Optimization Analysis of Max-Link Secure Relay Selection in Buffer-Aided Cooperative Networks

Yajun Zhang*, Jun Wu and Bing Wang
Army Academy of Artillery and Air Defense (Nanjing Campus), Nanjing, China

*Corresponding author email: yajun2000@foxmail.com

Abstract. Cooperative communication technology has been proved to be an useful approach to accomplish physical layer security. In recent years, more and more attention has been paid to the collaboration network with buffer relay. This paper studies the safety performance of the maximum link level options. Compared with the existing buffer-assisted cooperative security schemes, max-Link secure relay selection (Max-Link-SRS) does not require the eavesdropper's channel state information (CSI) and has a lower complexity. Based on markov chain theory, a new closed form expression of secure interrupt probability (SOP) is derived. Numerical simulation results confirm our analysis and demonstrate that the functioning of max-Link-SRS is superior to the previously reported buffer-less aided cooperative security scheme. It provides a significant coding obtain at a smaller buffer size, while ensuring diversity gain is close to the upper limit of the double number of relays at a bigger buffer zone.

1. Introduction
In recent years, more and more attentiveness has been paid to physical layer security (PLS). The basic concept of PLS is to use the physical properties of wireless channels, such as noise or fading, traditionally considered interference, to prevent eavesdropping attacks with lower computational overhead and improve transmission reliability. In Wyner's pioneering research [1], the maximum non-zero news delivery rate was defined as the ability of the sender to reliably send a secret information to the intended recipient when the pirate listener could not decode it. Until then, lots of articles and studies have been presented from different perspectives in the literature [1].

Many studies have shown that collaborative communication not only supply an effective way to make confidentiality better, but also greatly reform the transmission capacity of wireless networks [2-3]. By elaborately designing the relay, the information rate of the destination is maximized and the information rate of the eavesdropper is minimized, thus improving the security of the system. In recent years, buffer-assisted collaboration networks have attracted much attention due to their significant performance advantages [4]. At the relay end, the requirement that both the relay to destination and the optimal source-receiver link must be determined simultaneously can be relaxed by introducing a data buffer. With the development of buffer-assisted relay technology, literature [4-6] proposed buffer-assisted relay to ensure the safety of physical layer. In literature [5] and [6], a two-hop and half-duplex relay network composed of source (Alice), buffer assisted decoding and forwarding (DF) relay, destination (Bob) and eavesdrop (Eve) is considered. A link option scheme is studied by settling two optimization problems with two-hop transmission effectiveness and confidentiality constraints. Different from literature [5] and [6], this paper [4] studies multi-relay scenarios and proposes a new buffer-assisted direction-finding relay network with maximum relay option security transmission scheme. The scheme has a bug, which can intercept the signal of the relay node and the source node simultaneously. The results show that the
function of the maximum ratio relay option scheme is superior to the traditional maximum and minimum ratio strategy, and it is proved to be an attractive security method. In this paper, a simple buffer-assisted collaboration scheme, namely Max-Link-SRS, is studied. Inspired by literature [8], this scheme aims to ensure the security of buffer-assisted collaboration networks. Compared with the previous work, the main contributions are as follows:

- Differing from [7], we examined multi-relays scenario, as the increasing of the relay’s number, the performance will be better. Comparing to the paper [7], our Max-link SRS scheme doesn’t need to know any of the eavesdropper’s CSI, it reduces the complexity under acceptable performance loss.
- A new SOP closed form expression is derived based on the Markov chain method used to analyse outage performance.
- We study the average delay of the recommended maximum link SRS scheme. The results show that with the growing of the number of relays and buffer zone, the average time delay will be longer the slots’ number.

2. System Model and Max-link Secure Relay Selection (max-link-SRS) Scheme

The buffer-assisted direction-finding relay selection system model considered is shown in Figure 1, where it has a destination node (Bob), a source node (Alice), relay nodes (R, 1 ≤ k ≤ K), and an eavesdropper (Eve). All the panel joint work in half duplex mode, that means they don’t send and accept meantime. Each repeater is weaponed with a data buffer \( Q_k \) (1 ≤ k ≤ K) of a finite width \( L \) (in terms of data packets). Packets follow a first-in, first-out rule in the buffer.

