A Physical Layer Secure Wireless Communication Scheme with Partial CSI for High Speed Railway

Cui Yaping
Key Lab of Information Coding & Transmission
Southwest Jiaotong University
Chengdu 610031, China
cuiyaping321@163.com

Xuming Fang
Key Lab of Information Coding & Transmission
Southwest Jiaotong University
Chengdu 610031, China
xmfang@swjtu.edu.cn

***Abstract*—The high speed railway wireless communication system is quite different from public wireless communication system, because the service is train control message, which are closely related to the safety of train transportation. Thus it has much higher requirements for the safety and reliability. In this paper, secrecy capacity and outage probability at the high speed railway scenario with traditional MIMO and beamforming schemes are analyzed. The analytic results show that MIMO scheme can not meet the safety requirements and the beamforming scheme is also helpless while the eavesdropper is close to eNodeB. In order to guarantee the transmission safety of train control messages, a physical layer secure scheme with artificial noise (AN) is proposed for high speed railway communication system. In this proposed scheme, beamforming and AN transmitting directions are adjusted accordingly with the onboard legitimate receiver's channel state information (CSI) and eavesdropper's partial CSI to degrade the eavesdropper while maximize the system secrecy capacity. Simulation results demonstrate the proposed scheme decreases the outage probability under the secrecy capacity constraint, and can meet the safety communication requirements.**

Keywords—Railway wireless communication; Railway Safety; IMT-Advanced; Physical Layer Security; Beamforming; Artificial Noise

I. INTRODUCTION

Long Term Evolution (LTE), which has the characteristics of higher data rate and lower system latency, has been determined as the next generation of railway wireless communication system by the International Union of Railways (UIC). However, there are many different demands between railway professional systems and public wireless communication systems. For example, railway wireless communication system is used for the bi-directional exchange of train control messages between on-board sub-system and Radio Block Centre (RBC) of Train Control Systems (e.g. ETCS-3 in Europe and CTCS-3 in China). The train control messages are closely related to the safety of train transportation, and therefore have higher requirements on safety and reliability.

Much work has been devoted to the field of train control messages delivery safety. Hyun-JeongJo proposed a security mechanism[1], and a method for train signal control communication for the safe communication[2]. Z. Zhang constructed a service-oriented framework of information integration of safety and security for high speed railway[3]. T. Xiang used the cloud computing technology to achieve the sharing of the railway information resources[4].

However, the key based encryption technology is easily to be cracked if the codebook is acquired and chip processing capacity is powerful enough. Besides real-time train control messages delivery could also be detained by this technology. The cloud computing technology may lead to an indistinct physical boundary of the network. Those have bad influences on the delivery safety of train control messages.

Physical layer security was first inspired by Wyner. The 'secrecy capacity' is defined as the supremum of all achievable secrecy rates at which the legitimate receiver's decoding error probability tends to be zero, while the eavesdropper's error probability tends to be one[5]. Physical layer security has the advantage of perfect secrecy transmission without any key, which can also be combined with key based encryption technology to further improve the security. X. Zhang investigated the design of AN-aided secure multi-antenna transmission[6]. N. S. Ferdinand analyzed the effects of outdated CSI on the secrecy outage performance[7]. J.-B. Wang studied the imperfect CSI based joint resource scheduling problem for deadline constrained transmission[8].

If applying the technology of physical layer secure wireless communication in high speed railway, and achieving the positive secrecy capacity, train control messages can be delivered safety even when the messages are cracked, which will significantly improve the safety of train transportation. Consider the safety communication with partial CSI, this paper firstly analyzes the secrecy capacity, outage probability at the high speed railway scenario with traditional MIMO and beamforming schemes. And then a physical layer secure scheme with AN is proposed in high speed railway to meet the requirements of CTCS-3 and the future train control system based on IMT-Advanced.

The rest of this paper is organized as follows. The physical layer secure wireless communication system model at high speed railway scenario is presented in section II. Section III analyzes the secrecy capacity of traditional MIMO, beam-forming and the proposed physical layer secure scheme with

The work of authors is supported partially by the 973 Program under Grant 2012CB316100, the Programs of Technological R&D of the MoR under the Grant 2012X004-A and 2013X016-A.

978-1-4673-6380-8/13/$31.00©2013 IEEE

AN. System performance is analyzed in Section IV. Section V illustrates numerical results. Section VI concludes the paper.

