This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

Evaluating Secrecy Outage of Physical Layer Security in Large-Scale MIMO Wireless Communications for Cyber-Physical Systems

Danda B. Rawat, *Senior Member, IEEE,* Taylor White, Md Salik Parwez, *Student Member, IEEE,* Chandra Bajracharya, *Member, IEEE* and Min Song, *Senior Member, IEEE*

***Abstract*—Large-scale multiple input multiple output (MIMO) wireless system is regarded as a solution to provide high speed connection for exponentially increasing wireless subscriptions for emerging cyber-physical systems (CPS) and Internet-of-Things (IoT). In order to realize its full potential, there are several challenges to be addressed to achieve high secrecy rate or data rate. In this paper, we analyze outage probability for secrecy rate in MIMO wireless systems in the presence of eavesdroppers and jammers for CPS devices. Our proposed approach takes into account the impact of jammers while finding the best response to minimize the jamming/interfering effect (or to enhance the secrecy rate) and the impact of eavesdropper in secrecy rates of the users. We present formal analysis for secrecy outage probability and interception probability considering Rayleigh fading scenario. The performance is evaluated by using numerical results obtained from Monte Carlo simulations. Numerical results indicate that the system performance is improved significantly when the users adapt their transmit vectors based on their observed interference values. Furthermore, the secrecy outage probability increases with power of jammer and the secrecy capacity decreases when jammer power increases. We observed that the proposed approach outperforms the other existing approaches.**

***Keywords*—** *MIMO, physical layer security, secrecy outage, cyber-physical systems.*

I. Introduction

The demand for high data rate and reliability is increasing as user density is increasing exponentially because of bandwidth hungry and delay constraint emerging cyber-physical systems [1]–[4] and Internet-of-Things [5], [6]. Large-scale multiple input multiple output (MIMO) wireless system is an emerging technology to enhance the system capacity of next generation wireless networks where very large number of antennas are expected to be deployed at access point or base station [7] to support very large number of devices with a few or single antenna in cyber-physical systems and Internet-of-Things. In large-scale MIMO, all the complexity is at the central access point or base station which has more resources compared to IoT/CPS devices, thus it is suitable for IoT/CPS devices that have limited resources. The MIMO technology has been researched for last two decades and implemented in several wireless systems as it boosts both system capacity and reliability. However, concept of equipping the base station with very large number of antennas is still emerging [8], [9]. The large-scale MIMO system can serve several users simultaneously maximizing the overall system capacity that provides high data rates for the users [7], [10]. However, like other systems, large-scale MIMO system is also vulnerable to several physical layer security attacks. The concept of wiretap channel [11] and secrecy capacity [12] has recently prompted significant research in physical layer security of wireless communication systems [13]. Openness of wireless communications makes the entire system more vulnerable to several attacks including jamming and eavesdropping attacks. Recently, several efforts have been devoted to research and several developments are reported in the literature to enhance the secrecy capacity of wireless system [8], [14]–[19]. Physical layer security in MIMO wireless system has been studied [20], [21] using information theory. Artificial noise is generated to degrade the signal to noise ratio (SINR) of the eavesdropper without interfering the desired receiver to enhance the secrecy capacity of MIMO systems in [22]. Beamforming technique has been studied for multiple input single output system for enhancing the secrecy capacity of the system [23], [24]. Physical layer security has been studied in [25] where eavesdropper with very large number of antennas has been considered. With the knowledge of probability density function of SINR of the received signal at the receiver and at the eavesdropper, performance of the MIMO systems has been studied in [26]–[29]. In [30], the concept of secrecy outage capacity to ensure secure and efficient transmission with quality-of-service (QoS) requirements has been proposed. However, none of these approaches consider joint impact of eavesdropper and jammers while evaluating the physical layer security by considering secrecy outage probability, interception probability and average secrecy capacity of large-scale MIMO wireless system which supports robust and secure communications for cyber physical systems [1], [2], [31].

In this paper, we focus on formal analysis of the physical layer security in large-scale MIMO wireless system in the presence of jammers and eavesdropper by considering secrecy outage probability as a function of different parameters (e.g., SINR, jammers power, interference, number of antenna, path loss) and interception probability for cyber physical systems. We derive the expression for secrecy outage probability in

Manuscript received 6 January 2017.

Danda B. Rawat, Taylor White and Md Salik Parwez are with the Department of Electrical Engineering and Computer Science at Howard University, Washington, DC 20059, USA. E-mail: db.rawat@ieee.org.

Chandra Bajracharya is with the Department of Electrical Engineering at Capitol Technology University, Laurel, MD, USA. E-mail: cbajra@gmail.com.

Min Song is with the Department of Computer Science, Michigan Technological University, Houghton, MI 49931, USA. E-mail: mins@mtu.edu.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

terms of SINR of the user of interest at base station. Every time, each user in the system updates its transmit waveform based on the interference observed and chooses the eigenvector corresponding to the minimum eigenvalue of the interference matrix. This helps to avoid interference from jammers and results in increase in SINR at the receiver. Increase in SINR results in increase in secrecy rate of the system. We perform evaluation using numerical results obtained from Monte Carlo simulations. We found that the proposed approach gives better results and outperforms the existing methods.

The rest of the paper is organized as follows. We describe the system model and problem statement in Section II. In Section III, the best response and secrecy outage probability analysis for proposed large-scale MIMO model are discussed. Section IV provides the numerical results to validate our analysis and concluding remarks are given in Section V.

