactive eavesdropping reverses this point of view such that eavesdroppers are considered as legitimate monitors for the purpose of wireless surveillance. The main objective of the proactive eavesdropping is to overhear as much information as possible from suspicious users.

A basic proactive eavesdropping system model was proposed by [9] and [10] in which a legitimate monitor tries to intercept information between a suspicious pair. A key requirement for successful eavesdropping is to ensure that the data rate of the suspicious users is lower than the eavesdropping channel capacity in a way that the intercepted information can be reliably decoded from an information theoretic perspective. To this end, the legitimate monitor proactively controls the data rate of the suspicious users by jamming under the assumption that the suspicious users adaptively adjust their data rate based on the perceived channel quality.

This work was supported by the National Research Foundation through the Ministry of Science, ICT, and Future Planning (MSIP), Korean Government under Grant 2017R1A2B3012316.

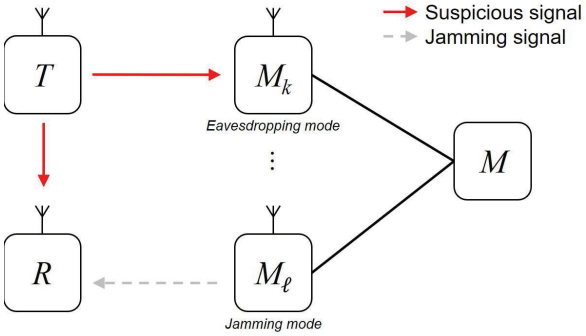

Fig. 1. Schematic diagram of the proposed proactive eavesdropping system

In [11], the single-antenna systems in [9] and [10] were extended to a scenario with a multi-antenna legitimate monitor. Wireless surveillancve of two-hop systems was studied in [12]–[14] where a relay facilitates the communications between the suspicious transmitter and receiver. The authors in [15] and [16] investigated proactive eavesdropping in orthogonal frequency division multiplexing (OFDM) based suspicious links. In addition, a new eavesdropping method by spoofing was introduced by [17] to further improve the eavesdropping performance.

However, all the works so far have assumed that the legitimate monitor has a direct link from eavesdropping targets. This assumption may be overly optimistic if the legitimate monitor wishes to covertly eavesdrop without being detected by the suspicious users. In line with these considerations, the recent works in [18]–[20] proposed relay-aided proactive eavesdropping systems. A central monitor in the absence of a direct eavesdropping link to suspicious users utilizes intermediate nodes for relay and jamming operations to enable distant eavesdropping. Still, these works have considered a situation where each node has a fixed operation only as an eavesdropper or jammer and does not change its mode. We may take advantage of mode switching between eavesdropping and jamming for the intermediate nodes to enhance the eavesdropping performance even more.

In this work, we study a legitimate proactive eavesdropping scenario where multiple intermediate nodes can either eavesdrop or jam by switching its mode to improve eavesdropping

978-1-5386-8088-9/19/$31.00 ©2019 IEEE

performance. The eavesdropping nodes forward the intercepted data from the suspicious users to the central monitor, while the jamming nodes transmit jamming signals to control the data rate of the suspicious users. Our goal is to optimize the mode selection and the transmit power of the intermediate nodes to achieve the maximum eavesdropping rate.

Generally, selection problems are difficult to solve due to its discrete nature which often requires a means of exhaustive search methods for the optimal solution. Meanwhile, the recent advancement in deep learning (DL) has paved the way for solving various classification tasks that had previously been considered unsolvable [21]. DL exploits deep neural network (DNN) architectures so that the complicated relationship between an input and the optimal output can be effectively learned. We thus leverage this powerful classification ability of the DL to provide the optimal mode selection as well as the optimal transmit power of the jamming nodes. Numerical results validate the efficiency of the proposed DL strategy in various system setups.

The rest of this paper is organized as follows: The proposed system model and the problem formulation are described in Section II. Then, the DL-based approach for the problem is discussed in Section III. Numerical results are compared in Section IV, and we conclude the paper in Section V.

Notations: We define $|a|$ and $\|\mathbf{a}\|$ as the absolute value of scalar a and the Frobenius norm of vector $\mathbf{a}$, respectively. Let $|\mathcal{A}|$ be the cardinality of set $\mathcal{A}$. Also, we define $\mathbf{A}^{-1}$ and $|\mathbf{A}|$ as the inverse and the determinant of matrix $\mathbf{A}$, respectively. $\mathcal{CN}\left(\mu,\sigma^2\right)$ denotes a circularly symmetric complex Gaussian distribution with mean μ and variance σ^2. Lastly, $\mathbf{I}_K$ indicates a $K\times K$ identity matrix.