II. PHYSICAL LAYER SECURE SYSTEM MODEL AT HIGH SPEED RAILWAY SCENARIO

Consider the physical layer secure system model at high speed railway scenario shown in Fig.1. eNodeB (eNB) sends train control messages to onboard receiver, while eavesdropper, who is stationary at the wayside of the track, tries to decode those messages.

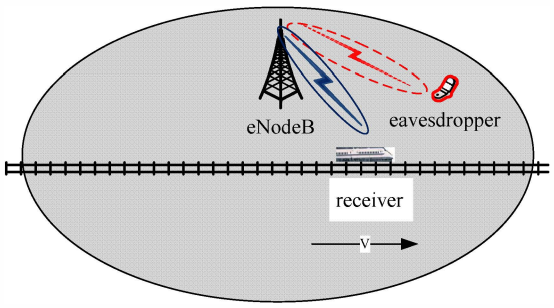


Fig. 1. Physical layer secure system model at high speed railway scenario

Denote channel between eNB and receiver as main channel and between eNB and eavesdropper as eavesdropper channel, respectively. Practically, perfect CSI of eavesdropper channel is difficult to obtain, only partial CSI is accessible[9]. Hence, eNB has the partial CSI of eavesdropper channel is assumed.

Let x be the transmitting signal vector of eNB, then the received signals at receiver and eavesdropper[10] are, respectively, modeled as

$$y = \boldsymbol{h}^H \boldsymbol{w} x + r_B \tag{1}$$

$$z = \boldsymbol{g}^H \boldsymbol{w} x + r_E \tag{2}$$

where $\boldsymbol{h}$ and $\boldsymbol{g}$ denote the main channel and eavesdropper channel gains, respectively, where Rician and Rayleigh fading channel with path loss and shadowing are considered, respectively. r_B and r_E are independent and identically distributed (i.i.d.) complex Gaussian noises with zero-mean and variance σ^2. $1/\sigma^2$ is denoted by ρ. The beamforming vector is $\boldsymbol{w}$, which adjusts the beamforming transmitting direction.

The eavesdropper channel $\boldsymbol{g}$ is modeled as [11]

$$\boldsymbol{g} = \sqrt{k}\boldsymbol{d} + \sqrt{1-k}\tilde{\boldsymbol{g}} \tag{3}$$

where $\boldsymbol{d}$ and $\tilde{\boldsymbol{g}}$ are respectively known and unknown components of the eavesdropper channel gains. k indicates the degree of knowledge that eNB has about the eavesdropper channel $\boldsymbol{g}$, $k = K/(1+K)$ [12]. K is the Rician K-factor [13].

III. PHYSICAL LAYER SECURE SCHEME UNDER BEAMFORMING

In this section, the secrecy capacity of each scheme is analyzed at high speed railway scenario.

A. Traditional MIMO Scheme

eNB transmits the train control messages with multiple antennas. The secrecy capacity is computed as[14]

$$C_S = \left[B\log_2 \frac{1+P\rho|\boldsymbol{h}|^2}{1+P\rho|\boldsymbol{g}|^2} \right]^+ \tag{4}$$

where P is the total transmit power, $[x]^+ = \max[0,x]$, and denoting $\gamma_B = P\rho|\boldsymbol{h}|^2$, $\gamma_E = P\rho|\boldsymbol{g}|^2$.

B. Beamforming Scheme

By means of beamforming, eNB transmits the train control messages with full transmitting power. The secrecy capacity is computed as[15]

$$C_S = \left[B\log_2 \frac{1+P\rho|\boldsymbol{h}^H\boldsymbol{w}|^2}{1+P\rho|\boldsymbol{g}^H\boldsymbol{w}|^2} \right]^+ \tag{5}$$

where $\|\boldsymbol{w}\|^2 = 1$, $\gamma_B = P\rho|\boldsymbol{h}^H\boldsymbol{w}|^2$, $\gamma_E = P\rho|\boldsymbol{g}^H\boldsymbol{w}|^2$.

