International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

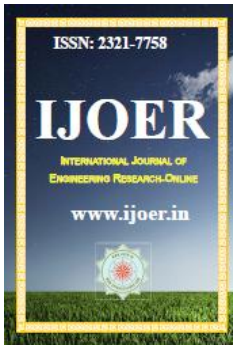
Vol.4., Issue.4., 2016
(July-August)

RESEARCH ARTICLE

ISSN: 2321-7758

SECRECY PERFORMANCE ANALYSIS OF RELAY SELECTION WITH DIFFERENT DIVERSITY

STEFFI JOSE
M.Tech scholar, Department of ECE, Mount zion college of engineering Kadamannitta, Kerala



ABSTRACT
A comprehensive investigation on the secrecy performance of opportunistic relay selection systems employing the decode and forward protocol over Rayleigh fading channels. Considering a practical setting where direct link between the source node (Alice) and the destination node (Bob) is available, we study the secrecy performance of three different diversity combining schemes, namely, maximum ratio combining (MRC), distributed selection combining (DSC), and distributed switch-and-stay combining (DSSC). Throughout the analysis, we consider two different scenarios based on the availability of the eavesdropper's channel state information (CSI), i.e., Scenario A, where the eavesdropper's CSI is not available at Alice and the relay, and Scenario B, where Alice and the relay have knowledge about the eavesdropper's CSI. For Scenario A, we derive exact closed-form expressions for secrecy outage probability and simple asymptotic approximations for the secrecy outage probability, which enable the characterization of the achievable secrecy diversity order and coding gains. For Scenario B, we derive closed-form expressions for the achievable secrecy rates. For both scenarios, we investigate the impact of feedback delay (outdated CSI) on the secrecy performance wherein exact and asymptotic secrecy outage probability and closed-form expressions of the secrecy achievable rates are obtained .

Keywords- Diversity combining, feedback delay, opportunistic relay selection, physical layer security

I. INTRODUCTION

Wireless security is an important issue, which has received enormous attention in recent years. The conventional way of providing security is to apply cryptography which nevertheless faces the problem of key distribution and management, on top of the fact that cryptography does not guarantee perfect secrecy. As such, physical layer security has emerged as a promising technique to address the shortcomings of the cryptography based techniques.

A. Related work

Early works on physical layer security mainly focus on the study of three-node wiretap channel model. In recent years, motivated by the advance of cooperative communication technique applying the cooperative technique to improve the secrecy performance of wireless systems has received significant interests. More recent works have considered the extension of deploying multiple relay for secrecy enhancement. With multiple relays, relay selection technique has been demonstrated as a simple and effective method to improve the system performance. In two new opportunistic relay selection schemes taking into account of the quality of relay-eavesdropper links were proposed, and it was demonstrated that the proposed relay

selection scheme can significantly improve the secrecy outage probability.

B. Technical contributions

The technical contributions of the paper can be summarized as follows:

- With perfect CSI, we investigate three popular destination diversity combining schemes, i.e., MRC, DSC, and DSSC, and present new exact analytical expressions for the key performance measures such as secrecy outage probability and average secrecy rate for all three diversity combining schemes.
- With outdated CSI, we derive new closed-form expressions for the secrecy outage probability and secrecy rate for all three diversity combing schemes. These expressions only involves standard mathematical functions, hence can be easily computed using standard software such as Matlab. As such, they provide an efficient means for the evaluation of the secrecy performance of the system.
- In the high SNR regime, we present simplified approximations for the secrecy outage probability and characterize the secrecy diversity order and coding gain for all three diversity schemes with/without perfect CSI.

II. SYSTEM MODEL

We consider a dual-hop relaying system operating in Rayleigh fading channels, where the source Alice (*A*) communicates with the destination Bob (*B*) with the help of *K* trusted relays (*Rk* denotes the *k*th relay), in the presence of a passive eavesdropper Eve (*E*), who tries to overhear the confidential information intended for *B*. The direct link between *A* and *B* is also considered. In addition, it is assumed that each node of *A*, *B*, *Rk*, and *E* is equipped with a single antenna. The relay operates in the half-duplex mode, hence a complete cycle of information transmission consists of two phases.