Notation: In this paper, matrix and vector are denoted by boldface upper and lower case symbols respectively. $(.)^T$ and $(.)^*$ represents the transpose and conjugate operation respectively. The determinant and trace operators are represented by $\det(.)$ and $Tr(.)$ respectively. $E\{.\}$ represents the expectation and $Pr(.)$ represent the probability.

II. System Model

A typical system model for an uplink wireless system considered in this paper is shown in Fig. 1 where the base station is equipped with N_r receive antennas to serve K number of legitimate users. These users need high speed and secure communications for controlling cyber-physical systems and to accomplish some tasks in Internet-of-Things in near real-time. To evaluate the secrecy outage of physical layer, we consider that there are J number of multi-antenna jammers targeting the base station and a multi-antenna eavesdropper for overhearing the legitimate communications. Each CPS user terminal k has $n_{t,k}$ transmit antennas and thus for K users, total number of transmit antenna becomes $N_t = \sum_{k=1}^{K} n_{t,k}$. The jammer consists of N_j antennas capable of jamming the communication between transmitter and receiver. We assume that the channel state information is available at both transmitter and receiver where base station estimates CSI using users' pilot sequences and share the information while decoding user signals. Note that the channel estimation overhead is independent of number of antennas at the base station in large-scale MIMO in time division duplex (TDD) and thus TDD is preferred for large-scale MIMO systems. Furthermore, in TDD uplink scenario, all the complexity is at the central base station which has more resources compared to CPS devices. The $\mathbf{H}_k = \sqrt{\alpha_k}\bar{\mathbf{H}}_k$ denotes the channel matrix where α_k is the distance-dependent path loss and $\bar{\mathbf{H}}_k$ is the small scale fading channel.

For the system model given in Fig 1, the received signal for kth CPS user at the base station can be expressed in a vector form as

$$\mathbf{r}_k = \mathbf{H}_k\mathbf{x}_k + \sum_{l=1,l\neq k}^{K} \mathbf{H}_l\mathbf{x}_l + \sum_{j=1}^{J} \hat{\mathbf{H}}_j\mathbf{v}_j + \mathbf{n}, \qquad (1)$$

where $\mathbf{r}_k$ is the $N_r \times 1$ dimensional received signal vector at base station from kth user, $\mathbf{x}_k = \sqrt{\mathbf{P}_k}\mathbf{s}_k$ is $n_{t,k} \times 1$ transmitted signal vector that contains transmitted symbols which satisfies $E\{\|\mathbf{s}\|^2\} = 1$. $\mathbf{n}_k$ is $N_r \times 1$ dimensional additive white Gaussian noise (AWGN) vector that corrupts the received signal with $\mathbf{n}_k \sim \mathcal{N}(0, \sigma_k^2\mathbf{I}_{N_r})$ and the noise correlation matrix $\mathbf{W} = E\{\mathbf{n}\mathbf{n}^T\}$ here σ_k^2 is noise power, $\mathbf{v}_j$ denotes $N_j \times 1$ dimensional jamming signal vector $\mathbf{H}_k$ is $N_r \times n_{t,k}$ dimensional channel matrix for kth user and $\hat{\mathbf{H}}_j$ is $N_r \times N_j$ channel matrix for jth jammer. Note that first term in (1) represents the desired signal, second and third term represent the interference due to other users in the system and jammers respectively.

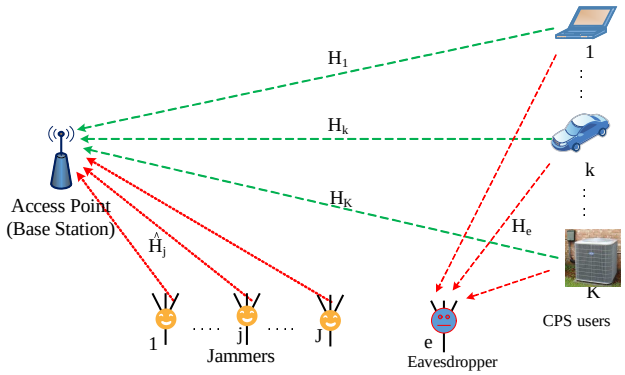

Fig. 1. A system model with an access point (or base station, smart meter at home in energy CPS, etc.) equipped with multiple antennas, K CPS users, an eavesdropper and J jammers.

Then, the correlation matrix of received signal in (1) can be written as

$$\mathbf{R} = \sum_{k=1}^{K} \mathbf{H}_k\mathbf{Q}_k\mathbf{H}_k^T + \sum_{j=1}^{J} \hat{\mathbf{H}}_j\mathbf{R}_j\hat{\mathbf{H}}_j^T + \mathbf{W}, \qquad (2)$$

where $\mathbf{Q}_k = E\{\mathbf{x}_k\mathbf{x}_k^T\}$ and $\mathbf{R}_j = E\{\mathbf{v}_j\mathbf{v}_j^T\}$ are the covariance matrices of the transmitted signal and jamming signal respectively.