II. System Model

Fig. 1 depicts the proposed proactive eavesdropping system with a suspicious transmitter T, a suspicious receiver R, a central monitor C, and K intermediate nodes M_k for $k=1,...,K$. We assume that the suspicious users are equipped with a single antenna and employ an adaptive transmission policy in which their data rate is adjusted according to the effective channel condition at the receiver [9]–[11], [17].

Let $\mathcal{K}_E$, $\mathcal{K}_J$, and $\mathcal{K}=\{1,2,...,K\}$ denote the set of indices for eavesdropping nodes, jamming nodes and all the intermediate nodes, respectively, such that $\mathcal{K}=\mathcal{K}_E\cup\mathcal{K}_J$ and $\mathcal{K}_E\cap\mathcal{K}_J=\emptyset$. Defining h_{XY} as the complex channel coefficient from node X to node Y where $\mathsf{X},\mathsf{Y}\in\{T,R,C,M_k\}$, the received signal at the k-th eavesdropping node for $k\in\mathcal{K}_E$ can be expressed as

$$y_{M_k}=h_{TM_k}x_T+\sum_{\ell\in\mathcal{K}_J}h_{M_\ell M_k}x_{M_\ell}+z_{M_k},\ \forall k\in\mathcal{K}_E, \quad (1)$$

where $x_T\sim\mathcal{CN}\left(0,P_T\right)$ and $x_{M_\ell}\sim\mathcal{CN}\left(0,P_{M_\ell}\right)$ denote the transmit signals from the suspicious transmitter and the ℓ-th jamming node, respectively, and $z_{M_k}\sim\mathcal{CN}\left(0,\sigma^2_{M_k}\right)$ represents the additive noise at the k-th eavesdropping node. It is assumed that global channel state information (CSI) is available at the central monitor and the intermediate nodes, while the suspicious users are unaware of being eavesdropped and only have its mutual CSI h_{TR} [1] [17]. Also, we assume that jamming interference $\sum_{\ell\in\mathcal{K}_J}h_{M_\ell M_k}x_{M_\ell}$ in (1) can be removed by sharing an identical codebook of jamming signals with specific individual orders among the intermediate nodes [7] [22].

The k-th eavesdropping node then forwards the received signal y_{M_k} to the central monitor through fiber links. In the presence of finite capacity on the links, each eavesdropping node performs compress-and-forward (CF) and quantizes its received signal y_{M_k} before transferring to the central monitor so that the central monitor can successfully decode information [23]. It has been shown in [23] that the successfully decompressed signal at the central monitor can be modelled as $\hat{y}_{M_k}=y_{M_k}+q_{M_k}$ where $q_{M_k}\sim\mathcal{CN}\left(0,Q_{M_k}\right)$ indicates the quantization noise of the k-th eavesdropping node if the mutual information $\mathrm{I}\left(y_{M_k};\hat{y}_{M_k}\right)$ between y_{M_k} and $\hat{y}_{M_k}$ is smaller than the channel capacity $\bar{r}_{M_k}$ from the k-th eavesdropping node to the central monitor, i.e.,

$$\mathrm{I}\left(y_{M_k};\hat{y}_{M_k}\right)\triangleq\log_2\left(1+\frac{\left|h_{TM_k}\right|^2P_T+\sigma^2_{M_k}}{Q_{M_k}}\right)\leq\bar{r}_{M_k},\ \forall k\in\mathcal{K}_E. \quad (2)$$

The received signal vector $\hat{\mathbf{y}}_E\in\mathbb{C}^{|\mathcal{K}_E|\times1}$ can be written by

$$\hat{\mathbf{y}}_E=\mathbf{h}_{TE}x_T+\mathbf{z}_E+\mathbf{q}_E, \quad (3)$$

where $\mathbf{h}_{TE}\in\mathbb{C}^{|\mathcal{K}_E|\times1}$, $\mathbf{z}_E\in\mathbb{C}^{|\mathcal{K}_E|\times1}$ and $\mathbf{q}_E\in\mathbb{C}^{|\mathcal{K}_E|\times1}$ represent vectors constructed by collecting $\left\{h_{TM_k}\right\}_{k\in\mathcal{K}_E}$, $\left\{z_{M_k}\right\}_{k\in\mathcal{K}_E}$ and $\left\{q_{M_k}\right\}_{k\in\mathcal{K}_E}$, respectively, in increasing order of index k. Then, the resulting eavesdropping channel capacity r_C of the central monitor is given as

$$r_C=\log_2\left|\mathbf{I}_{|\mathcal{K}_E|}+P_T\mathbf{Z}^{-1}\mathbf{h}_{TE}\mathbf{h}_{TE}^H\right|=\log_2\left(1+P_T\mathbf{h}_{TE}^H\mathbf{Z}^{-1}\mathbf{h}_{TE}\right), \quad (4)$$

where $\mathbf{Z}\in\mathbb{R}^{|\mathcal{K}_E|\times|\mathcal{K}_E|}$ represents a diagonal matrix with diagonal elements $\left\{\sigma^2_{M_k}+Q_{M_k}\right\}_{k\in\mathcal{K}_E}$.

