Max-ratio relay selection in secure buffer-aided cooperative wireless networks

This item was submitted to Loughborough University's Institutional Repository by the/an author.


Additional Information:

- This is an Open Access Article. It is published by the IEEE under the Creative Commons Attribution 3.0 Unported Licence (CC BY). Full details of this licence are available at: http://creativecommons.org/licenses/by/3.0/. Research data for this paper is available on request from the authors.

Metadata Record: https://dspace.lboro.ac.uk/2134/14510

Version: Published

Publisher: © the authors. Published by IEEE

Please cite the published version.
This item is distributed via Loughborough University’s Institutional Repository (https://dspace.lboro.ac.uk/) and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by/3.0/
Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks

Gaojie Chen, Member, IEEE, Zhao Tian, Student Member, IEEE, Yu Gong, Member, IEEE, Zhi Chen, Member, IEEE, and Jonathon A. Chambers, Fellow, IEEE

Abstract—This paper considers the security of transmission in buffer-aided decode-and-forward cooperative wireless networks. An eavesdropper which can intercept the data transmission from both the source and relay nodes is considered to threaten the security of transmission. Finite size data buffers are assumed to be available at every relay in order to avoid having to select concurrently the best source-to-relay and relay-to-destination links. A new max-ratio relay selection policy is proposed to optimize the secrecy transmission by considering all the possible source-to-relay and relay-to-destination links and selecting the relay having the link which maximizes the signal to eavesdropper channel gain ratio. Two cases are considered in terms of knowledge of the eavesdropper channel strengths: exact and average gains, respectively. Closed-form expressions for the secrecy outage probability for both cases are obtained, which are verified by simulations. The proposed max-ratio relay selection scheme is shown to outperform one based on a max-min-ratio relay scheme.

Index Terms—Secure wireless communications, cooperative networks, relay selection, secrecy capacity.

I. INTRODUCTION

TRADITIONALLY security in wireless networks has been focused on higher layers using cryptographic methods [1]. However, retaining security at high layers is becoming more challenging due to the increased potential for attack, therefore, there has been growing interest in implementing security at the physical layer. Related work was described as early as in the 1970s [2]–[5], and more recently for physical layer security in wireless communications [6]–[10]. The purpose of physical layer security is to prevent eavesdroppers from intercepting the data transmitted between the source and intended destination. The secrecy is quantified by the secrecy capacity, or the maximum rate of reliable information sent from the source to the intended destination in the presence of eavesdroppers [5]. Recent research shows that cooperative communication not only significantly improves the transmission capacity for wireless networks (e.g. [11] and [12]), but also provides an effective way to improve the secrecy capacity. This is achieved by carefully designing the relays to maximize the information rate at the intended destination and minimize that at the eavesdroppers [13]. In general, there are three ways to improve the secrecy capacity in a cooperative network:

- Distributed beamforming - The secrecy capacity can be maximized by optimizing the transmission weights (or the beamforming weights) at the relay and source nodes (e.g. [14] and [15]). Such distributed beamforming however requires high coordination (such as synchronization and central optimization) among source and relay nodes, which usually requires high overhead in implementation, i.e. a large amount of information needs to be exchanged between the relay nodes.
- Jamming - A jammer is used to inject artificial interference into the system. When the injected interfering power is higher at the eavesdroppers than that at the intended destination, the secrecy capacity can be improved (e.g. [16]–[18]). This often requires the jammer to be located closer to the eavesdroppers than to the destination node, which is not always possible in practice.
- Relay selection - Relay selection can increase the secrecy capacity by choosing an appropriate relay node with “strong” transmission link to the intended destination node and “weak” link to the eavesdropper [19]–[22]. The relay selection provides an attractive way to improve the secrecy capacity with little overhead in implementation. The performance of the relay selection depends strongly on the number of available links for selection, which again depends on not only the number of relays but also the relay selection scheme. When the number of available links is limited, so is the secrecy performance. Thus it is important to investigate relay selection schemes to have the best secrecy performance for a given number of relays, which is the main objective of this paper.

In traditional relay selection to improve wireless communications, the best relay is selected with the strongest link connecting the source and destination (e.g. [23] and [24]). It is shown in [19] that by using relay selection the secrecy capacity can also be improved when the best relay is selected...
to maximize the signal to eavesdropper channel gain ratio, which is abbreviated as the “gain ratio” in this paper. The relay selection scheme in [19] is based on the scenario that the eavesdropper can only intercept the signals from the relays but not the source node. On the other hand, if the eavesdropper intercepts signals from both the relay and source nodes, the best relay is selected as having the maximum secrecy capacity among every pair of source-to-relay and relay-to-destination links [18], which is termed as the max-min-ratio scheme in this paper. Alternatively, it is also possible to select a jammer from the available relays (e.g., [20]), but this is at the price of injecting more interference not only to the intended receivers but also to other users in the system. As was shown in [20], including a jammer does not necessarily lead to improvement in secrecy capacity, and thus a switching scheme was described to activate/deactivate the jammer.