Next, we can write the correlation matrix of the interference from others users and jammers, and the noise as

$$\begin{aligned}\mathbf{R}_k &= \sum_{l=1,l\neq k}^{K} \mathbf{H}_l\mathbf{Q}_l\mathbf{H}_l^T + \sum_{j=1}^{J} \hat{\mathbf{H}}_j\mathbf{R}_j\hat{\mathbf{H}}_j^T + \mathbf{W} \\ &= \sum_{l=1}^{K} \mathbf{H}_l\mathbf{Q}_l\mathbf{H}_l^T + \sum_{j=1}^{J} \hat{\mathbf{H}}_j\mathbf{R}_j\hat{\mathbf{H}}_j^T + \mathbf{W} - \mathbf{H}_k\mathbf{Q}_k\mathbf{H}_k^T \\ &= \mathbf{R} - \mathbf{H}_k\mathbf{Q}_k\mathbf{H}_k^T.\end{aligned} \qquad (3)$$

The $\mathbf{R}_k$ in (3) is the interference and noise for a given user signal k that depends on all other active users (including jammers) in the system except user k. Then the mutual information between the transmitter and receiver of the system $I(\mathbf{x}_k, \mathbf{r}_k)$ can be given by

$$I(\mathbf{x}_k, \mathbf{r}_k) = \log_2 \det\left(\mathbf{R}\right) - \log_2 \det(\mathbf{R}_k). \qquad (4)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

Substituting (2) and (3) into (4), the mutual information expression can be expressed as

$$\begin{aligned} I(\mathbf{x}_k, \mathbf{r}_k) &= \log_2 \det\left(\mathbf{R}_k + \mathbf{H}_k \mathbf{Q}_k \mathbf{H}_k^T\right) - \log_2 \det(\mathbf{R}_k) \\ &= \log_2 \det\left(\mathbf{I}_{N_r} + {\mathbf{R}_k}^{-1} \mathbf{H}_k \mathbf{Q}_k \mathbf{H}_k^T\right) \\ &= \log_2 \det\left(\mathbf{I}_{N_r} + ({\mathbf{R}_k}^{-\frac{1}{2}} \mathbf{H}_k) \mathbf{Q}_k ({\mathbf{R}_k}^{-\frac{1}{2}} \mathbf{H}_k)^T\right). \end{aligned} \tag{5}$$

The achievable rate is defined as the maximum mutual information with transmit power constraint $Tr(\mathbf{Q}_k) \leq \tilde{P}_k$, and is given by

$$\overline{C}_k = \max_{Tr(\mathbf{Q}_k) \leq \tilde{P}_k} \mathrm{I}(\mathbf{x}_\mathrm{k}, \mathbf{r}_\mathrm{k}), \tag{6}$$

where $\tilde{P}_k$ is the maximum average transmit power allowed for each user for wireless communications. The achievable transmission rate in (6) can be written as

$$\begin{aligned} \overline{C}_k &= \max_{Tr(\mathbf{Q}_k) \leq \tilde{P}_k} \log_2 \det\left(\mathbf{I}_{\mathrm{N_r}} + {\mathbf{R}_\mathrm{k}}^{-1} \mathbf{H}_\mathrm{k} \mathbf{Q}_\mathrm{k} \mathbf{H}_\mathrm{k}^\mathrm{T}\right) \\ &= \log_2 \det\left(\mathbf{I}_{N_r} + \tilde{P}_k \mathbf{R}_k^{-1} \mathbf{H}_k \mathbf{H}_k^T\right) \\ &\geq \log_2\left(1 + \tilde{P}_k \det\left(\mathbf{R}_k^{-1} \mathbf{H}_k \mathbf{H}_k^T\right)\right) \\ &\geq \log_2\left(1 + \tilde{P}_k \det\left(\mathbf{R}_k^{-1} \mathbf{H}_k \mathbf{H}_k^T\right)\right) \\ &= \log_2\left(1 + \gamma_k\right), \end{aligned} \tag{7}$$

where γ_k is the instantaneous SINR of the user k. Note that, for match filter based communication, the SINR γ_k can be expressed as

$$\gamma_k = \frac{\tilde{P}_k \det\left(\mathbf{H}_k \mathbf{H}_k^T\right)}{\mathbf{x}_k^T \mathbf{R}_k \mathbf{x}_k}. \tag{8}$$

Next, the received signal at (passive) eavesdropper from a given user k can be expressed as

$$\mathbf{r}_e = \mathbf{H}_e \mathbf{x}_k + \mathbf{n}_e, \tag{9}$$

where $\mathbf{r}_e$ is the $N_e \times 1$ dimensional received signal vector at a given eavesdropper e, $\mathbf{n}_e$ is $N_e \times 1$ the additive Gaussian noise [1] at the eavesdropper with $\mathbf{n}_e \sim \mathcal{N}(0, \sigma_e^2 \mathbf{I}_{N_e})$ and $\mathbf{H}_e$ is $N_e \times n_{t,k}$ channel matrix connecting users to eavesdropper.

The achievable transmission rate of eavesdropper by overhearing the transmitted message by users can be written as

$$\begin{aligned} C_e &= \log_2 \det\left(\mathbf{I}_{N_e} + \frac{1}{\sigma_e^2} \mathbf{H}_e \mathbf{Q}_k \mathbf{H}_e^T\right) \\ &\geq \log_2\left(1 + \frac{P_k}{\sigma_e^2} \det\left(\mathbf{H}_e \mathbf{H}_e^T\right)\right) \\ &\geq \log_2\left(1 + \gamma_e\right), \end{aligned} \tag{10}$$

where $\gamma_e = \frac{P_k}{\sigma_e^2} \det\left(\mathbf{H}_e \mathbf{H}_e^T\right)$ is the SINR at the eavesdropper.