**Figure 1.** Relay selection secure transmission system model.

Similar to [11], we assume that relay and Alice are in one cluster, while Eve and Bob are in another cluster [6-7]. In this condition, there is indirect link between the Alice-Eve and Bob-Alice channels, and communication can only depend on relay. At time \( t \), the channel coefficients of \( A \rightarrow R_k \), \( R_k \rightarrow B \) and \( R_k \rightarrow E \) are respectively expressed as \( h_{A,R_k}(t) \), \( h_{R_k,B}(t) \) and \( h_{R_k,E}(t) \). When CSI is available with the exact knowledge of Alice and the relay, and the routeway between the relay and Bob, as in [9], the Max-Link security option can be displayed as

\[
R^* = \arg \max_{k} \left\{ \max_{\Psi(Q_k) \leq L} \left[ h_{A,R_k} \right] \cdot \max_{\Psi(Q_k) \leq L} \left[ h_{R_k,B} \right] \right\}
\]

where \( R^* \) represents the chosen relay (for receiving or transmitting), and \( \Psi(Q_k) \) gives data packets’ number in buffer \( Q_k \).

In time slot \( t \), without losing generality, we suppose that \( A \rightarrow R_k \) is the selected link, so the source sends packet \( x(t) \) to the \( R_k \). In \( R_k \), the signal is received by

\[
y_{A,R_k}(t) = \sqrt{P_k} h_{A,R_k}(t) x(t) + n_{R_k}(t)
\]
where $n_k(t)$ is the extra AWGN noise at relay $R_k$, and $y_{A,R_k}(t)$ is stored in buffer $Q_k$, waiting for the turn to be transmitted. Suppose in the next $\tau$-th slot, $y_{A,R_k}(t)$ is forwarded from $R_k$ to the target node. When using the DF collaboration scheme, the relay processes $y_{A,R_k}(t)$ by decoding the estimated $\hat{x}(t)$ of the signal sent by the source. The signals received by Bob and Eve at the time slot $(t+\tau)$ are respectively by,

$$
y_{R_k,B}(t+\tau) = \sqrt{P_k} h_{R_k,B}(t+\tau) \hat{x}(t) + n_B(t+\tau)$$

(3)

$$
y_{R_k,E}(t+\tau) = \sqrt{P_k} h_{R_k,E}(t+\tau) \hat{x}(t) + n_E(t+\tau)
$$

(4)

where $n_B(t+\tau)$ and $n_E(t+\tau)$ are AWGN of relay Bob and Eve $E$ respectively.

The capacity of direction-finding transmission relay is the minimum capacity from relay to destination and from source to relay [5], because failure of relay destination or source relay link will result in failure of two-hop decoded forward (DF) transmission. Therefore, the confidential capacity of DF relay transmission with $R_k$ as the selected relay and $R_k$ as the buffer auxiliary is given by [6],

$$
C_i = C_{A,R_k,B} - C_{B,E} = \frac{1}{2} \log_2 \left( \frac{1 + \min \{ y_{A,R_k}(t), y_{R_k,E}(t+\tau) \} }{1 + y_{R_k,E}(t+\tau)} \right)
$$

(5)

where $y_{R_k,E}(t+\tau)$ and $y_{R_k,B}(t+\tau)$ are the instantaneous SNR (ISNR) of link $R_k \rightarrow E$ and $R_k \rightarrow B$ at time $t+\tau$ respectively.

3. Secrecy Outage Probability (SOP) Analysis

SOP is named as the probability that the successful confidentiality rate is less than the target confidentiality rate. If the probability is not higher than the target confidentiality rate, the safe transmission cannot be guaranteed. Therefore, this SOP can be expressed as [1]

$$
P_{ou}(R_i) = \Pr(C_i < R_s)
$$

(6)

where $R_s$ is the target secrecy rate.

Similar with the theoretical framework of paper [8], in the max-link relay option scheme, data packets’ number in each buffer form a “state” at any time, and all states can form a state Markov chain (MC). Because $K$ available relays exist, and each relay is provided with a buffer of zone L, which have $(L+1)^K$ states in total. The $l$-th state is explained as,

$$
s_l \triangleq (\Psi(Q_1)\Psi(Q_2)\ldots\Psi(Q_K)), \quad l \in \mathbb{N}_K, 1 \leq l \leq (L+1)^K
$$

(7)