Recent research shows that, by introducing data buffers at the relays, it is possible to relax the constraint that the best source-to-relay and relay-to-destination links for a packet transmission must be determined concurrently, and achieve significant performance advantage [25]–[30]. A typical buffer-aided relay selection is the max-max scheme described in [27], where the strongest source-to-relay and relay-to-destination links are selected alternatively so that it has significant coding gain over the traditional max-min scheme. Because the max-max relay selection still follows the traditional transmission order, that is the source-to-relay and relay-to-destination transmissions always carry on in an alternative manner, it can only attain a diversity order of N which is the same as that for the max-min scheme, where N is the number of available relay nodes. In the recent max-link approach [25], this constraint on the transmission order is further relaxed so that, at any time, a best link is selected among all available source-to-relay and relay-to-destination links. Depending on whether a source-to-relay or a relay-to-destination link is selected, either the source transmits a packet to the selected relay or the selected relay forwards a stored packet to the destination. It is shown in [25] that the max-link relay selection not only has coding gain over the max-min scheme, but also has higher diversity order than both the max-min and max-max schemes. In particular, the diversity order can approach 2N when the relay buffer size is large enough.

Inspired by the max-link scheme, in this paper, we propose a novel max-ratio relay selection scheme for secure transmission in decode-and-forward (DF) relay networks with an eavesdropper which can intercept signals from both the source and relay nodes. In the proposed max-ratio scheme, every relay is equipped with a data buffer, and the best link is always selected with the highest gain ratio among all available source-to-relay and relay-to-destination links. We consider two cases for which either the exact, or the average gain, for the eavesdropping channel is available; the latter case is of particular interest in practice since it is not always possible to obtain the exact channel information describing the eavesdropping channels. Both theoretical and simulation results show that the proposed max-ratio relay selection has significantly better performance than the conventional max-min-ratio scheme, confirming that it represents an attractive approach for secure wireless transmission. The main contributions of this paper are summarized as follows:

- **Propose the buffer-aided max-ratio relay selection policy for secure communications in a DF cooperative network.** This is the first approach in using buffer-aided relay selection in secure transmission under the scenario that the eavesdropper can intercept signals from both the source and relay nodes. Existing relay selection schemes for secure transmission mainly assume no source-to-eavesdropper link for simplicity (e.g., [19]). While in [22] both the source and relay to eavesdropper links are considered, the proposed scheme is for the two-way relay network and furthermore no closed form expression is obtained for the secrecy outage probability.

- **Derive closed-form expressions for the secrecy outage probability of the max-ratio scheme for both cases when either the exact, or average, gains of the eavesdropping channels are available.** Because the gain-ratios for the source-to-relay and relay-to-destination transmissions have different statistical distributions, the secrecy outage performance of the proposed max-ratio scheme is much more involved to analyze than existing approaches such as the relay selection scheme for secure transmission in [19] and the buffer-aided max-link scheme for wireless communications in [25]. In this paper, the problem arising from such “unbalanced” distribution has been successfully solved, and the analysis also provides a useful way in analyzing similar systems such as a typical relay selection scheme but without the usual assumption that the source-to-relay and relay-to-destination channels are independent and identically distributed (i.i.d.).

The remainder of the paper is organized as follows: Section II describes the system model; Section III proposes the max-ratio relay selection scheme; Sections IV and V analyze the secrecy outage probability for the cases with exact and average knowledge of the eavesdropping channels, respectively; Section VI discusses the performance of the max-ratio scheme when the relay buffer sizes go to infinity; Section VII gives numerical simulations to verify the proposed max-ratio scheme; finally, Section VIII summarizes the paper.

II. SYSTEM MODEL

The system model of the relay network with an eavesdropper is shown in Fig. 1, where there is one source node (S), one destination node (D), a set of K relays {R1, R2, . . . , RK}, and one eavesdropper (E) which can intercept signals from both the source and relay nodes. The relay nodes apply the DF protocol and perform the half-duplex mode so that they do not transmit and receive simultaneously.

In our model, we assume no direct link between the source and the destination due to path loss or shadowing effects. 1 The channel coefficients for $S \rightarrow R_k$, $S \rightarrow E$, $R_k \rightarrow D$ and $R_k \rightarrow E$ at time $t$ are denoted as $h_{sk}(t)$, $h_{se}(t)$, $h_{rk}(t)$ and $h_{rk}(t)$ respectively, where similar subscripts are also used for other parameters to indicate different channels in

1 Including the direct link has little effect on the relay selection which is the main issue in this paper.
this paper. We assume the channels are quasi-static Rayleigh fading so that the channel coefficients remain unchanged during one packet duration but independently vary from one packet time to another. We also assume that all source-to-relay links are independent and identically distributed (i.i.d.) fading and that $E[h_{k}(t)] = \gamma_{k}$ for all $k$; all relay-to-destination channel gains are also i.i.d. and $E[h_{rd}(t)] = \gamma_{rd}$, as are all relay-to-eavesdropper channel gains for which $E[h_{re}(t)] = \gamma_{re}$. The source-to-eavesdropper channel gain is denoted as $E[h_{se}(t)] = \gamma_{se}$. It is noted that we do not require any two of $\gamma_{kr}, \gamma_{rd}, \gamma_{se}$ and $\gamma_{re}$ to be the same, thereby representing a “practical” scenario. All noises are additive white Gaussian noise (AWGN), and without losing generality the noise variances are all normalized to unity. The transmission powers for source and relay nodes are all assumed to be $E_s$.