Next, we assume that jammers are interested to deteriorate the SINR of kth user and are not interested in eavesdroppers.

[1]When eavesdropping a given user, signal from all other users could be treated as an additive noise considering not knowing their distributions.

From the perspective of information theory, the achievable secrecy capacity using (7) and (10) for a user k is given by

$$C_k = [\overline{C}_k - \max\{C_e\}_{\forall e}]^+, \tag{11}$$

where, $[x]^+$ is $\max(x, 0)$. In (11), $\max\{C_e\}_{\forall e}$ gives the loss in user rate because of overhearing by the eavesdroppers, if there are multiple eavesdroppers.

III. Proposed Approach: The Best Response and Secrecy Outage Probability Analysis

A. The Best Response Strategy

Note that we can maximize the C_k by minimizing C_e or by maximizing $\overline{C}_k$ by minimizing the effect of the interference in (7) or (8) for a given user. In other words, we can minimize the interference function given in (12) experienced by each user k to maximize its secrecy capacity $\overline{C}_k$ to eventually maximize the secrecy rate C_k. The interference function, which depends on $\mathbf{R}_k$, can be written as

$$i_k = \mathbf{x}_k^T \mathbf{R}_k \mathbf{x}_k. \tag{12}$$

Thus the interference (given in (12)) minimization problem can be written as

$$\min \quad \mathbf{x}_k^T \mathbf{R}_k \mathbf{x}_k \text{ subject to } \mathbf{x}_k^T \mathbf{x}_k = Q_k, \quad \forall k, \tag{13}$$

and the interference minimization problem (13) can be solved by Lagrangian method as

$$\Delta_k(\mathbf{x}_k, \lambda_k) = \mathbf{x}_k^T \mathbf{R}_k \mathbf{x}_k + \lambda_k(\mathbf{x}_k^T \mathbf{x}_k - Q_k). \tag{14}$$

To minimize the Lagrangian function, we differentiate it with respect to $\mathbf{x}_k$ and equate the corresponding partial derivative to zero, then, we get

$$\frac{\partial \Delta_k(\mathbf{x}_k, \lambda_k)}{\partial \mathbf{x}_k} = 0 \Rightarrow \mathbf{R}_k \mathbf{x}_k = \kappa_k \mathbf{x}_k \Rightarrow \mathbf{R}_k \mathbf{s}_k = \kappa_k \mathbf{s}_k, \tag{15}$$

where κ_k is the minimum eigenvalue of $\mathbf{R}_k$ [32]. From (15), at an equilibrium point, the best response for the intended receiver that gives minimum interference is an eigenvector corresponding to the minimum eigenvalue κ_k of $\mathbf{R}_k$. This information is fed back to the transmitter using secure feedback channels [33]. Then, the given user can use it as a transmit vector to increase the secrecy capacity.

Note that, in our system model, each user chooses its best response a a transmit vector (i.e., minimum eigenvector corresponding to minimum eigenvalue of interference matrix $\mathbf{R}_k$) based on (15) to avoid impact of jamming/interference and noise each time while transmitting its information with the aim of increasing the rate $\overline{C}_k$ in (7) that results in increase in secrecy rate C_k in (11).

B. Analysis for Secrecy Outage Probability

To evaluate the physical layer security performance of an uplink of a large-scale MIMO system, we consider secrecy outage capacity. To analyze the secrecy outage capacity, we calculate the probability density function of kth user $f(\gamma_k)$ and eavesdropper $f(\gamma_e)$ considering both random variables (RVs) γ_k and γ_e that follow Rayleigh distribution with respective variances σ_k^2 and σ_e^2.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

The cumulative distribution function (CDF) of γ_k can be written as [34]

$$F(\gamma_k) = 1 - \exp\left(-\frac{\gamma_k}{\bar{\gamma_k}}\right), \qquad \gamma_k > 0. \tag{16}$$

Then, the corresponding probability density function (PDF) can be expressed as

$$f(\gamma_k) = \frac{1}{\bar{\gamma_k}} \exp(-\frac{\gamma_k}{\bar{\gamma_k}}), \tag{17}$$

where $\bar{\gamma_k}$ is the average SINR of the users which is given by

$$\bar{\gamma_k} = \frac{P_k E\{\|\mathbf{H_k}\|\}}{\sigma_k^2}. \tag{18}$$

Similarly, the CDF, $F(\gamma_e)$, and corresponding PDF, $f(\gamma_e)$, of γ_e can be expressed as

$$\begin{aligned} F(\gamma_e) &= 1 - \exp(-\frac{\gamma_e}{\bar{\gamma_e}}), \qquad \gamma_e > 0 \\ f(\gamma_e) &= \frac{1}{\bar{\gamma_e}} \exp(-\frac{\gamma_e}{\bar{\gamma_e}}), \end{aligned} \tag{19}$$

where $\bar{\gamma_e}$ is the average SINR of the eavesdropper which is based on kth user's transit power P_k and given as

$$\bar{\gamma_e} = \frac{P_k E\{\|\mathbf{H_e}\|\}}{\sigma_e^2}. \tag{20}$$

The variables γ_k and γ_e are independent and identically distributed (i.i.d) random variables. Thus, the joint probability density function of (γ_k, γ_e) can be written as follows

$$\begin{aligned} f(\gamma_k, \gamma_e) = f(\gamma_e).f(\gamma_k) = \frac{1}{\bar{\gamma_k}\bar{\gamma_e}} \exp(-\frac{\gamma_e}{\bar{\gamma_e}} - \frac{\gamma_k}{\bar{\gamma_k}}) \\ \gamma_k > 0, \gamma_e > 0. \end{aligned} \tag{21}$$