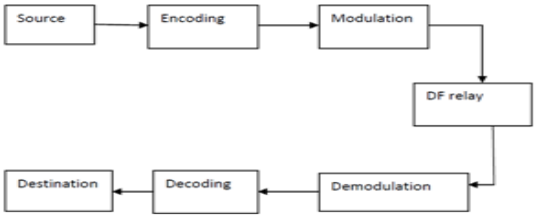


Fig:1 Existing system

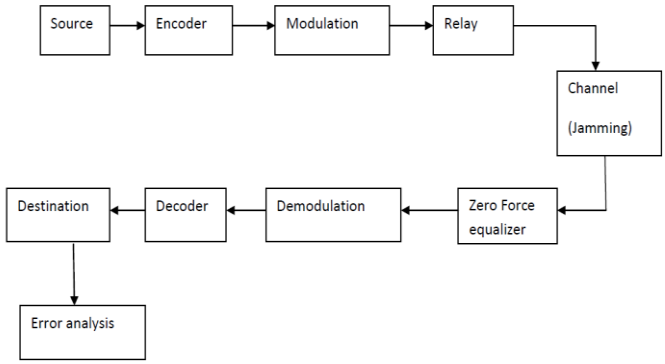


Fig:2 Proposed system

III. SECRECY PERFORMANCE

The exact closed-form expressions are derived for secrecy outage probability and probability of non-zero secrecy capacity. To gain further insights, we also look into the asymptotic secrecy outage probability at high SNR, and characterize the diversity and derive closed form expression of achievable secrecy rate.

A. Secrecy Outage Probability

The secrecy outage probability is defined as the probability of

the secrecy capacity *C*S being less than a predetermined secrecy rate *RS*.

$$P_{Out}(R_s)=\sum_{L=0}^{K}\sum_{DL} P_r\,[D_L]P_r(C_S< R_S\,|D_L)$$

B. Exact achievable secrecy rate

The achievable secrecy rate is defined as the expected value of the instantaneous secrecy capacity *C*S, which can be computed by

$$C=\sum_{L=0}^{K}\sum_{DL} P_r\,[D_L]C_*$$

Where C_* is given by

$$C_*=\frac{1}{2}E[log_2(1+y_*)- log_2(1+y_E]$$

IV. DISCUSSION OF RESULTS

In this section, numerical results are provided to verify our analytical results derived in the previous sections.

Fig. 1 depicts the secrecy outage probability versus $\bar{\gamma}ab$ for the MRC/MRC scheme. As can be observed, the analytical results are in exact agreement with the Monte-Carlo simulation results, which demonstrates the correctness of the derived analytical expressions, and the high SNR approximations are quite accurate. In addition, it can be observed that increasing the number of

relays significantly improves the secrecy outage probability.

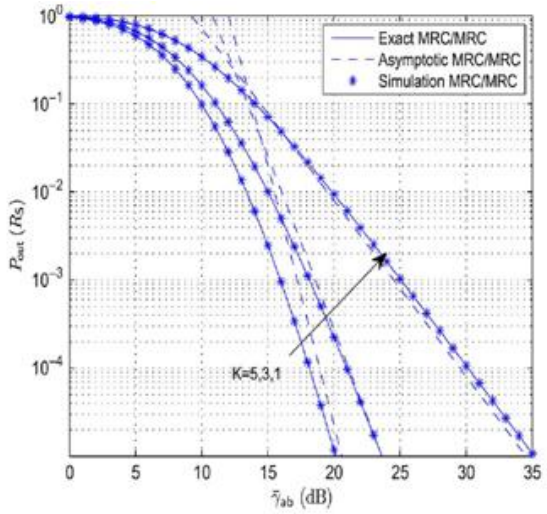


Fig:3 secrecy outage probability of opportunistic relay selection over *RS*=1 and *k*=1,3,5