With the DF applied at the relays, if the relay $R_k$ is selected for the data transmission, the instantaneous secrecy capacity for the overall system is obtained as [31]

$$C_k(t) = \max \left\{ \frac{1}{2} \log_2 \frac{1 + E_s |h_{se}(t)|^2}{1 + E_s |h_{se}(t)|^2 + E_s |h_{re}(t)|^2} \right\}$$

(1)

If the exact knowledge of the eavesdropping channels are available, the best relay node can be selected with the maximum $C_k(t)$. On the other hand, if only the average gains of the eavesdropping channels are known, the best relay maximizes $C_k(t)$ with $|h_{se}(t)|^2$ and $|h_{re}(t)|^2$ being replaced with the average gains $\gamma_{se}$ and $\gamma_{re}$ in (1) respectively. This scheme is termed as the max-min-ratio relay selection in this paper.

For convenience in development, the time index $t$ is ignored in the rest of the paper unless necessary.

III. MAX-RATIO RELAY SELECTION

The performance of the max-min-ratio scheme is limited by the constraint that the best source-to-relay and relay-to-destination links must be determined concurrently. In this paper, we propose a new max-ratio selection scheme by making use of data buffers at the relays. To be specific, we assume that every relay is equipped with a data buffer $Q_k$ ($1 \leq k \leq K$) of finite size $L$ (in the number of data packets), and the data packets in the buffer follow the “first-in-first-out” rule.

At any time, the best transmission link with the highest gain-ratio is selected among all available source-to-relay and relay-to-destination links. Depending on the knowledge of the eavesdropper channel, we have two selection criteria:

**Case 1** - If the exact knowledge of all channels, $h_{se}$ and $h_{re}$, are available, the max-ratio selects the best relay as

$$R_{case 1}^{(max-ratio)} = \arg\max_{R_k} \left\{ \max_{K: \Psi(Q_k) \neq L} \left\{ \frac{|h_{se}|^2}{|h_{rd}|^2} \right\}, \max_{R_k: \Psi(Q_k) \neq 0} \left\{ \frac{|h_{re}|^2}{|h_{rd}|^2} \right\} \right\},$$

(2)

where $\Psi(Q_k)$ gives the number of data packets in buffer $Q_k$.

**Case 2** - If only the average channel gains for the eavesdropping channels, i.e. $\gamma_{se}$ and $\gamma_{re}$, are available (but the exact knowledge for all other channels is known), the best relay for the max-ratio scheme is selected as:

$$R_{case 2}^{(max-ratio)} = \arg\max_{R_k} \left\{ \frac{\max_{K: \Psi(Q_k) \neq L} \left\{ |h_{se}|^2 \right\}}{\gamma_{se}}, \frac{\max_{R_k: \Psi(Q_k) \neq 0} \left\{ |h_{re}|^2 \right\}}{\gamma_{re}} \right\}.$$  

(3)

A. Secrecy Outage Probability

The secrecy outage probability is defined as $P_{out} = P(C < r_{sc})$, where $C$ is the instantaneous secrecy capacity, $r_{sc}$ is the target secrecy capacity and $P(.)$ gives the probability of the enclosed. In the max-ratio relay selection scheme, at any time, the numbers of data packets in every buffer form a “state”. Because there are $K$ available relays and every relay is equipped with a buffer of size $L$, there are $(L+1)^K$ states in total. The $l$-th state vector is defined as

$$s_l = [\Psi_l(Q_1), \ldots, \Psi_l(Q_K)]^T, \quad l = 1, \ldots, (L+1)^K,$$

(4)

where $\Psi_l(Q_k)$ gives the number of data packets in buffer $Q_k$ at state $s_l$. It is clear that $0 \leq \Psi_l(Q_k) \leq L$. Every state corresponds to one pair of $(K_1, K_2)$, where $K_1$ and $K_2$ are the numbers of available links for source-to-relay and relay-to-destination transmission, respectively. A source-to-relay or a relay-to-destination link is considered available when the buffer of the corresponding relay node is not full or not empty respectively. It is clear that $0 \leq K_1 \leq K$ and $0 \leq K_2 \leq K$. Specifically, if none of the buffers is full or empty, all links are available such that $K_1 = K_2 = K$.

At state $s_l$, the best link is selected among all $K_1$ source-to-relay and $K_2$ relay-to-destination links. We denote $p_{out}^{s_l}$ as the outage probability for state $s_l$. Considering all possible states, we obtain the secrecy outage probability for the max-ratio relay selection as

$$P_{out} = \sum_{l=1}^{(L+1)^K} \pi_l \cdot p_{out}^{s_l},$$

(5)

The CSI is usually estimated through pilots and feedback (e.g. [32]), and the CSI estimation without feedback may also be applied (e.g. [33]). Further detail of the CSI estimation is beyond the scope of this paper.
where $\pi_l = p(s_l)$ which is the stationary probability for state $s_l$.

### B. State Transition Matrix

Suppose at time $t$, the state for the relay buffers is $s_l$. At time $(t+1)$, there is one relay selected for either receiving or transmitting a data packet, so that the number of packets in the corresponding buffer is increased or decreased by one respectively. Depending on which relay receives or transmits data, at time $(t+1)$, the buffers may move from state $s_l$ to several possible states, forming a Markov chain. We denote $A$ as the $(L + 1)^K \times (L + 1)^K$ state transition matrix, where the entry $A_{n,l} = P(X_{t+1} = s_n | X_t = s_l)$ is the transition probability that the state moves from $s_l$ at time $t$ to $s_n$ at time $(t+1)$.

