Outage Performance Comparison of Adaptive Relaying Schemes Subject to Jamming

Van-Lan Dao, Svetlana Girs, and Elisabeth Uhlemann
Malardalen University,Västerås, Sweden, {van.lan.dao,svetlana.girs,elisabeth.uhlemann}@mdu.se

***Abstract*—Proper relay selection (RS) plays a key role for improving the reliability of wireless networks, especially in the presence of jamming attacks and/or interferers. In this work, we consider several RS schemes from the literature, using e.g. channel gains and signal-to-interference plus noise ratio (SINR) to select a relayer and evaluate them using outage probability (OP). We also propose an RS scheme which is selecting relayers to maximize the communication reliability in terms of minimizing the OP. The suggested RS strategy also takes the effect of jamming attacks and/or interferers into account. Accordingly, an intensive investigation of the OP of all RS schemes considering also jammers' positions in various scenarios is conducted. The results suggest that a combination of RS schemes using channel gains and SINRs of all hops achieves the best communication reliability in scenarios with intensive interference. The sensitivity for channel estimation errors of the relaying schemes is also investigated. Finally, discussions about the obtained results together with the complexity of all RS schemes are presented before providing guidelines on which schemes should be used in which scenarios to improve the communication reliability.**

***Index Terms*—strong interference, jamming attack, relaying strategy, adaptive relay selection**

I. Introduction

Relaying strategies have been proposed as promising techniques to improve communication reliability of wireless networks [1]. In such schemes, relayers located between a source node and a destination are selected to help the source's packet reaching the destination with a higher probability. As a result, relay selection (RS) plays a very important role in affecting the reliability performance of a relaying scheme. In the literature, there are a large number of RS schemes that have been proposed based on typical quality criteria such as channel gains between the source and relayers [2], channel gains between relayers and the destination [3], a combination of channel gains between the source and relayers and between relayers and the destination [4], signal-to-interference-plus-noise ratio (SINR) between the source and relayers [5], between relayers and the destination [6], and the combination of SINR between the source and relayers and relayers and the destination [7]. In addition to these criteria, various constraints are also added to further optimize the overall performance of the relaying schemes, e.g., power consumption, timeliness, etc [8], [9]. Consequently, all these schemes come with different complexity, require different types of channel state information (CSI), and provide different performance gains. However, existing interference from co-located clusters, other wireless networks, and even jamming attacks, which obviously exist in practice [10], [11] are not taken into account. Therefore, an investigation on all aforementioned RS criteria considering interference at different levels and jammer locations is needed together with an evaluation of the sensitivity to channel estimation errors. Moreover, the performance improvement achieved by selecting the best RS compared to others should be considered given the additional complexity that the scheme brings.

The research leading to these results has received funding from the Swedish Foundation for Strategic Research through the Serendipity Project.

Our first goal is to evaluate some important RS schemes using outage probability (OP). With the OP, we can determine how often the received SINR is below a certain threshold. Moreover, given that we have closed-form expressions of the OP, it can be obtained and recalculated fast for online decisions. This is very useful when we need to optimize both on individual nodes and all the packets in the whole wireless network [12]. We also suggest an RS scheme which is using the lowest OP to select the best relayer and taking any potential jammers and/or interferers into consideration. For the evaluation in terms of outage probability, different scenarios are considered which all are taking the jammers' positions in relation to the positions of the relayers and destination into account. This step gives us indications as to which RS schemes can provide the best reliability in which scenarios. Finally, we discuss the obtained performance of each scheme considering its complexity, to provide guidelines on selecting the best scheme for various scenarios.

The rest of the paper is organized as follows. Section II presents the related works, followed by the system model in Section III. Next, Section IV describes RS schemes available in the literature as well as our proposed RS scheme together with a way to evaluate each scheme using OP metric. Then, the semi-analytical setup used for evaluation is introduced in Section V. After that, the evaluation of all RS schemes is presented in Section VI. Section VII provides discussions on the proposed scheme and the complexity of each scheme. Finally, Section VIII concludes the paper.