Then, the instantaneous secrecy capacity in (11) can be expressed as

$$C_k(\gamma_k, \gamma_e) = \Big[\log_2\big(1+\gamma_k\big) - \log_2\big(1+\gamma_e\big)\Big]^+. \tag{22}$$

The outage probability measures the probability of failing to achieve the instantaneous secrecy capacity, C_k, that is, the probability of getting C_k less than the desired transmission secrecy capacity which is required for successful reception of information at the receiver. The outage probability can be denoted as

$$Pr_{out}(R_s) = Pr\big\{C_k(\gamma_k, \gamma_e) < R_s\big\}, \tag{23}$$

where R_s is the minimum required secrecy capacity for a desired service.

Proposition 1: For the considered system model, the secrecy outage probability is

$$Pr_{out}(R_s) = 1 - \frac{\bar{\gamma_k}}{\bar{\gamma_k} + \bar{\gamma_e} 2^{R_s}} \exp(-\frac{2^{R_s}-1}{\bar{\gamma_k}}). \tag{24}$$

Proof: The secrecy outage probability of the system in the presence of jammers and eavesdropper can be written as

$$\begin{aligned} Pr_{out}(R_s) &= Pr\left\{\log_2\left(\frac{1+\gamma_k}{1+\gamma_e}\right) < R_s\right\} \\ &= Pr\Big\{(\gamma_k - 2^{R_s}\gamma_e) < (2^{R_s}-1)\Big\} \\ &= Pr\Big\{(\gamma_k - 2^{R_s}\gamma_e) < \gamma_s\Big\}. \end{aligned} \tag{25}$$

$\gamma_s = 2^{R_s} - 1$ is the minimum required SINR.

By using the joint probability density function of random variables (γ_k, γ_e) given in (21), we can write secrecy outage probability in (25) as

$$\begin{aligned} Pr_{out}(R_s) &= 1 - \iint\limits_{(\gamma_k - 2^{R_s}\gamma_e) < \gamma_s} f(\gamma_k, \gamma_e) d\gamma_k d\gamma_e \\ &= 1 - \int\limits_{\gamma_s}^{\infty} \frac{1}{\bar{\gamma_k}} \exp(-\frac{\gamma_k}{\bar{\gamma_k}}) d\gamma_k \int\limits_{0}^{\gamma_s + \gamma_e 2^{R_s}} \frac{1}{\bar{\gamma_e}} \exp(-\frac{\gamma_e}{\bar{\gamma_e}}) d\gamma_e \\ &= 1 - \frac{\bar{\gamma_k}}{\bar{\gamma_k} + \bar{\gamma_e} 2^{R_s}} \exp(-\frac{2^{R_s}-1}{\bar{\gamma_k}}), \end{aligned} \tag{26}$$

which proves the *Proposition 1*.

Proposition 2: For the considered system model, the interception probability is

$$P_{int} = \exp\Big(\frac{2^{\overline{C}_k} - 1}{\bar{\gamma_e} P_k}\Big). \tag{27}$$

Proof: The secrecy outage is defined as maximum rate under which the outage probability that transmission rate exceeds the secrecy capacity is given by

$$\begin{aligned} \epsilon &= Pr\big\{C_k > \overline{C}_k - \max\{C_e\}_{\forall e}\big\} \\ &= Pr\big\{\gamma_e > 2^{(\overline{C}_k - C_k)} - 1\big\} \\ &= 1 - F\Big(\frac{2^{(\overline{C}_k - C_k)} - 1}{P_k}\Big), \end{aligned} \tag{28}$$

where $F(.)$ is the CDF of γ_e. From (19), we get that

$$F(\gamma_e) = 1 - \exp\Big(-\frac{2^{(\overline{C}_k - C_k)} - 1}{\bar{\gamma_e} P_k}.\Big) \tag{29}$$

Combining (28) and (29), we get

$$\epsilon = \exp\Big(-\frac{2^{(\overline{C}_k - C_k)} - 1}{\bar{\gamma_e} P_k}\Big). \tag{30}$$

The interception probability P_{int} i.e., the probability that the eavesdropper channel capacity is greater than legitimate channel capacity and when $C_k = 0$ in (30) can be given as

$$P_{int} = \exp\Big(\frac{2^{\overline{C}_k} - 1}{\bar{\gamma_e} P_k}\Big), \tag{31}$$

which proves the *Proposition 2*.