If the secrecy outage event occurs, the state $s_l$ remain unchanged at time $(t+1)$. Otherwise, $s_l$ moves to another state. Thus the probability for $s_l$ to leave for another state is given by

$$p_{l}^{\text{leave}} = 1 - p_{l}^{\text{stay}}. \quad (6)$$

It is clear from the selection rules (2) and (3) that, for both Cases 1 and 2, the probabilities to select the source-to-relay and relay-to-destination transmission at any time are not the same. This is very different from the max-link approach in [25] where the selection of any available link is equally likely. We denote $p_{l}^{\text{stay}}$ and $p_{l}^{\text{out}}$ as the probabilities that the source-to-relay link is selected and $U^{-}_{l}$ contains all states to which $s_l$ can move when a relay-to-destination link is selected and $U^{+}_{l}$ contains all states to which $s_l$ can move when a source-to-relay link is selected.

On the other hand, because we assume all source-to-relay channels are i.i.d. fading and all relay-to-destination channels are i.i.d. frequency flat fading and so are the relay-to-eavesdropper channels, the selection of one particular link within either $U^{+}_{l}$ or $U^{-}_{l}$ is equally likely. Therefore, the probability to select a source-to-relay or relay-to-destination link at state $s_l$ is given by

$$p_{l}^{\text{stay}} = p_{l}^{\text{leave}} \left( \frac{1}{K} p_{l}^{\text{stay}} \right) = \frac{1}{K} \left( 1 - p_{l}^{\text{out}} \right) \left( 1 - p_{l}^{\text{out}} \right),$$

and

$$p_{l}^{\text{out}} = p_{l}^{\text{leave}} \left( \frac{1}{K} p_{l}^{\text{out}} \right) = \frac{1}{K} \left( 1 - p_{l}^{\text{out}} \right) p_{l}^{\text{out}}, \quad (7)$$

respectively.

With these observations, the $(n,l)$-th entry of the state transition matrix $A$ is expressed as

$$A_{n,l} = \begin{cases} 
    p_{n}^{\text{out}}, & \text{if } n = l, \\
    \frac{1}{K} \left( 1 - p_{l}^{\text{out}} \right) \left( 1 - p_{l}^{\text{out}} \right), & \text{if } s_n \in U^{+}_{l}, \\
    \frac{1}{K} \left( 1 - p_{l}^{\text{out}} \right) p_{l}^{\text{out}}, & \text{if } s_n \in U^{-}_{l}, \\
    0, & \text{elsewhere.}
\end{cases} \quad (8)$$

Because the transition matrix $A$ in (8) is column stochastic, irreducible and aperiodic, the stationary state probability vector is obtained as (see [35] and [36])

$$\pi = (A - I + B)^{-1} b, \quad (9)$$

where $\pi = [\pi_1, \ldots, \pi_{(L+1)^K}]^T$, $b = (1, 1, \ldots, 1)^T$, $I$ is the identity matrix and $B_{n,l}$ is an $n \times l$ all one matrix.

Finally, substituting (8) and (9) into (5) re-formats the secrecy outage probability as

$$P_{\text{out}} = \sum_{l=1}^{(L+1)^K} \pi_l \cdot p_{l}^{\text{out}} = \text{diag}(A) \cdot \pi$$

$$= \text{diag}(A) \cdot (A - I + B)^{-1} b, \quad (10)$$

where $\text{diag}(A)$ is a vector consisting of all diagonal elements of $A$.

It is clear from (10) that the secrecy outage probability $P_{\text{out}}$ is determined by $A$ which, again, from (8), is determined by $p_{l}^{\text{out}}$ and $p_{l}^{\text{out}}$. The secrecy outage probabilities for both Cases 1 and 2 can be expressed as (10), but with different $p_{l}^{\text{out}}$ and $p_{l}^{\text{out}}$ which are derived below.

### IV. CASE 1 - EXACT KNOWLEDGE OF EAVESDROPPING CHANNELS

In Case 1, we assume exact knowledge for the instantaneous gains for all channels, including the eavesdropping channels. This is a typical assumption in many existing approaches (e.g. [20] and [21]).

#### A. $p_{l}^{\text{out}}$: Outage Probability at State $s_l$ for Case 1

The relay selection rule for Case 1 is shown in (2). For better exposition, we let $x = \max_{\psi(Q_i) \neq L} \{|h_{sr}x^2|, h_{sk}x^2\}$, $y = \psi(Q_i) \neq 0$ and $z = \max(x, y)$. In order to concentrate on the secrecy capacity, we assume the channel SNR is high enough so that the decoding is always successfully at the relay and destination nodes. The probability of outage event at state $s_l$ at the high SNR is given by

$$p_{l}^{\text{out}} = P(z < 2^{\frac{1}{2} \gamma_{l}}) = F_{Z}(z)|_{z = 2^{\frac{1}{2} \gamma_{l}}}, \quad (11)$$

where $F_{Z}(z)$ is the cumulative-probability-function (CDF) of $z$ which is derived below.