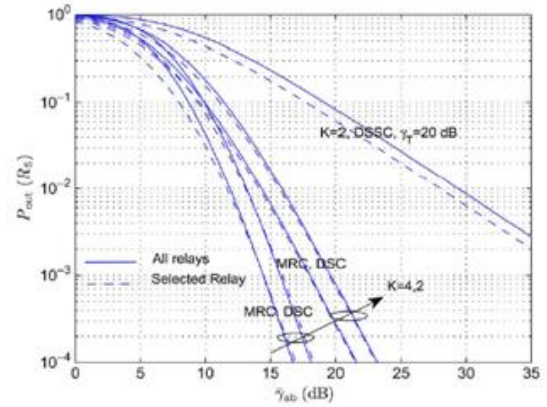


Fig:4 secrecy outage probability of multiple relay over *Rs*=1

Fig. 4 compares the secrecy outage probability of multiple relays and selected relay over Rayleigh fading channels. It can be observed that the secrecy performance of the selected relay outperforms slightly the case when all relays are involved in transmission. This implies that the eavesdropper receive multiple copies of the signal when multiple relays transmit, and hence degrades the secrecy performance.

Fig. 5 compares the achievable secrecy outage probability of three different combining schemes versus MER $\bar{\zeta}$. It can be readily observed that the MRC/MRC and DSC/MRC curves have the same slope, indicating that both schemes achieve the same secrecy diversity order. In addition, the MRC/MRC scheme slightly outperforms the DSC/MRC scheme by achieving slightly better coding gain. On the other hand, the achievable secrecy diversity order of DSSC/MRC scheme is strictly smaller.

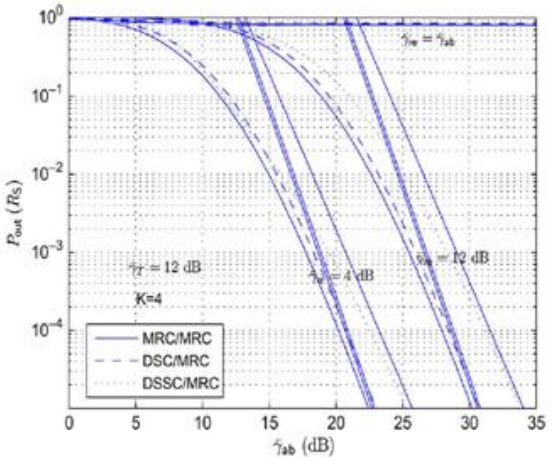


Fig:5 secrecy outage probability of opportunistic relay selection over *K*=5,2

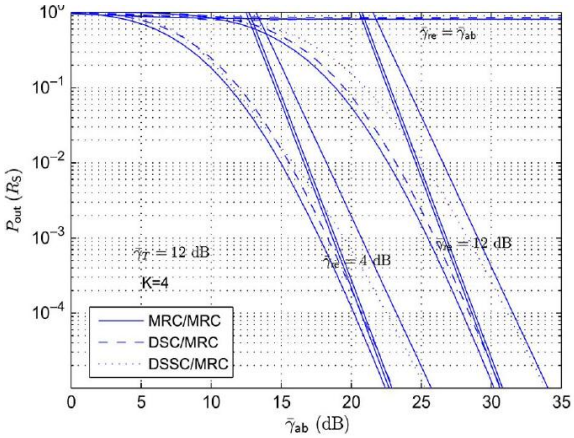


Fig 6 secrecy outage probability of opportunistic relay over *RS*=1

Fig. 6 examines the impact of the quality of the eavesdropper's mchannel on the secrecy performance when *K* = 4. Two distinct scenarios are studied: 1) when the eavesdropper's average channel gains are fixed, i.e., $\bar{\gamma}$ae = {4, 12} dB, 2) when the eavesdropper's average channel gain increases along with aver age channel gain of themain channel, i.e., $\bar{\gamma}$ae = $\bar{\gamma}$ab. Intuitively,the improvement of the quality of the eavesdropper's channel leads to the degradation of the secrecy outage performance. Nevertheless, the performance

degradation is due to reduction of coding gain, not diversity order. On the other hand, for case 2, we see that the secrecy outage probability converges to a constant value when the SNR is large, hence it achieves zero diversity order.