II. Related Works

This section reviews various RS schemes from the literature all using different criteria to decide on the best relayer. In [2], the authors proposed an RS scheme based on channel gains between the source and relayers and then investigated outage and throughput performance. Next, an RS scheme that uses channel gains between relayers and the destination to decide on the best relayer before deriving closed-form expression of the OP is presented in [3]. The authors in [4] combined both channel gains between the source and relayers and between relayers and the destination as a full RS strategy to select the best relayer.

In [5], SINR between the source and relayers was considered as a criterion to select the best relayer, whereas an RS strategy based on SINR between relayers and the destination was considered in [6]. A combination of SINRs between the source and relayers and between relayers and the destination to decide on the best relayer is proposed in [7]. The previous RS schemes, e.g., [3]–[7], did not take the jamming attack and/or interference into account to decide which relayer is the best.

The authors in [13] proposed a different way to select the best relayer based on the minimum OP among all relayers to the destination in the second hop. The results indicate that the proposed RS scheme outperforms the comparable strategies. This means that the OP is a useful metric to select the best relayer as well as to evaluate RS schemes. A closed-form expression of the OP over Nakagami-m fading channels is provided, adopting the minimum OP among all relayers to the destination to choose the best relayer in [14]. However, these papers have not considered statistics from the first hop in the selection strategy and also have not taken interference into account. The authors in [15] proposed an RS scheme based on the criterion in [2], [4] to evaluate the OP and the average channel capacity performance but not considering the effect of interference to select the best relayer. In [16], an RS scheme is proposed for two clusters to reduce the effect of the selected relayer on another cluster. However, a thorough evaluation of different RS strategies, their complexity, and their sensitivity to incorrect CSI, interference from co-located clusters and jamming is still lacking.

Due to the open nature of wireless communication, wireless transmissions are more vulnerable to being attacked by, e.g. malicious jammers [17]–[19]. In particular, harmful jammers can generate noise signals over relevant wireless channels to disturb the ongoing transmissions. Consequently, different legitimate nodes can be affected by jamming signals at different levels. Therefore, taking potential jamming attacks into account when deciding on the best relayer for an RS scheme will make the relay section strategy more robust and more useful in practice. Moreover, as the number of connected devices continues to increase, the result is dense node deployment and spectrum reuse [10], [20]. Consequently, different wireless networks are more likely to interfere with each other. To deal with this, all RS schemes should take jamming attacks and/or interferers into account to improve the communication reliability of legitimate wireless communication systems.

III. System Model

We consider a system model including a source node S communicating with a destination D aided by N relayers R_i, $i = 1, 2, ..., N$, using decode-and-forward (DF) relaying, Fig. 1. Accordingly, a slot is divided into two phases as follows. The source node transmits the packet during the first phase, while all relayers and destination are active in receiver mode. The selected relayer will try to decode the transmitted packet and then encode it before forwarding it to the destination in the second phase. The selected relayer is chosen following different RSs as presented in section IV. We assume that all legitimate nodes including source, destination, and relayers are located inside the border and protected by fences or walls. We also consider the presence of interferers and/or jamming nodes who are only allowed to be placed outside of the border, Fig. 1. We assume that only one jammer is active at each phase. Therefore, the destination and all relayers must take a jamming attack from jammer 1 into account in the first phase, while only the destination must consider a jamming attack from jammer 2 in the second phase. We assume that all nodes operate in half-duplex and single antenna mode as it is common for simpler off-the-self devices. All channels $\widetilde{g}_x$ follow Nakagami-m fading, where $x = \{SR_i, R_iD, SD, J_1R_i, J_1D, J_2D\}$ are indexes of channel, distance, and SINR between S and R_i, R_i and D, S and D, J_1 and R_i, J_1 and D, and J_2 and D, respectively.