IV. Simulations and Numerical Results

To corroborate the analysis presented above, we consider a single cell uplink large-scale MIMO system where eavesdroppers overhear the legitimate communication and jammers send jamming signal toward the receiver. Base station is assumed to be equipped with $N_r = 50$ antennas and user devices are equipped with $n_{t,k} = 10$ antenna. Individual jammers and eavesdroppers are equipped with $N_j = 10$ and $N_e = 10$ antennas respectively. The additive white noise covariance matrix at legitimate receiver and the eavesdropper are considered $0.1\mathbf{I}_{N_r}$ and $0.1\mathbf{I}_{N_e}$ respectively. The channel matrix $\mathbf{H}_k$, $\hat{\mathbf{H}}_j$, $\mathbf{H}_e$ are generated randomly. All simulation results are averaged over several trials.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

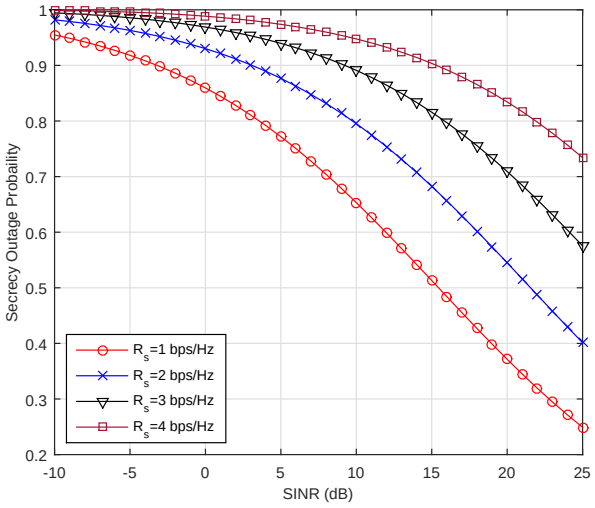

Fig. 2. Secrecy Outage Probability vs. SINR with $n_{t,k} = 10$, $N_r = 50$ in the presence of an eavesdropper and jammers with $Rs = \{1, 2, 3, 4\}$ (bps/Hz).

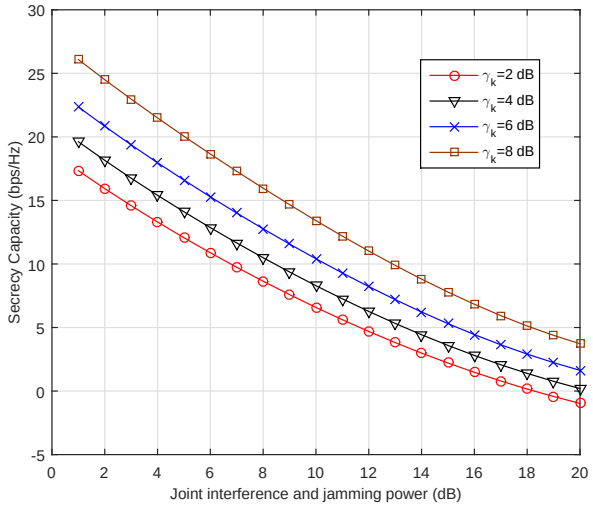

Fig. 3. Variation of Secrecy Capacity with Increasing Interference and Jammer Power.

First, we have plotted the variation of secrecy outage probability vs SINR for different value of minimum required secrecy rates i.e., $Rs = \{1, 2, 3, 4\}$bps in the presence of jammers and eavesdroppers as shown in Fig 2. We observed in Fig 2 that as SINR increases, the secrecy outage probability decreases for a given minimum required secrecy rate. Furthermore, the secrecy outage probability increases when given minimum required secrecy rate increases. We note that higher the SINR and lower the minimum required secrecy rate requirement, the lower the secrecy outage probability for a given scenario.

Next, we have plotted the variation of secrecy capacity vs. the interference power (contributed by other legitimate users and jammers) as shown in Fig. 3. As expected, secrecy capacity decreases when interference/jammer power increases and it increases with SINR for a given interference/jammer power as shown in Fig. 3.

We have also plotted the variation of secrecy outage probability vs. the minimum required secrecy rate for different values of SINR ranging from -10dB to 20dB as shown in Fig 4. It is seen from Fig 4 that the secrecy outage probability gradually increases and finally converges to 1 with increasing values of minimum required rate values. It is also seen that as SINR increases from -10 dB to 20 dB, the secrecy outage probability decreases for a given minimum required secrecy rate value as shown in Fig 4.

Then, we have plotted the secrecy outage probability vs. SINR for single input single output (SISO), multiple input multiple output (MISO), single-input multiple output (SIMO), MIMO and large-scale MIMO as shown in Fig. 5. We observed in Fig. 5 that large-scale MIMO results in lowest secrecy outage probability for given SINR value. Furthermore, increase in SINR results in decrease in outage secrecy probability, which is expected.

Next, we have plotted interception probability with the path loss factor as shown in Fig. 6. When $\alpha > 1$ (i.e., the eavesdropper is nearer to the transmitter than the intended

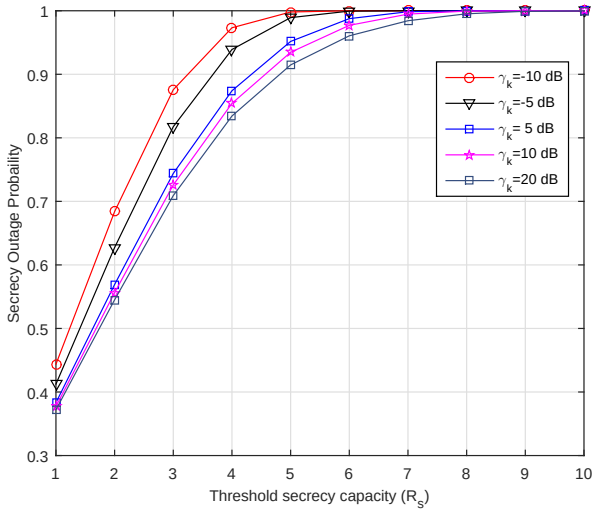

Fig. 4. Variation of Secrecy Outage Probability with R_s for different $\gamma_k = \{-10, -5, 5, 10, 20\}(dB)$.

receiver), the interception probability is higher than that of $\alpha < 1$ as shown in Fig. 6. Furthermore, the interception probability increases with power as shown in Fig. 6.