As for the suspicious receiver, the received signal becomes

$$y_R=h_{TR}x_T+\sum_{\ell\in\mathcal{K}_J}h_{M_\ell R}x_{M_\ell}+z_R, \quad (5)$$

where $z_R\sim\mathcal{CN}\left(0,\sigma^2_R\right)$ indicates the additive noise at the suspicious receiver. The achievable data rate of the suspicious user pair is thus obtained by

$$r_R=\log_2\left(1+\frac{\left|h_{TR}\right|^2P_T}{\sum_{\ell\in\mathcal{K}_J}\left|h_{M_\ell R}\right|^2P_{M_\ell}+\sigma^2_R}\right), \quad (6)$$

and the eavesdropping rate is defined in [1] [9] by

$$r_e=\begin{cases}r_R & , \text{ if } r_C\geq r_R,\\ 0 & , \text{ otherwise.}\end{cases} \quad (7)$$

We then formulate the eavesdropping rate maximization problem as

$$\text{(P):}\ \max_{\mathcal{K}_E,\{Q_{M_k}\},\mathcal{K}_J,\{P_{M_k}\}}\ r_e \quad (8a)$$

$$\text{subject to}\quad \mathrm{I}\left(y_{M_k};\hat{y}_{M_k}\right)\leq\bar{r}_{M_k},\ \forall k\in\mathcal{K}_E, \quad (8b)$$

$$0\leq P_{M_k}\leq\bar{P}_{M_k},\ \forall k\in\mathcal{K}. \quad (8c)$$

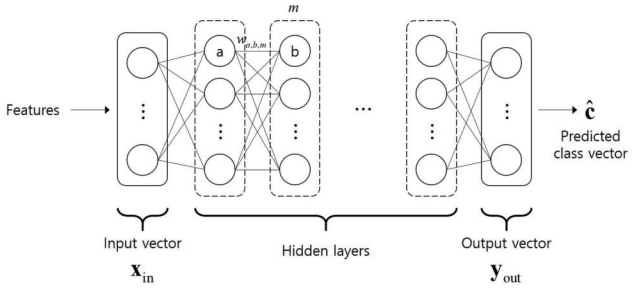

Fig. 2. An architecture of feedforward DNN

In (P), we determine the eavesdropping node set $\mathcal{K}_E$ and the jamming node set $\mathcal{K}_J$ and optimize the quantization levels $\{Q_{M_k}\}$ and the transmit power $\{P_{M_k}\}$ to maximize the eavesdropping rate r_e. We also desire to fulfill the limited capacity condition of the fiber links in (8b) while maintaining the transmit power of the intermediate nodes below the maximum allowed budget $\bar{P}_{M_k}$ as in (8c). In what follows, we provide a DL based algorithm to obtain the optimal solutions.

III. DL Based Optimal Solution

To begin with, (P) is first reformulated as

$$\text{(P.1)}: \min_{\substack{\mathcal{K}_E,\{Q_{M_k}\},\\ \mathcal{K}_J,\{P_{M_\ell}\}}} \sum_{\ell\in\mathcal{K}_J} \left|h_{M_\ell R}\right|^2 P_{M_\ell} \tag{9a}$$

$$\text{s.t.} \sum_{k\in\mathcal{K}_E} \frac{\left|h_{TM_k}\right|^2}{\sigma^2_{M_k}+Q_{M_k}} \geq \frac{|h_{TR}|^2}{\sum\limits_{\ell\in\mathcal{K}_J}\left|h_{M_\ell R}\right|^2 P_{M_\ell}+\sigma^2_R}, \tag{9b}$$

$$\frac{1}{\sigma^2_{M_k}+Q_{M_k}} \leq \frac{2^{\bar{r}_{M_k}}-1}{\sigma^2_{M_k}2^{\bar{r}_{M_k}}+\left|h_{TM_k}\right|^2 P_T}, \ \forall k\in\mathcal{K}_E, \tag{9c}$$

$$0 \leq P_{M_\ell} \leq \bar{P}_{M_\ell}, \ \forall \ell\in\mathcal{K}_J, \tag{9d}$$