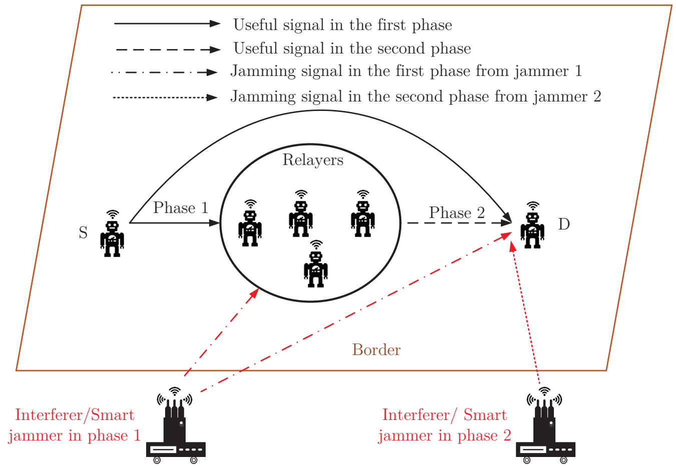

Fig. 1. System model.

In practice, perfect CSI is not available at the transceivers. In this paper, imperfect CSI is taken into consideration as $\widetilde{g}_y = (\widehat{g}_y + e_y)d_y^{-\frac{\zeta_y}{2}}$, where $y = \{SR_i, R_iD, SD\}$, d_y, ζ_y, $\widehat{g}_y$ and $e_y \sim CN(0, \sigma_y^2)$ are the distance, path-loss exponent, estimated channel coefficient and channel estimation error, respectively.

The received SINR at the destination D and R_i during the first phase can be expressed as

$$\gamma_S^D = \frac{h_{SD}}{h_{J_1.D} + \rho_{SD}\sigma_{SD}^2 + 1}, \quad (1)$$

$$\gamma_i^R = \frac{h_{SR_i}}{h_{J_1R_i} + \rho_{SR_i}\sigma_{SR_i}^2 + 1}, \quad (2)$$

where $h_{SD} = \rho_{SD}|\widehat{g}_{SD}|^2$, $\rho_{SD} = \frac{P_S}{d_{SD}^{\zeta_{SD}} N_D}$, $h_{J_1D} = \rho_{J_1D}|\widetilde{g}_{J_1D}|^2$, $\rho_{J_1D} = \frac{P_{J_1}}{d_{J_1D}^{\zeta_{J_1D}} N_D}$, $h_{SR_i} = \rho_{SR_i}|\widehat{g}_{SR_i}|^2$, $\rho_{SR_i} = \frac{P_S}{d_{SR_i}^{\zeta_{SR_i}} N_i}$, $h_{J_1R_i} = \rho_{J_1R_i}|\widetilde{g}_{J_1R_i}|^2$, $\rho_{J_1R_i} = \frac{P_{J_1}}{d_{J_1R_i}^{\zeta_{J_1R_i}} N_i}$. Here, N_D, N_i, P_S, and P_{J_1} are the noise power at the destination, relayer-i, transmit power of the source node S, and transmit power of the jammer J_1, respectively. Note that channel gains $|.|^2$ are characterized by a Gamma distribution with unit mean and shape m_x and hence $h_x \sim \left(m_x, \frac{\rho_x}{m_x}\right)$.

In the second phase, the received SINR at the destination D_i is represented as

$$\gamma_i^D = \frac{h_{R_iD}}{h_{J_2D} + \rho_{R_iD}\sigma_{R_iD}^2 + 1}, \quad (3)$$

where $h_{R_iD} = \rho_{R_iD}|\widehat{g}_{R_iD}|^2$, $\rho_{R_iD} = \frac{P_{R_i}}{d_{R_iD}^{\zeta_{R_iD}} N_D}$, $h_{J_2D} = \rho_{J_2D}|\widetilde{g}_{J_2D}|^2$, $\rho_{J_2D} = \frac{P_{J_2}}{d_{J_2D}^{\zeta_{J_2D}} N_D}$.