States are defined randomly as a combination of all possible buffer sizes ($((L+1)^K$), and the transition probability between them is a key factor in deducing the secret interrupt probability. Let $A$ represent the $(L+1)^K \times (L+1)^K$ state transition matrix of markov chain, from state $s_j$ of time $t$ to state $s_i$ of time $(t+1)$, where entry $A_{i,j} = p(s_j \rightarrow s_i) = p(X_{i+1} = s_j | X_t = s_j)$ is the probability. The transition probability relays on the relative number of links available to participate in the relay selection decision and on each buffer (the state relay buffer). More specifically, a relay node with a complete or vacuous data buffer can’t receive or send data separately, i.e., $\Psi(Q_s) = 0$ or $\Psi(Q_s) = L$, so in both cases it provides only one link during the chosen process; When $\Psi(Q_s) = 0$, $k$-th relay provides link $S \rightarrow R_s$, while $\Psi(Q_s) = L$ provides link $R_s \rightarrow D$. Otherwise, the relay node provides two links for choice.
(S → R₁, R₁ → D) and can be used for transmission or reception. Therefore, the available links’ total number in the \( s_i \) state of the buffer participating in the maximum link chosen process is equivalent to

\[
D_i = \sum_{i=1}^{K} \Phi(Q), \quad \text{where} \quad \Phi(Q) = \begin{cases} 
2 & \text{if } 0 < \Psi(Q) < L; \\
1 & \text{elsewhere.}
\end{cases}
\]  

(8)

So as to obtain the matrix \( A \), we demand to determine the connectivity in the different states of buffer. For every time slot, the state of the buffer can be changed to the following three situations:

- when the source node is chosen for transfer and the transfer is achievable, the elements’ number in the buffer can be increased by one,
- when a relay node is chosen for transfer and the transfer is successful, the elements’ number in the relay buffer can be reduced by one,
- When an interrupt occurs (for example, a repeater is chosen for transmission and the relay destination link is in an interrupted state, or a source is chosen for transmission and the selected source relay link is in an interrupted state), the buffer state remains unchanged.

We define an association set \( U_i \) for \( s_i \) states to represent the above buffer state connectivity, which is given by

\[
U_i = \bigcup_{s_{L+2} \subset \Theta} \{ s_i : s_i - s_j \in \Theta \}
\]

(9)

where \( \Theta \equiv \{ U_{1s} \} \} \) number of stored elements in each buffer and \( s_i \) represents a \( 1 \times K \) vector whose terms are \( s_j \) state. According to the previous connection rules, set \( U_i \) includes all buffer states linked to state \( s_i \). For the calculation of transition probability from one to another, we should consider the following factors:

- Through the maximum link chosen process, the corresponding channel links was selected,
- The selected link was successfully transmitted without interruption.

Assuming identically and independent distributed (i.i.d.) symmetric channel connection, for \( s_i \) buffer state, the possibility of selecting a particular link is equivalent to \( 1/D_i \), and the probability can be calculated using sequence statistics [12], that is, the selected link is not in a secure interrupt state. Therefore, the probability of an interrupt event, i.e. the buffer state does not change, is equivalent to

\[
\bar{P}_{D_i} = 2\lambda_b \sum_{k_i=0}^{D_i} \left( \frac{(-1)^{k_i} e^{-\lambda_b k_i [2^2 L - 1]}}{ \lambda_b k_i 2^{2k_i} + \lambda_e} - \lambda_e \sum_{k_2=0}^{2D_i} \left( \frac{(-1)^{k_2} e^{-\lambda_b k_2 [2^2 L - 1]}}{ \lambda_b k_2 2^{2k_2} + \lambda_e} \right) \right)
\]

(10)

The probability of leaving from the condition \( s_i \) is equivalent to

\[
P_{D_i} = \frac{1}{D_i} \left( 1 - 2\lambda_b \sum_{k_i=0}^{D_i} \left( \frac{(-1)^{k_i} e^{-\lambda_b k_i [2^2 L - 1]}}{ \lambda_b k_i 2^{2k_i} + \lambda_e} \right) + \lambda_e \sum_{k_2=0}^{2D_i} \left( \frac{(-1)^{k_2} e^{-\lambda_b k_2 [2^2 L - 1]}}{ \lambda_b k_2 2^{2k_2} + \lambda_e} \right) \right)
\]

(11)

where \( \lambda_b = 1/\Omega_{R,E}, \ \Omega_{R} = \Omega_{A,R} = \Omega_{R,B}, \) and \( \lambda_e = 1/\Omega_{e} \).