where (9b) comes from the fact that $\mathbf{h}^H_{TE}\mathbf{Z}^{-1}\mathbf{h}_{TE} = \left\|\mathbf{Z}^{-1/2}\mathbf{h}_{TE}\right\|^2 = \sum_{k\in\mathcal{K}_E}\frac{\left|h_{TM_k}\right|^2}{\sigma^2_{M_k}+Q_{M_k}}$. Since $\left|h_{TM_k}\right|^2 \geq 0$ and $Q_{M_k} \geq 0$, (9b) and (9c) imply that the optimal $Q^\star_{M_k}$ should be set to

$$Q^\star_{M_k} = \frac{\sigma^2_{M_k}2^{\bar{r}_{M_k}} + \left|h_{TM_k}\right|^2 P_T}{2^{\bar{r}_{M_k}}-1} - \sigma^2_{M_k}, \tag{10}$$

such that the equality holds in (9c).

It is still not straightforward to solve (P.1) optimally since it involves discrete optimization variables $\mathcal{K}_E$ and $\mathcal{K}_J$ as well as continuous optimization variables $\{P_{M_k}\}$. Finding the optimal solutions $\mathcal{K}^\star_E$ and $\mathcal{K}^\star_J$ in general incurs an exhaustive search process over 2^K candidates. Hence, we propose a two-step approach for (P.1) in which we train a DNN to first provide the optimal mode selection $\mathcal{K}^\star_E$ and $\mathcal{K}^\star_J$ when given system parameters are fed in. Subsequently, the transmit power $\{P_{M_\ell}\}_{\ell\in\mathcal{K}^\star_J}$ for the jamming nodes is optimized based on the obtained $\mathcal{K}^\star_E$ and $\mathcal{K}^\star_J$.

A. Optimal mode selection $\mathcal{K}^\star_E$ and $\mathcal{K}^\star_J$

Let us first illustrate a method to obtain the optimal mode selection variables $\mathcal{K}^\star_E$ and $\mathcal{K}^\star_J$ with DL. An architecture of a feedforward DNN is shown in Fig. 2 which consists of three parts; an input vector $\mathbf{x}_{\text{in}}$, hidden layers and an output vector $\mathbf{y}_{\text{out}}$ [21]. $w_{a,b,m}$ represents the weight parameter between neuron a in the $(m-1)$ hidden layer and neuron b in the m-th hidden layer. We define $\mathcal{S}_{\text{train}}$ as a train set that comprises N_{train} train sample vectors $\{\mathbf{x}_{\text{train},i}\}$ and the corresponding one-hot correct class vectors $\{\mathbf{c}_{\text{train},i}\}$ for $i = 1, ..., N_{\text{train}}$. For a N_{class}-classification task, an ideal DNN should be able to predict the correct class vector $\mathbf{c}_{\text{train},i}$ when $\mathbf{x}_{\text{train},i}$ is fed in.

A DNN is trained by a number of iterations of *feedforward* and *backpropagation*. During the feedforward stage, the DNN takes a batch of N_{batch} train samples $\{\mathbf{x}_{\text{train},i}\}$ as input, which then propagate through the hidden layers with $\{w_{a,b,m}\}$. Specifically, a neuron in each hidden layer takes a weighted sum of the outputs from the neurons in the previous layer and performs a specified transformation such as sigmoid, tanh or rectified linear unit (ReLU) [24].

At the last hidden layer, a softmax transformation is implemented on the neurons to provide predicted class vectors $\{\hat{\mathbf{c}}_{\text{train},i}\}$. Note that $\hat{\mathbf{c}}_{\text{train},i}$ is obtained by setting the $n_{\max}$-th element as one and the others as zeros, where $n_{\max}$ corresponds to the index of the largest element in $\mathbf{y}_{\text{out},i}$. Hence, a valid loss function $\mathcal{L}$ which measures the difference between the prediction $\hat{\mathbf{c}}_{\text{train},i}$ and the correct class vector $\mathbf{c}_{\text{train},i}$ is given by

$$\mathcal{L} = -\sum_{i=1}^{N_{\text{batch}}}\sum_{n=1}^{N_{\text{class}}} c_{\text{train},i,n}\log\left(y_{\text{out},i,n}\right), \tag{11}$$

where $y_{\text{out},i,n}$ and $c_{\text{train},i,n}$ are the n-th elements in $\mathbf{y}_{\text{out},i}$ and $\mathbf{c}_{\text{train},i}$, respectively.