Two beamforming vectors are defined as $\boldsymbol{w}_{ZF} = \frac{\prod_{\boldsymbol{d}}^{\perp}\boldsymbol{h}}{\|\prod_{\boldsymbol{d}}^{\perp}\boldsymbol{h}\|}$, $\boldsymbol{w}_{ZF}^{\perp} = \frac{\prod_{\boldsymbol{d}}\boldsymbol{h}}{\|\prod_{\boldsymbol{d}}\boldsymbol{h}\|}$. $\boldsymbol{w}_{ZF}$ is the zero-forcing (ZF) vector in the direction of the projection of $\boldsymbol{h}$ onto the null space of $\boldsymbol{d}$, and $\boldsymbol{w}_{ZF}^{\perp}$ is the vector in the direction of the projection of $\boldsymbol{h}$ onto $\boldsymbol{d}$. $\prod_{\boldsymbol{d}} = \boldsymbol{d}\left(\boldsymbol{d}^H\boldsymbol{d}\right)^{-1}\boldsymbol{d}^H$, $\prod_{\boldsymbol{d}}^{\perp} = \boldsymbol{I} - \prod_{\boldsymbol{d}}$. Then, the optimal $\boldsymbol{w}$ solving (5) is obtained as[16]

$$\boldsymbol{w}(\tau) = \sqrt{\tau}\boldsymbol{w}_{ZF}^{\perp} + \sqrt{1-\tau}\boldsymbol{w}_{ZF} \tag{6}$$

where $0 \le \tau \le 1$.

C. Physical Layer Secure Scheme with AN

eNB transmits data with AN through beamforming in the null space of $\boldsymbol{h}$. The secrecy capacity is computed as[15]

$$C_S = \left[B\log_2\left(1+P\rho|\boldsymbol{h}^H\boldsymbol{w}|^2\right) - B\log_2\left(1+\frac{P\rho|\boldsymbol{g}^H\boldsymbol{w}|^2}{1+P\rho\|\boldsymbol{g}^H\boldsymbol{W}\|^2}\right) \right]^+ \tag{7}$$

where $\boldsymbol{w}$ is used for data transmission and the $\boldsymbol{W}$ is used for creating AN, with the constraints $\|\boldsymbol{w}\|^2 = \phi$, $tr\left(\boldsymbol{W}\boldsymbol{W}^H\right) = 1-\phi$. ϕ is power splitting parameter with $0 \le \phi \le 1$.

Contrary to the transmission scheme that transmits AN uniformly in the null space of $\boldsymbol{h}$ in [17], our proposed scheme, which splits AN power into two parts ξ and (1-ξ) with $0 \le \xi \le 1$, creates AN in a particular direction corresponding to CSI. Then the AN is

$$\boldsymbol{r}_x = \sqrt{\xi}\frac{\prod_{\boldsymbol{h}}^{\perp}\boldsymbol{d}}{\|\prod_{\boldsymbol{h}}^{\perp}\boldsymbol{d}\|}r_0 + \frac{\sqrt{1-\xi}}{n_T-2}\sum_{k=1}^{n_T-2}\boldsymbol{u}_k r_k \tag{8}$$

where the power $\xi(1-\varphi)$ is allocated for the AN in direction $\prod_{\boldsymbol{h}}^{\perp}\boldsymbol{d}$, the remaining ($n_T$-2) dimensional subspace is spanned by the corresponding vectors $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n_T-2}$.

By substituting (8) into (7), we get [10]

$$C_S = B\left[\log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right)\right]^+ \tag{9}$$

denoting $\gamma_B = P\rho\phi|\boldsymbol{h}^H\boldsymbol{w}(\tau)|^2$,

$$\gamma_E = \frac{P\rho\phi\left|\boldsymbol{g}^H \boldsymbol{w}(\tau)\right|^2}{1+P\rho(1-\phi)\left(\xi\left|\boldsymbol{g}^H \frac{\prod_{\boldsymbol{h}}^{\perp}\boldsymbol{d}}{\left\|\prod_{\boldsymbol{h}}^{\perp}\boldsymbol{d}\right\|}\right|^2 + \frac{1-\xi}{n_T-2}\sum_{k=1}^{n_T-2}\left|\boldsymbol{g}^H \boldsymbol{u}_k\right|^2\right)}.$$

IV. System Performance Analysis

The schemes are evaluated with the performance metrics of secrecy capacity and outage probability. Secrecy capacity is defined in the previous section, and outage probability will be defined in this section.