Recall that state $s_l$ corresponds to $(K_1, K_2)$. From the theory of order statistics [37], if the number of available source-to-relay links is $K_1$, the CDF of $x_1 = \max \{|h_{sr}x^2|, h_{sk}x^2\}$ is given by

$$F_{X_1}(x) = [1 - e^{-\frac{x}{\theta}}]^K_1, \quad (12)$$

Noting that $x = x_1/|h_{sr}x^2|$, the CDF of $x$ is then obtained as

$$F_{X}(x) = \sum_{i=0}^{K_1} C_{K_1} \left( -\frac{1}{1 + M} \right) \frac{M}{1 + M}, \quad (13)$$

3 Column stochastic means all entries in any column sum up to one, irreducible means that it is possible to move from any state to any state, and aperiodic means that it is possible to return to the same state at any steps [34], [35].

4 This is a typical assumption in most existing secure communications literature (e.g. [19], [20]).
where \( C_{K_1}^{i} = K_1^i / [i!(K_1 - i)!] \) which is the binomial coefficient, and \( M_1 = \gamma_{sr} / \gamma_{se} \) which is the average gain ratio between the source-to-relay and source-to-eavesdropper channels.

On the other hand, because the number of available relay-to-destination links is \( K_2 \), the CDF of \( y \) is given by

\[
F_Y(y) = \left[ \frac{y}{M_2 + y} \right]^{K_2},
\]

where \( M_2 = \gamma_{rd} / \gamma_{se} \) which is the average gain ratio between the relay-to-destination and relay-to-eavesdropper channels.

Because \( x \) and \( y \) are mutually independent, from (13) and (14), the CDF of \( z = \max(x, y) \) is obtained as:

\[
F_Z(z) = F_X(z)F_Y(z) = \sum_{i=0}^{K_1} C_{K_1}^{i} (-1)^{i} \frac{M_1}{i^2 \gamma_{se} + M_1} \left[ \frac{z}{M_2 + z} \right]^{K_2}.
\]

Substituting (15) into (11) gives

\[
p_{out}^{ii} = \sum_{i=0}^{K_1} C_{K_1}^{i} (-1)^{i} \frac{M_1}{i^2 \gamma_{se} + M_1} \left[ \frac{2^{2\gamma_{se}}}{M_2 + 2^{2\gamma_{se}}} \right]^{K_2}.
\]

The next subsection will provide the probability of selecting the relay to destination transmission at state \( s_l \).

B. \( p_{out}^{R-D} \): Probability of Selecting the Relay-to-Destination Transmission at State \( s_l \) for Case 1

If there are no relay-to-destination links available (or \( K_2 = 0 \)), we have \( p_{out}^{R-D} = 0 \). On the other hand, if there are no source-to-relay links available (or \( K_1 = 0 \)), we have \( p_{out}^{R-D} = 1 \). For other cases, \( p_{out}^{R-D} \) is obtained in Appendix I. In summary, we have obtained \( p_{out}^{R-D} \) (17), as shown at the bottom of the page, where \( B(x, y) = \int_{0}^{1} t^{x-1} (1 - t)^{y-1} \) which is the Beta function and \( F_{2,1}(a, b, c, z) \) is the first hypergeometric function. Finally, substituting (16) and (17) into (10) gives the secrecy outage probability at the high SNR for Case 1.

V. Case 2 - Knowledge of the Average Channel Gains for Eavesdropping Channels

In case 2, we only have knowledge of the average gains for eavesdropping channels, while the exact information for all other channels is still available.

A. \( p_{out}^{ii} \): Outage Probability at State \( s_l \) for Case 2

We let \( u_{ab} = |h_{ab}|^2 / \gamma_{ab} \) be the normalized gain for channel \( h_{ab} \), where \( \{ab\} \in \{sr_k, se, r_kd, r_ke\} \). Because of the normalization, all \( u_{ab} \) have the same probability-density-distribution (PDF) as

\[
f_U(u) = e^{-u},
\]

The selection rule in (3) can then be expressed as

\[
K_b^{(2)} = \arg \max_{R_k} \left[ \max_{\{s_kr_k, s_kd, s_ke\}} \left[ M_1 \cdot u_{sr_k} \right] \right],
\]

where \( M_1 \) and \( M_2 \) are defined in (13) and (14), respectively. We further let \( f = \max_{R_k; \Psi(Q) \neq L} \left[ M_1 \cdot u_{sr_k} \right] \) and \( g = \max_{R_k; \Psi(Q) \neq 0} \left[ M_2 \cdot u_{rd} \right] \). It is clear that \( w \) is directly obtained from the selection rule (3) which is based on the average gain of the eavesdropping channels. On the other hand, the secrecy outage is determined by the instantaneous gains of the data and eavesdropping channels. Therefore, in order to obtain the outage probability, \( w \) needs to be divided by \( u \) which is normalized exponentially distributed with PDF given by (18). Or the outage probability for state \( s_l \) for Case 2 is given by

\[
p_{out}^{ii} = P(w < 2^{2\gamma_{se}}) = F_V(v)_{v=2^{2\gamma_{se}}},
\]

where \( v = w/u \).