In the backpropagation stage, the weight parameters $\{w_{a,b,m}\}$ in the hidden layers are optimized by a stochastic gradient descent method so that $\mathcal{L}$ is minimized. Precisely, if α denotes a learning rate, each $\{w_{a,b,m}\}$ is updated by

$$w_{a,b,m} \leftarrow w_{a,b,m} - \alpha\frac{\partial\mathcal{L}}{\partial w_{a,b,m}}. \tag{12}$$

It now remains to design the input vector $\mathbf{x}_{\text{in}}$ and the output vector $\mathbf{y}_{\text{out}}$ for our considered system. From (P.1), $\mathbf{x}_{\text{in}}$ should include channel gains $|h_{TR}|^2$, $\left\{\left|h_{M_\ell R}\right|^2\right\}$, $\left\{\left|h_{TM_k}\right|^2\right\}$ as well as $\left\{Q^\star_{M_k}\right\}$ and $\left\{\bar{P}_{M_k}\right\}$ as features. However, it is worth noting that they may greatly vary in magnitude. This results in an imbalance among the features since the DNN can fail to capture the significance of features with small magnitudes. Therefore, $\mathbf{x}_{\text{in}}$ must be carefully designed before fed into the hidden layers by normalization so that the elements in $\mathbf{x}_{\text{in}}$ are in similar scales.

Besides, manipulation of features for $\mathbf{x}_{\text{in}}$, as known as *feature processing* [25], also plays a key role in building an effective DNN. Fig. 3 reveals the prediction performance of a DNN with different feature processing for $K = 4$. In this experiment, feature processing 1 directly uses $\mathbf{x}_{\text{feature},1} = [|h_{TR}|^2, \{\left|h_{M_\ell R}\right|^2\}, \{\left|h_{TM_k}\right|^2\}, \{Q^\star_{M_k}\}, \{\bar{P}_{M_k}\}]^T$ as $\mathbf{x}_{\text{in}}$. We can see from the figure that the prediction accuracy is the worst with this simplest type of feature processing. Meanwhile, feature processing 2 combines h_{TM_k} and $Q^\star_{M_k}$ such that

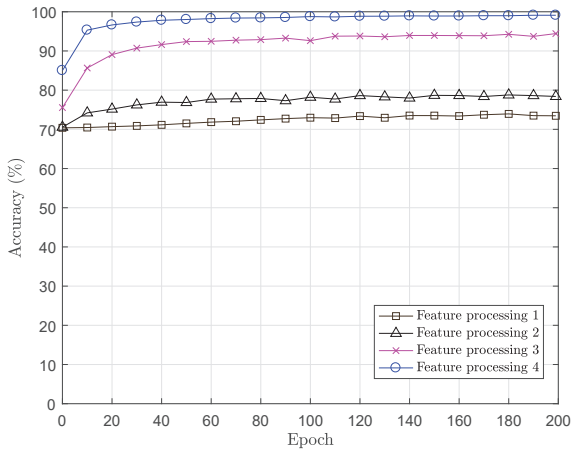

Fig. 3. Prediction accuracy of DNN with different feature processing

$\mathbf{x}_{\text{feature},2} = [|h_{TR}|, \left\{\frac{|h_{M_\ell R}|^2}{|h_{TR}|}\right\}, \left\{\frac{|h_{TM_k}|^2}{|h_{TR}|(\sigma^2_{M_k}+Q^\star_{M_k})}\right\}, \{\bar{P}_{M_k}\}]^T$ is set for $\mathbf{x}_{\text{in}}$. This design is motivated by the structure of constraint (9b) in (P.1) and has seen an improvement of more than 5% in the DNN performance. Even more enhancements are observed with additional non-linear transformations as feature selection 3 and 4 where $\mathbf{x}_{\text{feature},3} = \sqrt{\mathbf{x}_{\text{feature},2}}$ and $\mathbf{x}_{\text{feature},4} = \log(\mathbf{x}_{\text{feature},2})$, respectively. From the figure, the logarithmic transformation by feature processing 4 yields the best prediction performance which achieves nearly 100%. We thus conclude that an adequate feature processing and normalization for $\mathbf{x}_{in}$ is important for training an accruate DNN.

As for the one-hot encoded output vector $\mathbf{y}_{\text{out}}$, it should be able to infer the optimal mode selection from all possible 2^{K-1} candidates. Hence, we assign each correct class vector $\mathbf{c}_{\text{train},i}$ to a unique mode selection. The dimensions of $\mathbf{y}_{\text{out}}$ as well as $\mathbf{c}_{\text{train},i}$ are 2^{K-1} to express 2^{K-1} different mode selections. Note that $\{\mathbf{c}_{\text{train},i}\}$ for train set $\mathcal{S}_{\text{train}}$ can be collected by performing an exhaustive search method for corresponding $\{\mathbf{x}_{\text{train},i}\}$ in offline. After training, the optimal $\mathcal{K}_E^\star$ and $\mathcal{K}_J^\star$ can easily be inferred from the accurately predicted class vector $\hat{\mathbf{c}}$.