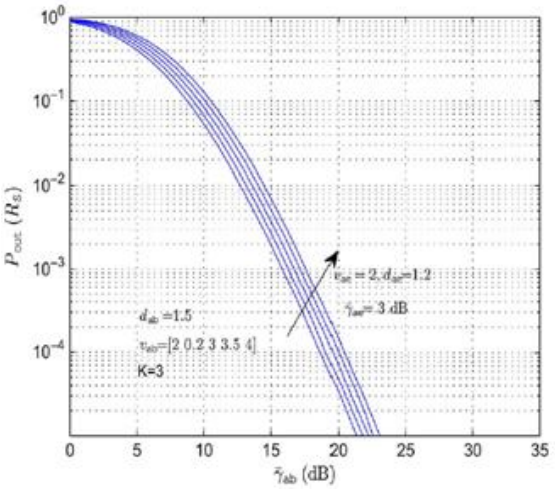


Fig:7 impact of pathloss on the secrecy outage probability of opportunistic relaying over *RS*=1

In Fig. 7, we study the impact of path loss on the secrecy performance of opportunistic relay selection. We define the average channel gain between Alice and Bob as Ωab(Ωrb) = /*d*ab/−*v*ab (/*d*rb/−*v*rb), where *d*ab(*d*rb) denotes the distance between Alice (Relay) and Bob, and *v*ab(*v*rb) is the path loss, and between Alice (Relay) and Eve as Ωae(Ωre) = /*d*ae/−*v*ae (/*d*re/−*v*re). We observe that the secrecy outage probability increases when the value of the path loss becomes larger.Nevertheless, the performance degradation is not substantial.

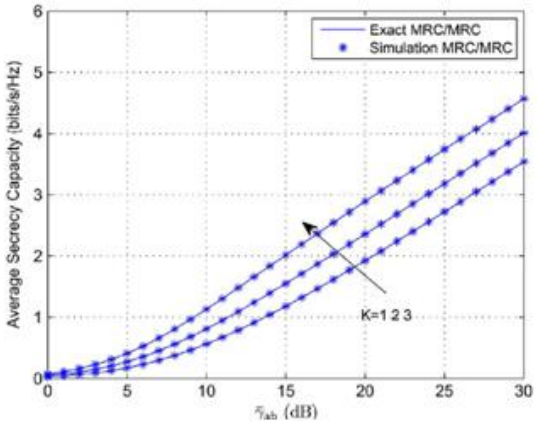


Fig:8 average secrecy outage probability of opportunistic relay selection over *K*=1,2,3

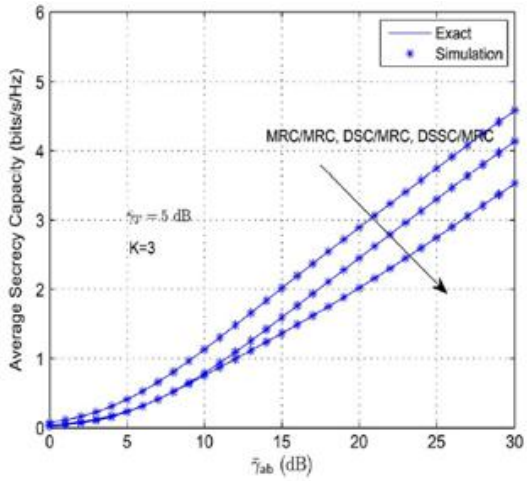


Fig:9 average secrecy outage probability of opportunistic relay selection over *K*=3

Fig. 8and Fig.9 investigates the achievable average secrecy capacity of the system when $\bar{\gamma}_{re}$ = 4 dB. From Fig. 8, it can be observed that increasing the number of relay significantly improves the achievable secrecy capacity. While in Fig. 9, we see that the MRC/MRC scheme always attains the highest secrecy capacity. In addition, at the low SNRs, the DSC/MRC and DSSC/MRC schemes achieve similar secrecy capacity, while at the high SNRs, the DSC/MRC scheme outperforms the DSSC/MRC scheme.