The CDF-s of \( f \) and \( g \) are given by

\[
F_f(f) = \left[ 1 - e^{-f/M_1} \right]^{K_1} \text{ and } F_G(g) = \left[ 1 - e^{-g/M_2} \right]^{K_2},
\]

respectively. Because \( f \) and \( g \) are mutually independent, the CDF of \( w = max\{f, g\} \) is obtained as

\[
F_W(w) = F_F(w)F_G(w) = \left[ 1 - e^{-w/M_1} \right]^{K_1} \left[ 1 - e^{-w/M_2} \right]^{K_2}.
\]

Then the CDF of \( v = w/u \) is

\[
F_V(v) = \int_{0}^{\infty} \left[ 1 - e^{-uv/M_1} \right]^{K_1} \left[ 1 - e^{-uv/M_2} \right]^{K_2} e^{-u} du
\]

\[
= \sum_{i=0}^{K_1} \sum_{j=0}^{K_2} C_{K_1}^{i} C_{K_2}^{j} (-1)^{i+j} \frac{M_1 M_2}{v(M_2i + M_1j) + M_1 M_2}.
\]
Substituting (23) into (11) gives

\[
p_{\text{out}}(s_i) = \sum_{k_1} \sum_{k_2} C_{k_1}^{i} C_{k_2}^{i} (-1)^{i+j} \frac{M_1 M_2}{2^{2r_{\text{avg}}(M_2 i + M_1 j) + M_1 M_2}}.
\]

(24)

The next subsection will provide the probability of selecting the relay to destination transmission at state \(s_i\).

B. \(p_{\text{R}}^{R\rightarrow D}\): Probability of Selecting the Relay-to-Destination Transmission at State \(s_i\) for Case 2

Similar to that in Case 1, we have \(p_{s_i}^{R\rightarrow D} = 0\) for \(K_2 = 0\), and \(p_{s_i}^{R\rightarrow D} = 1\) for \(K_1 = 0\). But otherwise, we have

\[
p_{s_i}^{R\rightarrow D} = P(f < g) = \int \int f_{FG}(f, g) df dg,
\]

where \(f_{FG}(f, g)\) is the joint PDF of \(f\) and \(g\).

From (21), the PDFs of \(f\) and \(g\) are obtained as

\[
f_f(f) = \frac{K_1}{M_1} e^{-\frac{f}{M_1}} (1 - e^{-\frac{f}{M_1}})^{K_1-1},
\]

\[
f_g(g) = \frac{K_2}{M_2} e^{-\frac{g}{M_2}} (1 - e^{-\frac{g}{M_2}})^{K_2-1},
\]

(26)

respectively. Because \(f\) and \(g\) are mutually independent, we have \(f_{FG}(f, g) = f_f(f) f_g(g)\).

Substituting (26) into (25) gives (27), as shown at the bottom of the page. Therefore, we have \(p_{s_i}^{R\rightarrow D}\) in (28), as shown at the bottom of the page. Finally, substituting (24) and (28), into (10) gives the secrecy outage probability at high SNR for Case 2.

VI. DISCUSSION

In this section, we consider a specific scenario that the average gain ratios for the source-to-relay and relay-to-destination transmissions are the same, or \(M_1 = M_2\). Of particular interest is the outage performance for \(L \rightarrow \infty\) which shows the best potential performance for the max-ratio scheme.

First, we consider Case 2. Because \(M_1 = M_2\), the probabilities to select a source-to-relay and relay-to-destination link are the same, and both equal \(1/(K_1 + K_2)\). This is similar to the max-link scheme in [25]. Thus, building upon the analysis in [25], we can obtain that, if \(L \rightarrow \infty\), the stationary probability for any state corresponding to \(K_1 \neq K\) or \(K_2 \neq K\) must be 0, or we have

\[
\sum_{s_i; K_1 = K_2 = K} P(s_i) = 1.
\]

(29)

This implies that, if \(L \rightarrow \infty\), at any time, the best link is always selected from \(K_1 + K_2 = 2K\) available channels with the max-ratio scheme in Case 2.

In Case 1, unfortunately, we cannot have a simple form as in (29) for \(L \rightarrow \infty\), because the probabilities to select a source-to-relay and relay-to-destination link are not equal, even with \(M_1 = M_2\). In order to illustrate the performance for \(L \rightarrow \infty\), the original scheme can be assumed to be equivalent to a virtual relay section scheme having equal probability to select a source-to-relay and relay-to-destination link, or \(P(x < y) = 0.5\) where \(x\) and \(y\) are defined in Section IV-A.

Then in the virtual scheme with \(L \rightarrow \infty\), the number of available source-to-relay and relay-to-destination links are always \(K_1'\) and \(K_2'\), respectively, or \(\sum_{s_i; K_1 = K_1', K_2 = K_2'} P(s_i) = 1\). If we let \(K_1' = K\), then \(K_2'\) can be obtained by solving \(P(x < y) = 0.5\) as (30), as shown at the bottom of the page, where \(P(x < y)\) is given by (35) in the Appendix I.

Since \(K_2'\) obtained from (30) is usually not an integer, the virtual selection scheme cannot be realized in practice. However, it provides interesting insight in understanding the secrecy performance of the original max-ratio scheme in Case 1 for \(L \rightarrow \infty\). Normally, we have \(K_2' < K\), which implies that, on the average, the best link is always selected from \(K_1' + K_2'\) available channels at any time and \(K \leq K_1' + K_2' \leq 2K\).