B. Optimal jamming transmit power $P^\star_{M_\ell}$

We now optimize the transmit power of the jamming nodes based on the optimal mode selection $\mathcal{K}_E^\star$ and $\mathcal{K}_J^\star$. In this case, (P.1) can be recast to

$$\text{(P.2)}: \min_{\{P_{M_\ell}\}} \quad \sum_{\ell\in\mathcal{K}_J^\star} |h_{M_\ell R}|^2 P_{M_\ell} \tag{13a}$$

$$\text{subject to} \quad \sum_{\ell\in\mathcal{K}_J^\star} |h_{M_\ell R}|^2 P_{M_\ell} \geq \frac{|h_{TR}|^2}{\sum\limits_{k\in\mathcal{K}_E^\star} \frac{|h_{TM_k}|^2}{\sigma^2_{M_k}+Q^\star_{M_k}}} - \sigma_R^2, \tag{13b}$$

$$0 \leq P_{M_\ell} \leq \bar{P}_{M_\ell}, \ \forall \ell \in \mathcal{K}_J^\star, \tag{13c}$$

Note that (P.2) belongs to linear programming with respect to $\left\{P_{M_\ell}\right\}$, and existing efficient algorithms such as the simplex method [26] can readily solve for the optimal solutions $\left\{P^\star_{M_\ell}\right\}$. The overall algorithm for solving (P.1) is summarized in Algorithm. 1.

Algorithm 1: DL based optimal solution for (P.1)

Offline:
Load a train set $\mathcal{S}_{\text{train}}$ with N_{train} train sample vectors $\{\mathbf{x}_{\text{train},i}\}$ and the correct class vectors $\{\mathbf{c}_{\text{train},i}\}$.
Train the DNN by the method in Section III-A.

Online:
Obtain $\mathcal{K}_E^\star$ and $\mathcal{K}_J^\star$ by the offline trained DNN.
Solve for $\left\{P^\star_{M_\ell}\right\}$ by (P.2).

IV. Numerical Results

In this section, the performance of the proposed algorithm is evaluated from numerical simulations. We adopt the channel model $|h_{\mathsf{XY}}|^2 = L_{\mathsf{XY}} \left|\hat{h}_{\mathsf{XY}}\right|^2$, $\forall \mathsf{X},\mathsf{Y} \in \{T, R, C, M_k, \forall k\}$, where $L_{\mathsf{XY}} \triangleq L_0 \left(\frac{d_{\mathsf{XY}}}{d_0}\right)^{-\beta}$ is defined by the distance-dependent path loss between X and Y [7]. Here, L_0 stands for the path loss at reference distance d_0, β represents the path loss exponent, and d_{XY} indicates the distance between X and Y. Also, the small-scale channel variable $\hat{h}_{\mathsf{XY}}$ follows an independent complex Gaussian distribution with zero mean and unit variance. We set $L_0 = 10^{-3}$, $d_0 = 1$ m and $\beta = 3.5$.

The suspicious receiver is randomly placed with a fixed distance d_{TR} from the suspicious transmitter. Also, the k-th intermediate node are randomly located from the suspicious transmitter with distance d_{TM_k}. Moreover, we fix the system bandwidth as $W = 20$ MHz, the transmit power at the suspicious transmitter as $P_T = 23$ dBm, the transmit power at the k-th intermediate node as $\bar{P}_{M_k} = 23$ dBm, and the thermal noise variance as -170 dBm/Hz.

Table 1: DNN parameters

Number of train samples:	$190,000$
Layers and neurons:	$K=2$: $[16, 2^K-1]$ $K=3$: $[256, 2^K-1]$ $K=4$: $[64, 64, 2^K-1]$ $K=5$: $[128, 128, 2^K-1]$ $K=6$: $[128, 128, 2^K-1]$
Activations:	ReLU
Minibatch size:	1024
Parameter update:	ADAM [27]
Learning rate	0.001
Epochs	200