Using the previous notation, the \( A \) can be given as follows

\[
A_{i,j} = \begin{cases} 
\bar{P}_{D_i} & \text{if } s_i \not\in U_j, \\
p_{D_i} & \text{if } s_i \in U_j, \\
0 & \text{elsewhere, for } i, j \in \{1, \ldots, (L+1)^K\}
\end{cases}
\]

(12)
Since the $A$ in (8) is irreducible, aperiodic and random in columns, the steady-state possibility vector can be obtained as follows (refer to [8] and [7]).

$$\pi = (A - I + B)^{-1} b$$

(13)

where $b = [1,1,\ldots,1]^T$, $B_{ij} = 1, \forall i,j$, $\pi = [\pi_1, \ldots, \pi_{(L+1)p}]^T$, is the stationary distribution.

Finally, substituting (13) and (14) into (6), and rewrite the SOP as

$$P_{out}(R_i) = \sum_{j=0}^{(L+1)p} \pi_j p_{D_j} = \text{diag}(A) \pi$$

(14)

where $\text{diag}(A)$ is a vector, which consist of whole elements of transition matrix $A$.

4. Discussions

4.1. Performance of Extreme Case with Infinite Size Buffers ($L \rightarrow \infty$)

For extreme cases with an infinite size buffer ($L \rightarrow \infty$), analogous to the analysis in Section V-B in [11], the SOP can be simplified to

$$P_{out}^\infty = P_{2,K}$$

(15)

4.2. Performance of Average Packet Delay

In the relay nodes in the Max-Link scheme, the average packet delay can be received by Little law [10]: the average queue length is obtained by multiplying the average delay by the throughput. Here, we omit the analysis process. In the case that the relaying to destination and sourcing-relaying channel are symmetric, which is the assumption of this paper, the total average delay becomes,

$$E(T) = 1 + KL$$

(16)

In the next section, some simulation examples are provided, it illustrates the right of (16), to illustrate the average packet delay for Max-link SRS scheme.

5. Simulation Results

In this part, the SOP of max-Link safe relay option scheme in DF buffer auxiliary collaboration network is simulated. Compared with the existing non-buffered auxiliary DF coordination schemes such as T-DFBORS and P-DFBORS, the performance of the improved scheme is presented. In the simulation, we normalized all noise variances and transmitted power to one, and set the instantaneous channel gain of relaying to destination and transmitting from source to relay as $\gamma_{AR} = \gamma_{AR_i} = \gamma_{R_i} R_i$.

Figure 2 compares the proposed Max-Link SRS with the SOP of the existing T-DFBORS and P-DFBORS schemes. We can see that in the figure, the performance of Max-Link-SRS is significantly better than other non-buffered auxiliary schemes, indicating that code gains can be obtained through buffering [8]. In addition, the theoretical curves agree well with montecarlo simulation results for different buffer widths, which verifies the accuracy of the analysis. Finally, it can be observed that for the Max-Link SRS scheme, when the size of buffer rises, the value of $A$ will gradually decrease and gradually approach the performance limit, which further proves the rightness of our theoretical analysis. In Figure 3, we plotted the relationship between the SOP of the maximum link SRS scheme and the size of $L$ (repeater buffer), for $K=2$ Repeaters, $\gamma_{KE} = 5$dB, $R_i = 1$ and $\gamma_{AR} = 10, 20, 30$dB; The buffer zone $L$ ranges from [1-50] and is equivalent to a low-complexity real-world scenario [8]. As you can see, the performance gained as the buffer size growing is close to the chosen bound. We can get that a relatively small buffer (e.g., $L = 30$ for $\gamma_{AR} = 20$dB ) is sufficient to achieve optimal SOP. However, With the
increase of main channel’s SNR, the required value of length $L$ increase (e.g., $L = 5$ for $\gamma_{AR} = 10$dB; $L = 30$ for $\gamma_{AR} = 20$dB and $L > 50$ for $\gamma_{AR} = 30$dB).

Figure 2. $P_{out}(R_s)$ versus $\gamma_{AR}$ for different DF secure schemes at $K = 2$, $\gamma_{RE} = 5$dB and $R_s = 1$.

Figure 3. $P_{out}(R_s)$ versus $L$ for max-link SRS scheme at $K = 2$, $\gamma_{RE} = 5$dB and $R_s = 1$.

Figure 4. $P_{out}(R_s)$ versus $\gamma_{AR}$ for different relays’ number at $L = 2$, and $R_s = 1$.

Figure 5. Average delay in number of time slots versus buffers size for different relays’ number at $\gamma_{AR} = 10$dB, $\gamma_{RE} = 5$dB, $L = 2$, and $R_s = 1$.