For both Case 1 and 2, with a limited buffer size \(L\), we always have \(K_1 + K_2 \geq K\) at any time. On the contrary, in the max-min-ratio selection scheme, the best link is selected from only \(K\) links. Therefore, it follows that the max-ratio scheme has significantly better secrecy outage performance than the benchmark max-min-ratio scheme, and the best potential performance for the max-ratio scheme is reached when \(L \rightarrow \infty\).

This will be verified the next section.

VII. NUMERICAL RESULTS

In this section, simulation results are given to verify the secrecy outage probabilities for the proposed max-ratio relay selection scheme. Both Case 1 and 2 are considered. In the
Fig. 2. The secrecy outage probabilities for different relay selection schemes. (a) Case 1. (b) Case 2.

Fig. 3. The secrecy outage probabilities of the max-ratio scheme for Cases 1 and 2.

Fig. 4. The secrecy outage probabilities of the max-ratio scheme for different relay numbers $K$. (a) Case 1. (b) Case 2.

In every simulation below, both theoretical and simulated secrecy outage probabilities are shown to essentially perfectly match, where the theoretical results are based on (10) and simulation results are obtained by averaging 5,000,000 independent runs. This verifies the closed-form secrecy outage probabilities obtained in this paper.

Fig. 2 compares the secrecy outage performance of the proposed max-ratio scheme with those for the no relay selection and the traditional max-min-ratio schemes, where the relay number is set as $K = 5$ in all relay selection schemes. It is clearly shown that the no relay selection scheme has the worst outage performance and the proposed max-ratio has the best. It is interesting to observe that, for both Cases 1 and 2, with buffer size $L = 1$, the max-ratio still performs significantly better than the max-min-ratio scheme. We highlight that the max-min-ratio scheme is effectively also equipped with a buffer of size 1, because the relays need to store the decoded data at one time and transmit out at the next time. However, even with $L = 1$, the max-ratio does not reduce to the max-min-ratio scheme. This is because, for any relay receiving a data packet in the max-ratio scheme, it has the choice of whether to transmit the packet out at the next time or not.
On the contrary, the relays in the max-min-ratio schemes do not have such choices. Therefore, the max-ratio scheme has “coding gain” over the max-min-ratio approach. On the other hand, with $L \to \infty$, the best potential performance of the max-ratio is reached, which is clearly shown in Fig. 2(a) and (b) for both Case 1 and 2 respectively.

Fig. 3 compares the secrecy outage probabilities of the max-ratio scheme for Cases 1 and 2, where the buffer size is fixed at $L = 3$, the average gain ratios are set as $M_1 = M_2 = 2$ or 5, and the relay number is set as $K = 2$ or 5. It is clearly shown that the max-ratio scheme in Case 1 has consistently better performance than that in Case 2.

Fig. 4 compares the secrecy outage probabilities of the max-ratio scheme for different numbers of relays, where the buffer size is fixed as $L = 5$ and the average gain ratios are set as $M_1 = M_2 = 5$. It is clearly shown that, in both cases, the increase of the relay number can significantly improve the secrecy outage performance. For example, for the target secrecy capacity $\gamma_{se} = 0.5$, when the relay number is increased from $K = 2$ to $K = 5$, the secrecy outage probability decreases by approximately 10 dB in Case 1, and by almost 6 dB in Case 2. This verifies the effectiveness of using the max-ratio relay selection in improving the secrecy performance.

Fig. 5 compares the secrecy outage probabilities of the max-ratio scheme for different relay buffer sizes $L$. (a) Case 1. (b) Case 2.

Fig. 6. The secrecy outage probabilities vs SNR, where $\gamma_{se} = \gamma_{re} = 30$ dB and target secrecy capacity is unity. (a) Case 1. (b) Case 2.
secr eny outage probability is already very close to that for
$L \to \infty$.

Fig. 6 shows the secrecy outage probabilities vs the SNR
for the proposed max-ratio scheme. It is clear that, in both
Cases 1 and 2, the secrecy outage probability improves
significantly with increased number of the relay nodes.

VIII. CONCLUSION

This paper proposed a new max-ratio relay selection policy
for secure buffer-aided cooperative DF networks. With the help
of buffers at the relays, the best relay was selected with the
largest gain ratio among all available source-to-relay and relay-
to-destination links. Both cases with knowledge of exact and
average gain for eavesdropping links were considered, and for
the first time, in the challenging secure transmission context,
closed-form expressions for the secrecy outage probabilities
for both cases were derived. Both analysis and simulations
show that the proposed max-ratio relay selection has sig-
ificantly better performance in secrecy outage probability
than the benchmark max-min-ratio scheme, and provides an
attractive way to realize and improve secure transmission at
the physical layer of wireless communications.

APPENDIX I
PROOF OF (17)

Noting the definition of $x$ and $y$ in Section IV-A, we have

$$p_{S_i}^{R \to D} = P(x < y) = \int_{x < y} f_{XY}(x, y) dxdy$$

$$= \int_{0}^{\infty} \int_{0}^{y} f_{XY}(x, y) dxdy, \quad (31)$$

where $f_{XY}(x, y)$ is the joint PDF of $x$ and $y$.