A. Outage Probability

The outage probability is the probability that the instantaneous secrecy capacity is less than a target secrecy rate R_S>0[14], and given by

$$P_{out}(R_S) = P[C_S < R_S] \tag{10}$$

If R_S<C_S, eavesdropper channel is worse than eNB's estimate and ensures perfect secrecy. Otherwise, if R_S>C_S, information-theoretic security is compromised.

Recommended data transmission rate requirement is 4.8 kbps for the CTCS-3 in railway wireless communication system[18]. If GSM-R is evolved to LTE/LTE-A system, the link spectral efficiency requirement is 0.25 bit/s/Hz at high speed vehicular environment[19]. That is the target secrecy rate should be greater than or equal to 4.8 kbps or target secrecy spectral efficiency should be greater than or equal to 0.25 bit/s/Hz to guarantee the train control messages delivery safety.

Take the probability theorem,

$$\begin{aligned} P_{out}(R_S) = {} & P(\gamma_B > \gamma_E) P(C_S < R_S \mid \gamma_B > \gamma_E) \\ & + P(\gamma_B \le \gamma_E) P(C_S < R_S \mid \gamma_B \le \gamma_E) \end{aligned} \tag{11}$$

Since $\boldsymbol{h}$ and $\boldsymbol{g}$ are Rician and Rayleigh fading channel gains, respectively, and $\gamma_B \propto |\boldsymbol{h}|^2$, $\gamma_E \propto |\boldsymbol{g}|^2$, it follows that γ_B is non-central chi-square distributed and γ_E is exponentially distributed[20], specially

$$p(\gamma_B) = \frac{(1+K)e^{-K}}{\overline{\gamma}_B}\exp\left[-\frac{(1+K)\gamma_B}{\overline{\gamma}_B}\right] I_0\left(2\sqrt{\frac{K(1+K)\gamma_B}{\overline{\gamma}_B}}\right) \tag{12}$$

$$p(\gamma_E) = \frac{1}{\overline{\gamma}_E}\exp\left(-\frac{\gamma_E}{\overline{\gamma}_E}\right) \tag{13}$$

where γ_B>0, γ_E>0, $I_0(\bullet)$ is the modified Bessel function of the first kind and zero order.

The first term in (11) is expressed as (14)(15), where M is Mellin transform, Q_1 is Marcum Q function of the first order. The second term in (11) is expressed as (16)(17), and since $R_S > 0$, we have

$$P(C_S < R_S \mid \gamma_B \le \gamma_E) = 1 \tag{17}$$

V. Simulation Results

The simulation scenario is shown in Fig.1. eNB is configured with four transmit antennas. For the proposed scheme, the optimal τ, φ, ξ are found by exhaustive search. Detailed simulation parameters are listed in Table 1[13].

TABLE I. Simulation Parameters

Parameters	Value
Bandwidth	10 MHz
Carrier Frequecy	2.5 GHz
Total transmit power	46 dBm
eNB transmit antennas	4
Receiver received antenna	1
Eavesdropper received antenna	1
Cell Radius	3 km
Path loss model	WINNER II
Rician K-factor	7 dB
Speed	350 km/h

Fig.2 illustrates the secrecy capacity for traditional MIMO scheme when eavesdropper is at different locations, and receiver is on the train. Consider the value of R_S is 4.8 kbps, the results show that secrecy capacity is at a low level when eavesdropper is closely to eNB and receiver is far away from eNB. When distance between eNB and eavesdropper is 140m and receiver is 490m away from eNB, the secrecy capacity is lower than 4.8 kbps. Safety of train control messages can not be guaranteed in this situation. While when distance between eNB and eavesdropper is 1300m, the safety of train control messages can be assured during the whole operation.

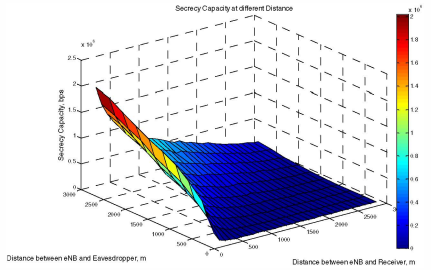


Fig. 2. Secrecy capacity for traditional MIMO scheme

The outage probability for traditional MIMO scheme with different R_S is depicted in Fig.3. We can find that the outage probability increases rapidly with the increasing distance between eNB and receiver. Consider R_S is 4.8 kbps, it can be seen in Fig.3(a) that the outage probability is larger than 90%, when distance between eNB and eavesdropper is 140m and receiver is 390m away from eNB. In this situation, the probability of eavesdropper channel is better than main channel and is large enough to ensure the safety communication.