Finally, we have compared our approach with the approach in [35] by considering identical simulation scenarios. We have plotted the secrecy capacity for both approaches as shown in Fig. 7. It is found that the proposed approach gives better secrecy capacity than the method in [35] even with and without jammers and eavesdropper. The main reason is that our approach uses the best response strategy while choosing the transmit vector which helps to avoid jammers and interference from other coexisting users.

V. Conclusion

In this paper, we have presented an analysis for secrecy outage probability and interception probability in large-scale

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

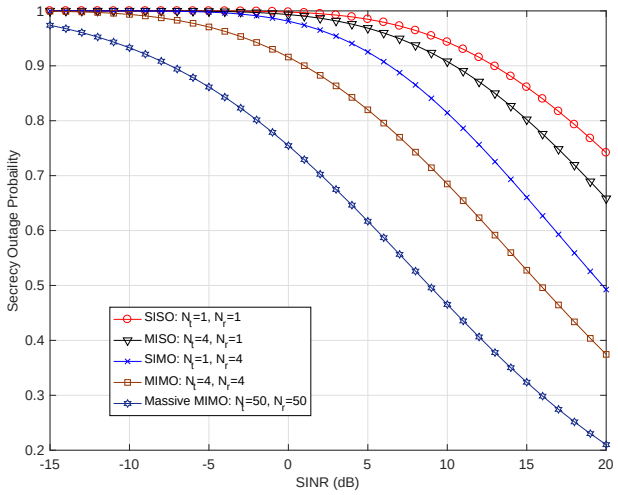

Fig. 5. Comparison of secrecy outage probability of SISO, MISO, SIMO, MIMO, large-scale MIMO.

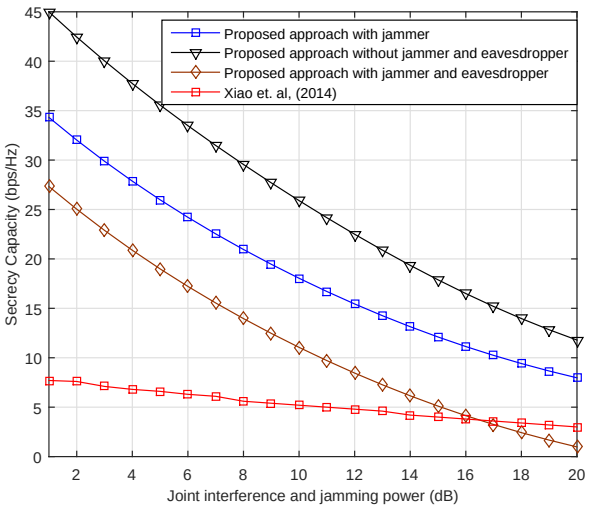

Fig. 7. Comparison of secrecy capacity/rate between the proposed best response approach and an approach in [35].

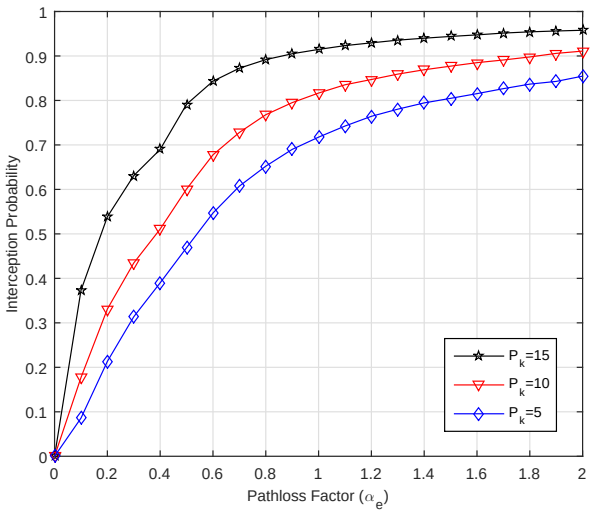

Fig. 6. Interception probability variation with path loss factor.

MIMO systems in the presence of eavesdroppers and jammers considering Rayleigh fading scenario for emerging cyber-physical systems and Internet-of-Things. Each legitimate CPS user can use the best response strategy as its transmit vector to avoid/minimize jamming/interfering effect as well as the impact of eavesdropper to enhance its secrecy rate. Numerical results obtained from Monte Carlo simulations are used to evaluate the performance. We found that the system performance cen be improved by applying the adaptive best response. Furthermore, the secrecy outage probability increases with jamming power of the jammers, and the secrecy capacity decreases when jammer power increases. Also after comparing with the existing approaches, the proposed approach found to be outperforming.

ACKNOWLEDGMENTS

This project is funded in part by the US National Science Foundation (NSF) under grants CNS-1650831 and CNS-1658972. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. The authors would like to thank the anonymous reviewers for their constructive comments on this paper. The authors acknowledge Mr. K. Neupane for discussions on the topic presented in the paper.

REFERENCES

[1] X. Yang, J. Lin, W. Yu, P.-M. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 4–18, 2015.