From the CDF-s of $x$ and $y$ given by (13) and (14)
respectively, the PDF-s of $x$ and $y$ are obtained as

$$f_X(x) = \sum_{i=0}^{K_1} C_{K_1}^i (-1)^{i+1} M_1 i \frac{1}{(M_1 + ix)^{2}} \quad \text{and} \quad f_Y(y) = \frac{y^{K_1-1} K_2 M_2}{(M_2 + y)^{K_2+1}}. \quad (32)$$

respectively. Because $x$ and $y$ are mutually independent, we have

$$f_{XY}(x, y) = f_X(x) f_Y(y) = \sum_{i=0}^{K_1} C_{K_1}^i (-1)^{i+1} \frac{M_1 M_2 K_2 (iy)^{K_2-1}}{(M_1 + ix)^{2}(M_2 + y)^{K_2+1}}. \quad (33)$$

Substituting (33) into (31) gives

$$p_{S_i}^{R \to D} = \int_{0}^{\infty} \int_{0}^{y} \left[ \sum_{i=0}^{K_1} C_{K_1}^i (-1)^{i+1} \frac{M_1 M_2 K_2 iy^{K_2-1}}{(M_1 + ix)^{2}(M_2 + y)^{K_2+1}} \right] dxdy$$

$$= 1 + \sum_{i=1}^{K_1} C_{K_1}^i (-1)^{i} M_1 M_2 K_2 \int_{0}^{\infty} \frac{y^{K_2-1}}{(M_1 + iy)(M_2 + y)^{K_2+1}} dy. \quad (34)$$

Then according to [38], if $K_2 > 1$, we obtain

$$p_{S_i}^{R \to D} = 1 + \sum_{i=1}^{K_1} C_{K_1}^i (-1)^{i} M_1 \frac{1}{M_2} K_2 B(2, K_2)$$

$$\mathcal{F}_{2,1}\left(\{K_2 + 1, K_2\}, K_2 + 2, 1 - \frac{M_1}{M_2}\right); \quad (35)$$

if $K_2 = 1$ and $M_1 = M_2$, we have

$$p_{S_i}^{R \to D} = 1 - K_1/2 + \sum_{i=2}^{K_1} C_{K_1}^i (-1)^{i} \frac{i[\ln(i) - 1] + 1}{(i - 1)^2}; \quad (36)$$

and if $K_2 = 1$ and $M_1 \neq M_2$, we have

$$p_{S_i}^{R \to D} = 1 + \sum_{i=1}^{K_1} C_{K_1}^i (-1)^{i} M_1$$

$$i\ln(i) M_2 + i\ln(M_2) M_2 - i\ln(M_1) M_2 - i M_2 + M_1$$

$$(M_1 - i M_2)^2. \quad (37)$$

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers and the
editor for their constructive comments.

REFERENCES

based key management in mobile ad hoc networks: Techniques and applications,”


interference and broadcast channels with confidential messages: Secrecy
rate regions,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2493–2507,
June 2008.

less information-theoretic security,” IEEE Trans. Inf. Theory, vol. 54,


fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492,

of fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 10,

[8] Y. Liang and H. V. Poor, “Multiple-access channels with confidential

models,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2437–2452,

over fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 6,

selective feedback design for multicell cooperative networks,”

multiplexing loss through successive relaying using repetition coding,”
IEEE Trans. Wireless Commun., vol. 6, no. 12, pp. 4484–4493,

infrastructure-aided cooperation,” IEEE Trans. Inf. Forensics Security,


Jonathon A. Chambers (S’83–M’90–SM’98–F’11) received the Ph.D. and D.Sc degrees in signal processing from the Imperial College of Science, Technology, and Medicine (Imperial College London), London, U.K., in 1990 and 2014, respectively. From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Center, Cambridge, U.K. In 1994, he returned to Imperial College London, as a Lecturer in signal processing and was promoted as a Reader (Associate Professor) in 1998. From 2001 to 2004, he was the Director with the Centre for Digital Signal Processing and a Professor of signal processing with the Division of Engineering, King’s College London, London. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Wales, U.K. In 2007, he joined the Department of Electronic and Electrical Engineering, Loughborough University, Loughborough, U.K., where he heads the Advanced Signal Processing Group and serves as the Associate Dean (Research) for Loughborough University. He is a coauthor of the books Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures, and Stability (Hoboken, NJ, USA: Wiley, 2001) and EEG Signal Processing (Hoboken, NJ, USA: Wiley, 2007). He has advised more than 50 researchers through to Ph.D. graduation and published more than 350 conference proceedings and journal articles, many of which are in IEEE journals. His current research interests include adaptive and blind signal processing, and their applications. He is a fellow of the Royal Academy of Engineering, U.K., and the Institution of Electrical Engineers. He was the Technical Program Chair of the 15th International Conference on Digital Signal Processing and the 2009 IEEE Workshop on Statistical Signal Processing, both held in Cardiff, U.K., and a Technical Program Cochair for the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing, Prague, Czech Republic. He received the first QinetiQ Visiting Fellowship in 2007 for his outstanding contributions to adaptive signal processing and his contributions to QinetiQ as a result of his successful industrial collaboration with the international defense systems company QinetiQ. He has served on the IEEE Signal Processing Theory and Methods Technical Committee for six years, the IEEE Signal Processing Society Awards Board for three years, and is currently a member of the IEEE Signal Processing Conference Board and the European Signal Processing Society Best Paper Awards Selection Panel. He has served as an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING for three terms from 1997 to 1999, from 2004 to 2007, and since 2011, and is currently a Senior Area Editor.