Figure 4 shows $P_{out}(R_s)$ and $\gamma_{AR}$ with different relays at $L = 2$ and $R_s = 1$. First of all, we can notice that the theoretical curve is in good agreement with the Monte Carlo simulation results for different relay numbers, which verifies the accuracy of the analysis. Secondly, the research shows that $P_{out}(R_s)$ value is enhanced when the eavesdropper’s channel SNR is reduced, which is the congruous with the case without buffer assistance. Finally, for the proposed maximum link SRS scheme, we also observe that the value of $P_{out}(R_s)$ goes down with the increase of the relays number, mainly because the larger $K$ is, the larger the secure diversity order (SDO) is.

Figure 5 depicts the relationship between average time delay and buffer size in different scenarios to give the concept of average time delay. The theoretical curves are in good consistent with monte Carlo simulation consequence. In addition, it can be seen that with the increase of relays, the average delay increases, mainly because the probability of selecting a particular relay for transmission decreases. Moreover, as the size of buffer grows, the probability of a full relay decreases, and the probability of selecting a specific relay reduces, resulting in a growth in the average delay. As shown in figures 2 and
4. diversity performance improves with an increase in relay number K or buffer size L by tolerating higher latency.

6. Conclusion
This paper studies the safety performance SOP of the maximum link SRS scheme in buffer assisted DF collaboration networks. A new closed SOP expression is derived and the average postpone of the proposed maximum link SRS scheme is studied. We concluded that compared with the existing buffer auxiliary security scheme, under the acceptable performance losses, the 1) Max - link SRS without buffer auxiliary scheme performs better than previously reported, it provides a significantly smaller buffers of coding gain, while ensuring the diversity gain is close to the big buffer size relay twice the upper limit of the number; 2) The larger the relays number and the buffer size, the longer the average time delay in slot. Secondly, a partial channel knowledge (partial CSI) and a method to consider the delay constraint are proposed.

References
[1] Furqan H M, Hamamreh J M and Arslan H 2019 A Comprehensive Survey: Classifications and Applications of Physical Layer Security Techniques for Confidentiality vol 21 (IEEE Commun. Surveys & Tutorials) pp 1773-1828
[2] Petropulu A P, Jiangyuan L, and Weber S 2011 On Cooperative Relaying Schemes for Wireless Physical Layer Security vol 59 (IEEE Trans. on Signal Processing) pp 4985-4997
[3] Xianbin W, Yulong Z, and Weiming S 2013 Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks vol 31 (IEEE J. Selected Areas in Communications) pp. 2099-2111
[4] T, Yu G, Gaojie C, Zhao Zhi C, and Chambers J A 2014 Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks vol 9 (IEEE Trans. on Information Forensics and Security) pp 719-729
[5] Ikhlief A, Zlatanov N, Islam T, and Schober R 2008 Buffer-aided cooperative communications: opportunities and challenges vol 52 (IEEE Commun. Mag.) pp 146-153
[6] Yijia F, Bing X, Thompson J, and Poor H V 2008 Buffering in a Three-Node Relay Network vol 7 (IEEE Trans. Wireless Commun.) pp 4492-4496
[7] IkMichalopoulos D S, hlef A, and Schober R 2012 Max-Max Relay Selection for Relays with Buffers vol. 11 (IEEE Trans. Wireless Commun.) pp 1124-1135
[8] Charalambous T, Krikidis I, and Thompson J S 2012 Buffer-Aided Relay Selection for Cooperative Diversity Systems without Delay Constraints vol 11 (IEEE Trans. Wireless Commun.) pp 1957-196
[9] Liu J, He J, Shen Y, Jiang X and Shiratori N 2020 Link Selection for Security-QoS Tradeoffs in Buffer-Aided Relaying Networks vol 15 (IEEE Trans. Inf. Forensics Secur.) pp 1347-1362
[10] Little J D C and Graves S C 2008 Little’s law vol 115 (International Series in Operations Research & Management Science) pp 81–100
[11] Tian Z, Chen G, Gong Y, and Chambers J 2014 Decode-and-Forward Buffer-Aided Relay Selection in Cognitive Relay Networks vol. 63 (IEEE Trans. on Vehicular Technology) pp 4723-4728
[12] Ryzhik I M and Gradshteyn I S 2007 Table of Integrals, Series, and Products, 7th Edition ed (Academic).