IV. Relay Selection and Outage Probability

In the literature, a wide range of RS strategies has been proposed to improve the system performance. In this work, we consider and evaluate several RS schemes and also include our proposed scheme in the following subsections.

A. Group A: Relay selection based on channel gains

RSs in this group select the best relayer based on instantaneous estimated channel gains from the first and/or second hops. The following schemes are considered in this work.

- RS1: The main idea of this RS is that the best relayer is selected based on the information about the channel gains between the source node and all relayers [2]. The maximum channel gain during the first hop decides on which relayer is chosen. In other words, $l_1 = \arg\max_i \{h_{SR_i}\}$ is the selected relayer index. This means that the instantaneous channel gains between the source node and relayers are adopted, leading to that the best relayer can be changed in different slots.
- RS2: Similar to the first RS scheme, however, the best relayer is decided based on the relationship among channel gains between relayers and destination [3]. Therefore, the index of the best relay is determined as $l_2 = \arg\max_i \{h_{R_iD}\}$.
- RS3: Both RSs 1 and 2 are partial schemes since the best relay is only selected based on either channel gains between the source node and relayers or channel gains between relayers and destinations. To improve the system performance, RS3 scheme uses channel gain information in both hops, from the source node to all relayers and from relayers to the destination. Accordingly, the index of the best relay is found as $l_3 = \arg\max_i \min \{h_{SR_i}, h_{R_iD}\}$ [4].

B. Group B: Relay selection based on SINR

In this group, instantaneous SINRs for the first and/or second hops taking jamming attacks into account are determined first based on instantaneous estimated channel gains, estimated transmit power of jammers, and estimated positions of jammers in (2) and (3). Then, the best relayer is decided based on the obtained instantaneous SINRs. We consider three schemes as follows:

- RS4: RS4 adopts SINR during the first phase between the source node and relayers to decide on the best relayer with index as $l_4 = \arg\max_i \{\gamma_i^R\}$ [5].
- RS5: Similar to the RS4, RS5 scheme uses SINR in the second hop between relayers and the destination for selecting the best relay as $l_5 = \arg\max_i \{\gamma_i^D\}$ [6].
- RS6: We can see that both RSs 4 and 5 are partial ones with knowledge of SINR only for one of the two hops. Therefore, to enhance the performance of the legitimate communication system, RS6 scheme combines the SINRs in both phases to decide on the best relayer. Accordingly, the index of the best relay is defined as $l_6 = \arg\max_i \min \{\gamma_i^R, \gamma_i^D\}$ [7].

C. Group C: Benchmarking RS schemes

In this group, the best relayer is chosen based on the lowest OP, as our proposed scheme RS7 does. The other two schemes are added for comparison.

- RS7: All aforementioned RSs consider instantaneous channel gains or SINRs to select the best relay for every slot. This can lead to higher latency and overhead problems. To this end, we propose an RS scheme where the best relayer is selected based on the lowest OP among all relayers. In other words, the index of the best relay is determined as $l_7 = \min_i \{p_i\}$. Here p_i is the OP for each relayer as defined in (4) below.
- RS8: To evaluate the gain of selecting a good relayer, we benchmark against the worst case, i.e. scheme where the relayer is selected based on the maximum OP among all relayers as $l_8 = \max_i \{p_i\}$.
- RS9: Finally, we benchmark with an RS scheme, in which the relay is selected randomly as $l_9 = rand[1..N]$.

D. Outage Probability

To evaluate the performance of all RSs above, the OP is used in this work [12]. Accordingly, the transmitted packet is decoded successfully at the receiver if the received SINR is above a threshold. This threshold can be found in practice, e.g. [21], [22]. For each relayer, an outage occurs when: (i) the transmitted packet cannot be decoded correctly at the destination by the direct link between the source node and destination in the first phase, and (ii) the source packet can not be delivered successfully to the destination via relay over both phases. In other words, the OP for each relay-i can be defined as follows:

$$p_i = \Pr\left\{\left(\gamma_S^D < \gamma_0\right) \cap \left[\left(\gamma_i^R < \gamma_0\right) \cup \left(\gamma_i^D < \gamma_0\right)\right]\right\}, \quad (4)$$

where γ_0 is the threshold to decode correctly the transmitted packet at the receivers including relayers and destination in both phases.