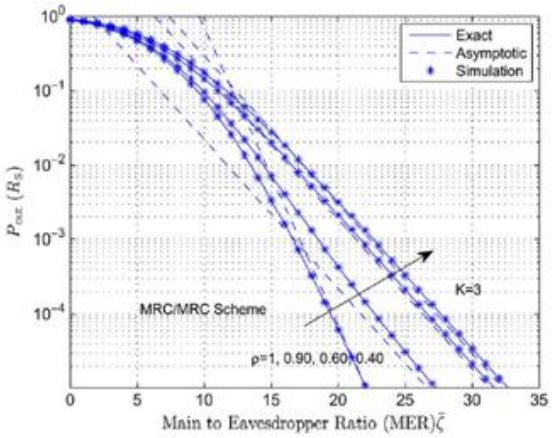


Fig:10 average secrecy outage probability of opportunistic relay selection with feedback delay K=3

Fig. 10 and Fig. 11 illustrates effect of feedback delay on the secrecy outage probability when *K* = 3. As can be readily observed, full diversity order of four is achieved only if *ρ* = 1, which corresponds to the case with no feedback delay.

When ρ = 0.90, 0.60, 0.40, the achievable diversity order of the MRC/MRC scheme reduces to two to the reference MER $\overline{\zeta}$.Fig. 11 compares the secrecy outage probability of the proposed three schemes with ρ = 0.60 and K = 3. Similarly, we see that the performance gab between the MRC/MRC and DSC/MRC scenarios is rather small, which is similar to the case with no feedback delay. In contrast, the performance gap between the MRC/MRC scheme and the DSSC/MRC scheme is substantial, indicating that the outdated feedback have a significant detrimental impact on the secrecy performance of DSSC/MRC scheme.

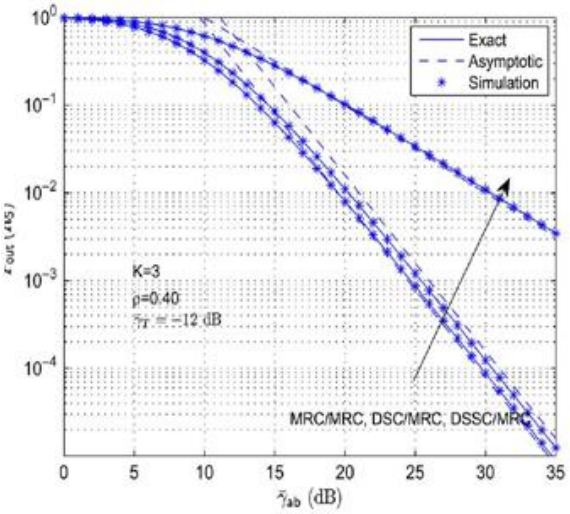


Fig:11 secrecy outage probability of dual hop DF trusted selected relay

V. CONCLUSIONS

Secrecy performance of opportunistic relay selection employing the decode-and-forward protocol over Rayleigh fading channels .Considered two practical scenarios based on the eavesdropper's CSI availability including Scenario A: when Alice and the relay have no knowledge about the eavesdropper's CSI, and Scenario B: when both Alice and the relay have knowledge about the eavesdropper's CSI. For Scenario A, we presented new analytical expressions for the secrecy outage probability. In addition, in the high SNR regime, asymptotic expressions were presented for the secrecy outage probability, which facilitate the characterization of secrecy diversity order and coding gain. For Scenario B, we derived closed-form of feedback delay (outdated CSI) on the secrecy performance was examined for both scenarios.

REFERENCES

[1] Yulong ZOU and Jia Zhu,"Relay selection for wireless communication against eavesdropping" ," IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Dec. 2014.

[2] Lifeng and Nan Yang" Physical layer security of maximal ratio combining in two wave diffuse power fading channel IEEE J. Sel. Areas Commun., vol. 6, no. 20, pp. 2099–2111, Feb 2014

[3] Jing Huang and A.Lee " Wireless physical layer security enhanced with buffer aided relaying IEEE J. Sel. Areas Commun., vol.9, no. 18, pp. 2099–2111,june 2013

[4] C. Cai, Y. Cai, W. Yang, and W. Yang, "Average secrecy rate analysis with relay selection using decode-and-forward strategy in cooperative networks," in Proc. WCSP, Hangzhou, China, Oct. 2013, pp. 1–4.

[5] Y. Zou, X.Wang, andW. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," IEEE J. Sel. Areas Commu *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.