Fig.4 illustrates the secrecy capacity of beamforming scheme. Consider R_S is 4.8 kbps, when distance between eNB and eavesdropper is 140m and receiver is 2400m away from eNB, the secrecy capacity is lower than 4.8 kbps while receiver is 2400m away from eNB. Safety of train control messages can not be guaranteed in this situation. While when distance between eNB and eavesdropper is 400m, safety of train control messages can be ensured during the whole operation.

$$P(\gamma_B > \gamma_E) = \int_0^\infty \int_o^{\gamma_B} p(\gamma_B, \gamma_E)\, d\gamma_E d\gamma_B = \int_0^\infty \int_o^{\gamma_B} p(\gamma_B)\, p(\gamma_E)\, d\gamma_E d\gamma_B = \int_0^\infty p(\gamma_B)\left[1 - \exp\left(-\frac{\gamma_B}{\overline{\gamma}_E}\right)\right] d\gamma_B$$

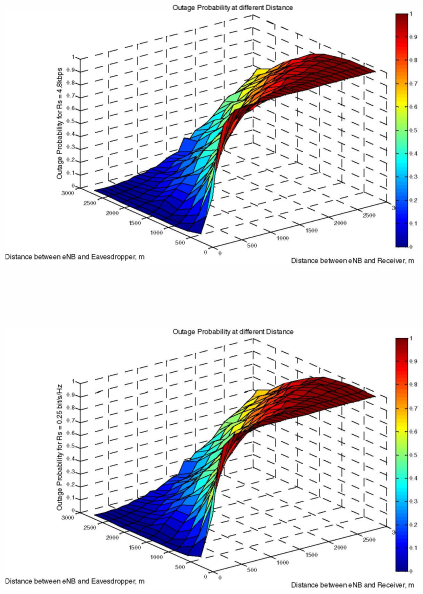
$$= \frac{e^{-\frac{K}{2}}}{\sqrt{K}} M\left[-\frac{1}{2}, 0\right] - (1+K)\exp\left(-\frac{K(1+K)\overline{\gamma}_E + 2K\overline{\gamma}_B}{2\left((1+K)\overline{\gamma}_E + \overline{\gamma}_B\right)}\right)\sqrt{\frac{\overline{\gamma}_E}{K(1+K)^2\overline{\gamma}_E + K(1+K)\overline{\gamma}_B}} M\left[-\frac{1}{2}, 0\right] \tag{14}$$

$$P(C_S < R_S \mid \gamma_B > \gamma_E) = \int_0^\infty \int_{\gamma_E}^{2^{R_S/B}(1+\gamma_E)-1} p(\gamma_B, \gamma_E \mid \gamma_B > \gamma_E) d\gamma_E d\gamma_B = \int_0^\infty \int_{\gamma_E}^{2^{R_S/B}(1+\gamma_E)-1} \frac{p(\gamma_B)\, p(\gamma_E)}{P(\gamma_B > \gamma_E)} d\gamma_E d\gamma_B$$

$$= \frac{1}{P(\gamma_B > \gamma_E)} \int_0^\infty \left[Q_1\left(\sqrt{2K}, \sqrt{\gamma_E}\sqrt{\frac{2(1+K)}{\overline{\gamma}_B}}\right) - Q_1\left(\sqrt{2K}, \sqrt{2^{R_S/B}(1+\gamma_E)-1}\sqrt{\frac{2(1+K)}{\overline{\gamma}_B}}\right)\right] p(\gamma_E)\, d\gamma_E \tag{15}$$

$$P(\gamma_B \le \gamma_E) = 1 - P(\gamma_B > \gamma_E)$$

$$= 1 - \frac{e^{-\frac{K}{2}}}{\sqrt{K}} M\left[-\frac{1}{2}, 0\right] + (1+K)\exp\left(-\frac{K(1+K)\overline{\gamma}_E + 2K\overline{\gamma}_B}{2\left[(1+K)\overline{\gamma}_E + \overline{\gamma}_B\right]}\right)\sqrt{\frac{\overline{\gamma}_E}{K(1+K)^2\overline{\gamma}_E + K(1+K)\overline{\gamma}_B}} M\left[-\frac{1}{2}, 0\right] \tag{16}$$