Parameters related to DNN are summarized in Table 1. The DNN is trained with train set $\mathcal{S}_{\text{train}}$ where each train sample $\mathbf{x}_{\text{train},i}$ and the corresponding correct class vectors $\mathbf{c}_{\text{train},i}$ are collected from randomly drawn system configuration of $d_{TR} \in [1\text{ m}, 200\text{ m}]$, $d_{TM_k} \in [1\text{ m}, 100\text{ m}]$, $P_T \in [0\text{ dBm}, 50\text{ dBm}]$, $\bar{P}_{M_k} \in [0\text{ dBm}, 50\text{ dBm}]$ and $\bar{r}_{M_k} \in [1\text{ bps/Hz}, 15\text{ bps/Hz}]$. The logarithmic non-linear feature processing in Section III-A is adopted for our numerical results. We compare our proposed schemes with *Optimal*, where an exhaustive search

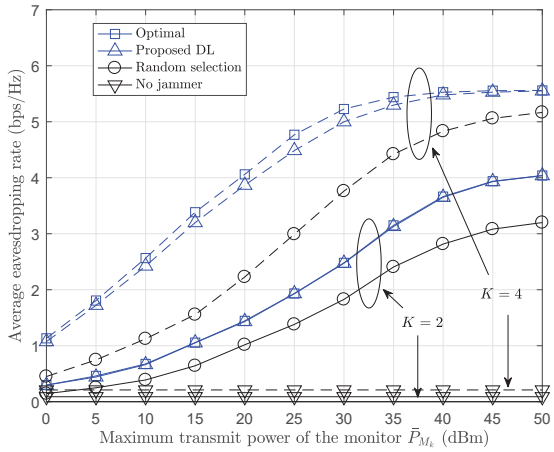

Fig. 4. Average eavesdropping rate as a function of $\bar{P}_{M_k}$

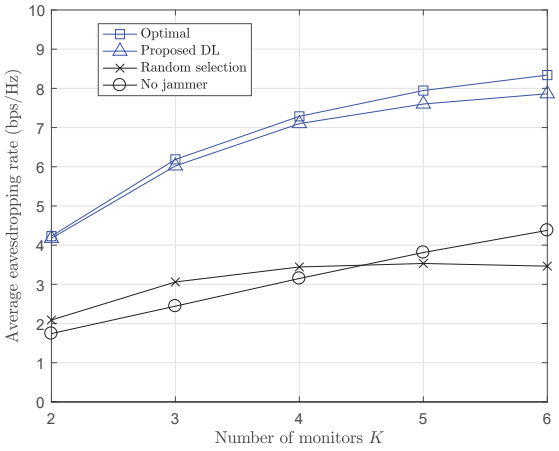

Fig. 5. Average eavesdropping rate as a function of K

is employed for finding the optimal operation modes, with *Random selection*, in which one intermediate node is randomly selected as a jamming node, and with *No jammer*, where every intermediate node operates in the eavesdropping mode. The performance is averaged over 10000 different node placements and small-scale channel coefficients in the subsequent figures.

Fig. 4 illustrates the average eavesdropping rate as a function of the maximum transmit power $\bar{P}_{M_k}$ with $K = 2$ and 4. The link capacity $\bar{r}_{M_k}$ equals 5 bps/Hz for $k \in \mathcal{K}$, d_{TR} is set by 50 m and d_{TM_k} is randomly chosen between 1 m and 300 m. Our proposed DL method shows a remarkable performance gain compared to non-optimized ones such as the random selection and the no jammer schemes. At $\bar{P}_{M_k} = 30$ dBm, the DL method outperforms the random selection by 35% and 38% when $K = 2$ and 4, respectively. It is also verified that the DL method is near-optimal for all values of $\bar{P}_{M_k}$. We see that the no jammer scheme does not achieve any meaningful eavesdropping rate, which emphasizes the significance of jamming nodes for the maximum performance.

Fig. 5 exhibits the average eavesdropping rate of different schemes as a function of the number of intermediate nodes

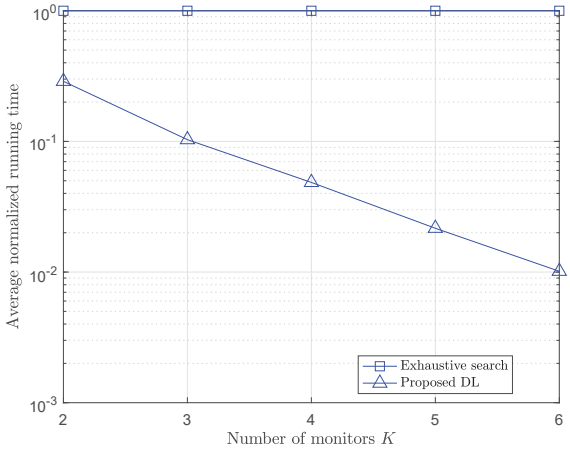

Fig. 6. Average normalized running time as a function of K

K with $\bar{r}_{M_k} = 10$ bps/Hz. The eavesdropping performance steadily improves with the number of intermediate nodes. We can also confirm that the proposed DNN architecture provides near-optimal mode selections for all K. In addition, the result shows that the DL method outperforms the random selection by more than 100% for $K = 4$. This clearly highlights the need of careful mode selections among the intermediate nodes.