[2] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-Physical Systems: Foundations, Principles and Applications*. Elsevier and Morgan Kaufmann, 2016.

[3] H. Song, G. A. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications*. UK: Wiley-IEEE Press, 2017.

[4] D. B. Rawat and C. Bajracharya, *Vehicular Cyber Physical Systems: Adaptive Connectivity and Security*. Springer, 2016.

[5] R. H. Weber and R. Weber, *Internet of things*. Springer, 2010, vol. 12.

[6] S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things: Cybermanufacturing Systems*. Springer, 2016.

[7] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Transactions on Wireless Communications*, vol. 9, no. 11, pp. 3590–3600, 2010.

[8] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40–60, 2013.

[9] J. Hoydis, S. Ten Brink, and M. Debbah, "Massive MIMO: How many antennas do we need?" in *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2011, pp. 545–550.

[10] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436–1449, 2013.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2017.2691352, IEEE Internet of Things Journal

[12] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.
[13] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure Massive MIMO transmission in the presence of an active eavesdropper," in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 1434–1440.
[14] E. Larsson, O. Edfors, F. Tufvesson, and T. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014.
[15] T. Amin, D. B. Rawat, and M. Song, "Performance analysis of secondary users in the presence of attackers in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, 2015, pp. 1–7.
[16] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[17] Q. Du, L. Sun, H. Song, and P. Ren, "Security enhancement for wireless multimedia communications by fountain code," *IEEE COMSOC MMTC Communications C Frontiers*, vol. 11, no. 2, pp. 47–51, 2016.
[18] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.
[19] Q. Xu, P. Ren, H. Song, and Q. Du, "Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions," *IEEE IoT Journal*, vol. PP, no. 99, pp. 1–1.
[20] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.
[21] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.
[22] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067–2076, 2011.
[23] J. Zhang and M. C. Gursoy, "Collaborative relay beamforming for secrecy," in *2010 IEEE International Conference on Communications (ICC)*, 2010, pp. 1–5.
[24] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, 2012.
[25] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.
[26] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.
[27] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–154, 2013.
[28] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 247–258, 2014.
[29] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure Transmission With Antenna Selection in MIMO Nakagami-Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, pp. 6054–6067, 2014.
[30] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Communications Letters*, vol. 17, no. 4, pp. 637–640, 2013.
[31] D. B. Rawat, J. J. Rodrigues, and I. Stojmenovic, *Cyber-physical systems: from theory to practice*. CRC Press, 2015.
[32] G. Strang, *Linear Algebra and its Applications*. Academic Press, 1980.
[33] D. J. Love, R. W. Heath Jr, V. K. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 8, pp. 1341–1365, 2008.
[34] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.
[35] Y. Xiao, P. Lan, and D. Wang, "A novel secure MIMO cognitive network," in *2014 IEEE International Symposium on Circuits and Systems (ISCAS'14)*, 2014, pp. 1476–1479.

Danda B. Rawat (S'07, M'09, SM'13) is an Associate Professor in the Department of Electrical Engineering & Computer Science at Howard University, Washington, DC, USA. His research focuses on wireless networks, cybersecurity, cyber-physical systems, Internet-of-Things, big data analytics, wireless virtualization and vehicular ad-hoc networks. He is the recipient of NSF CAREER award in 2016. He has been serving as an Organizing Committee for several international conferences such as IEEE INFOCOM, IEEE CCNC, IEEE AINA, etc. He is the recipient of Outstanding Research Faculty Award 2015 in the College of Engineering & IT at GSU. He is the Founder and Director of CWiNs Research Lab (www.CWiNs.org). He received the Ph.D. in Electrical and Computer Engineering from Old Dominion University, USA in December 2010.

Taylor White (S'16) is a Masters student in the Department of Electrical Engineering and Computer Science, Howard University, Washington, DC, USA. She received her Bachelor's Degree in Electrical Engineering from Howard University, Washington, DC, in 2015. Her research interests include wireless networking, network security, machine learning, data analytics and cyber-physical systems.

Md. Salik Parwez (S'16) is a PhD student in the Department of Electrical Engineering & Computer Science, Howard University, Washington, DC, USA. He received his BS degree from University of Engineering and Technology, Pakistan, in 2008 and MS degree in Electrical Engineering from University of Oklahoma, USA in 2016. His research interests are next generation wireless networks and cyber-physical systems.

Chandra Bajracharya (S'10, M'14) is a faculty member in the Department of Electrical Engineering at Capitol Technology University, USA. She received her PhD in Electrical & Computer Engineering from Old Dominion University, USA in 2014. Her research interests include cyber-physical systems, power electronics, alternative energy, communication systems, numerical electromagnetics,UWB antenna design and signal/image processing.

Min Song (SM'10) is the Chair and Professor in the Department of Computer Science at Michigan Tech, USA. He served as Program Director with the NSF from October 2010 to October 2014. He received the prestigious NSF Director's award in 2012 and the NSF CAREER award in 2007. His research interests include design, analysis, and evaluation of wireless networks and systems, network security, cyber-physical systems, and mobile computing. He was founding Editor-in-Chief of three international journals. He also served as Editor or Guest Editor of 13 international journals, and as General Chair and Technical Program Chair for many conferences including INFOCOM 2016 and GLOBECOM 2015. He received his PhD degree from the University of Toledo in 2002.