(a)

(b)

Fig. 3. Outage probability with different R_S for traditional MIMO scheme: (a) secrecy rate is 4.8 kbps; (b) secrecy spectral efficiency is 0.25 bit/s/Hz

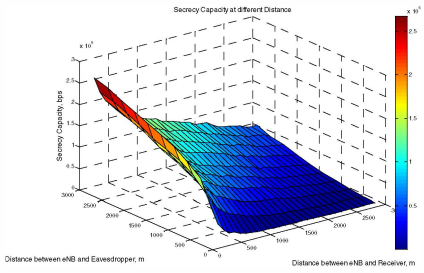
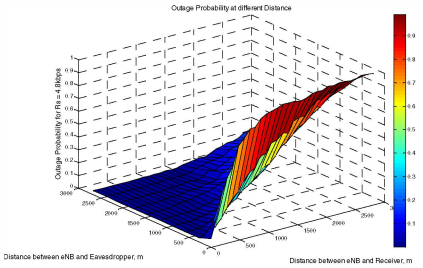
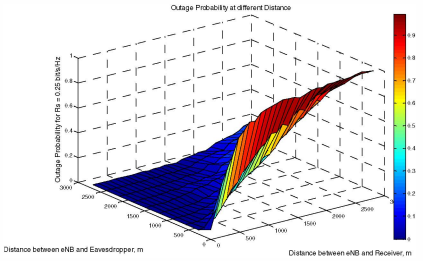


Fig. 4. Secrecy capacity for beamforming scheme

The outage probability for beamforming scheme is depicted in Fig.5. Consider R_S is 4.8 kbps, it can be seen in Fig.5(a) that the outage probability elevates sharply and is greater than 90%, when distance between eNB and eavesdropper is 140m and receiver is 1200m away from eNB.



(a)



(b)

Fig. 5. Outage probability with different R_S for beamforming scheme: (a) secrecy rate is 4.8 kbps; (b) secrecy spectral efficiency is 0.25 bit/s/Hz

Based on above analysis, it can be drawn that the traditional MIMO and beamforming schemes can not guarantee the transmission safety of train control messages when the eavesdropper is close to eNB. Hence AN and other technologies are required to enhance the safety of railway wireless communication system.

Secrecy capacity of proposed scheme is demonstrated in Fig.6. It can be seen that the influence of eavesdropper location changes is not obvious because the transmit directions of beamforming and AN are adjusted with the receiver's CSI and eavesdropper's partial CSI. The secrecy capacity decreases continuously and is consistent with 10^6 bps order of quantity finally.

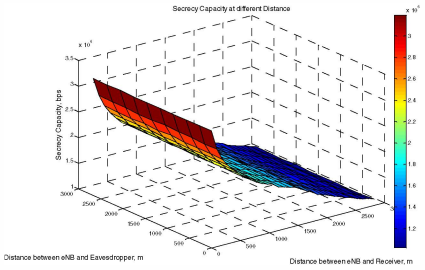
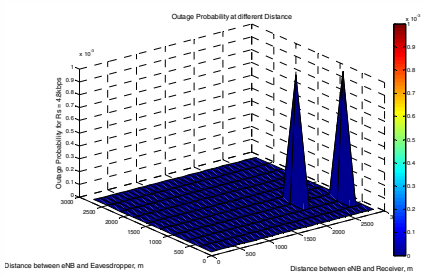
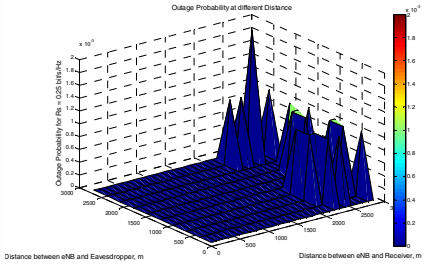


Fig. 6. Secrecy capacity forproposed scheme

Fig.7 plots the outage probability of proposed scheme. It can be seen that the outage probability can be approximated to zero during the whole operation.