With the same system configurations, Fig. 6 shows the normalized running time of the proposed DL method on average. The normalized running time is obtained by dividing the actual running time by that of the exhaustive search. From the figure, it can be concluded that the DL method greatly reduces computational complexity once trained with small performance degradation, yielding a desirable performance and time complexity trade off.

V. Conclusion

In this paper, we have studied a legitimate proactive eavesdropping scenario where a central monitor covertly wiretaps the communication between a pair of suspicious users via multiple intermediate nodes. The intermediate nodes are divided into two separate groups, namely eavesdropping nodes and jamming nodes to aid the central monitor in efficient eavesdropping. We have developed a DL based strategy that yields the optimal mode selection and the transmit power of the intermediate nodes with a reduced computational burden. Numerical results have validated the efficiency of the developed DL method in various system setups.

References

[1] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm," *IEEE Wireless Commun.*, vol. 24, pp. 152–159, Aug. 2017.

[2] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2470–2492, Jun. 2008.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 4961–4972, Aug. 2011.

[4] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, pp. 2083–2114, Apr. 2011.

[5] H. Lee, C. Song, J. Moon, and I. Lee, "Precoder designs for MIMO Gaussian multiple access wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 66, pp. 8563–8568, Sep. 2017.

[6] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 64, pp. 1850–1863, Apr. 2014.

[7] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol.*, vol. 65, pp. 180–190, Jan 2016.

[8] H. Lee, S. Eom, J. Park, and I. Lee, "UAV-aided secure communications with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 67, pp. 9385–9392, Oct. 2018.

[9] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Commun. Lett.*, vol. 5, pp. 80–83, Feb. 2016.

[10] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 2790–2806, May 2017.

[11] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, pp. 4585–4599, Jul. 2017.

[12] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications," *in Proc. IEEE Int. Workshop Signal Adv. Wireless Comm. (SPAWC)*, Jul. 2017.

[13] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in relaying systems," *IEEE Signal Process. Lett.*, vol. 24, pp. 917–921, Jun. 2017.

[14] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *IEEE Signal Process. Lett.*, vol. 24, pp. 1714–1718, Nov. 2017.

[15] B. Li, Y. Yao, H. Zhang, Y. Lv, and W. Zhao, "Energy efficiency of proactive eavesdropping for multiple links wireless system," *IEEE Access*, vol. 6, pp. 26081–26090, May 2018.

[16] B. Li, Y. Yao, H. Chen, Y. Li, and S. Huang, "Wireless information surveillance and intervention over multiple suspicious links," *IEEE Signal Process. Lett.*, vol. 25, pp. 1131–1135, Aug. 2018.

[17] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, pp. 1449–1461, Dec. 2016.

[18] H. Tran and H.-J. Zepernick, "Proactive attack: A strategy for legitimate eavesdropping," *in Proc. IEEE ICCE*, pp. 457–461, Sep. 2016.

[19] J. Moon, H. Lee, C. Song, S. Lee, and I. Lee, "Proactive eavesdropping with full-duplex relay and cooperative Jamming," *IEEE Trans. Wireless Commun.*, vol. 17, pp. 6707–6719, Oct. 2018.

[20] J. Moon, H. Lee, C. Song, S. Kang, and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, pp. 6958–6971, Oct. 2018.

[21] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, May 2015.

[22] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Trans. Commun.*, vol. 65, pp. 764–774, Feb. 2017.

[23] S.-H. Park, O. Simeone, O. Sahin, and S. S. Shitz, "Fronthaul compression for cloud radio access networks: Signal processing advances inspired by network information theory," *IEEE Signal Process. Mag.*, vol. 31, pp. 69–79, Nov. 2014.

[24] G. E. Dahl, T. N. Sainath, and G. E. Hinton, "Improving deep neural networks for LVCSR using rectified linear units and dropout," *in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, May. 2013.

[25] S. P. Rath, D. Povey, K. Veselý, and J. Černocký, "Improved feature processing for deep neural networks," *in Proc. Interspeech*, pp. 109–113, 2013.

[26] D. G. Luenberger and Y. Ye, *Linear and nonlinear programming*. Springer, Jun. 2015.

[27] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *in Proc. 3rd Int. Conf. Learn. Representations*, Dec. 2014.