(a)



(b)

Fig. 7. Outage probability with different R_S for proposed scheme: (a) secrecy rate is 4.8 kbps; (b) secrecy spectral efficiency is 0.25 bit/s/Hz

VI. CONCLUSION

To improve the traditional MIMO system and guarantee the railway safety, a physical layer secure scheme with AN is proposed. Simulation results demonstrate the proposed scheme can decrease outage probability and meet the requirements of train control systems based on IMT-Advanced. However, the results are under ideal conditions because feedback delay resulted from high mobility is ignored. How to adjust beamforming and AN transmitting directions precisely in high mobility is also unconsidered. In future work, the influences of those factors will be investigated deeply.

REFERENCES

[1] J. Hyun-Jeong, H. Jong-Gyu, S. Seung-Kwon, and K. Yong-Kyu, "Safety guaranteeing method & tool development in railway communication system," in *31st International Telecommunications Energy Conference. INTELEC 2009*, 2009, pp. 1-5.

[2] J. Hyunjeong, B. Jonghyen, L. Kangmi, C. Eunkyung, and K. Yongkyu, "Wireless security method for on-board centered train control system," in *7th International Conference on Computing and Convergence Technology (ICCCT)*, 2012, pp. 88-93.

[3] Z. Zhang, X. Wang, and Y. Zhang, "Study on service-oriented framework of information integration of safety and security for high-speed railway," in *International Conference on Information Networking and Automation (ICINA 2010)*, 2010, pp. V2-307-V2-311.

[4] T. Xiang and A. Bo, "The issues of cloud computing security in high-speed railway," in *International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT 2011)*, 2011, pp. 4358-4363.

[5] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory,* vol. 24, pp. 451-456, 1978.

[6] X. Zhang, X. Zhou, and M. R. McKay, "On the Design of Artificial-Noise-Aided Secure Multi-Antenna Transmission in Slow Fading Channels," *IEEE Transactions on Vehicular Technology,* vol. 62, pp. 2170-2181, 2013.

[7] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Effects of Outdated CSI on the Secrecy Performance of MISO Wiretap Channels with Transmit Antenna Selection," *IEEE Communications Letters,* vol. 17, pp. 864-867, 2013.

[8] J.-B. Wang, M. Feng, X. Song, and M. Chen, "Imperfect CSI Based Joint Bit Loading and Power Allocation for Deadline Constrained Transmission," *IEEE Communications Letters,* vol. 17, pp. 826-829, 2013.

[9] W. Xiyuan, W. Kun, and Z. Xian-Da, "Secure Relay Beamforming With Imperfect Channel Side Information," *IEEE Transactions on Vehicular Technology,* vol. 62, pp. 2140-2155, 2013.

[10] 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, pp. 704-716, 2012.

[11] C. Xu, X. Yuan, L. Ping, and X. Lin, "Power Allocation for Linearly Precoded OFDM Systems with Imperfect CSIT," *IEEE Wireless Communications Letters,* vol. 2, pp. 315-318, 2013.

[12] L. Jiangyuan and A. P. Petropulu, "Ergodic Secrecy Rate for Multiple-Antenna Wiretap Channels With Rician Fading," *IEEE Transactions on Information Forensics and Security,* vol. 6, pp. 861-867, 2011.

[13] J. Meinilä, P. Kyösti, T. Jämsä, and L. Hentilä, "WINNER II Channel Models," *Radio Technologies and Concepts for IMT-Advanced,* pp. 39-92, 2009.

[14] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory,* vol. 54, pp. 2515-2534, 2008.

[15] S. Gerbracht, A. Wolf, and E. A. Jorswieck, "Beamforming for fading wiretap channels with partial channel information," in *International ITG Workshop on Smart Antennas (WSA 2010)*, 2010, pp. 394-401.

[16] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Beamforming for secrecy rate maximization under outage constraints and partial CSI," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, 2011, pp. 193-197.

[17] Z. Xiangyun and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *3rd International Conference on Signal Processing and Communication Systems. ICSPCS 2009*, 2009, pp. 1-5.

[18] UIC ERTMS/GSM-R, "Radio Transmission FFFIS for EuroRadio ", ed, 2010.

[19] ITU-R M.2134, "Requirements related to technical performance for IMT-Advanced radio interface(s) ", ed, 2008.

[20] D. Tse and P. Viswanath, *Fundamentals of wireless communication*: Cambridge university press, 2005.