V. Semi-analytical Setup

For relay schemes RSs 1, 2, 3, 4, 5, 6, and 9 a relayer is first chosen, based on the different criteria presented above. Then, the performance in terms of the outage probability is obtained from (4) for the selected relayer, and this is done for each transmission round. The final OP is then the average OP for each transmission round. The RSs schemes 7 and 8 instead determine the OP for each relayer using (4), before selecting its relayer, and this relayer is then used for all transmission rounds. Hence, the OP remains the same.

Algorithm 1 Simulation procedure

1: **Step 1:** Setup positions of S, D, N relayers, border, and jammers 1 and 2
2: **Step 2:** Setup pathloss exponent among legitimate nodes, legitimate nodes, and jammers
3: **Step 3:** Setup Nakagami-m values among legitimate nodes, legitimate nodes, and jammers
4: **Step 4:** Setup transmit power of legitimate nodes and jammers and SINR threshold
5: **Step 5:** Simulation procedure
6: **function** main
7:   **for** l = 1:L **do**
8:     Generate channel gains h_{SR_i}, h_{R_iD}, h_{SD}, $h_{J_1R_i}$, h_{J_1D}, and h_{J_2D} following a Gamma distribution
9:     Calculate SINRs in (1), (2), and (3)
10:     Check the outage condition for each relayer in (4):
11:     **if** outage occurs **then**
12:       $P_i(l) = 1,\ i = 1, 2, ..., N$;
13:     **else**
14:       $P_i(l) = 0,\ i = 1, 2, ..., N$;
15:     **end if**
16:     Check outage condition for RS1:
17:     Find l_1 = max(h_{SR_i}); $P_1^{RS}(l) = p_{l_1}(l)$
18:     Check outage condition for RS2:
19:     Find l_2 = max(h_{R_iD}); $P_2^{RS}(l) = p_{l_2}(l)$
20:     Check outage condition for RS3:
21:     Find l_3 = max[min(h_{SR_i}, h_{R_iD})]; $P_3^{RS}(l) = p_{l_3}(l)$
22:     Check outage condition for RS4:
23:     Find l_4 = max(γ_i^R); $P_4^{RS}(l) = p_{l_4}(l)$
24:     Check outage condition for RS5:
25:     Find l_5 = max(γ_i^D); $P_5^{RS}(l) = p_{l_5}(l)$
26:     Check outage condition for RS6:
27:     Find l_6 = max[min(γ_i^R, γ_i^D)]; $P_6^{RS}(l) = p_{l_6}(l)$
28:     Check outage condition for RS9:
29:     $l_9 =$ Random $\{1, ..., N\}$; $P_9^{RS}(l) = p_{l_9}(l)$
30:   **end for**
31:   **Step 6:** Determine the OP for RSs 1-6 and 9:
32:   $p_j^{RS} = \frac{\text{Sum}(P_j^{RS})}{L}$, $j \in \{1, 2, 3, 4, 5, 6, 9\}$
33:   **Step 7:** Determine the OP for RSs 7 and 8:
34:   OP for each relayer: $p_i = \frac{\text{Sum}(P_i)}{L}$
35:   OP for RS7: $p_7^{RS} = \min(p_i)$
36:   OP for RS8: $p_8^{RS} = \max(p_i)$
37: **end function**

The main evaluation procedure is described in Algorithm 1. First, positions of all legitimate nodes and jammers are generated, in which all legitimate nodes are located inside the border, while jammers are only allowed to be appeared outside of the border, Fig. 2. Second, path-loss exponents and Nakagami-m parameters are configured, e.g. $\zeta_{SR_i} = \zeta_{R_iD} = \zeta_{SD}$, $\zeta_{J_1R_i} = \zeta_{J_1D} = \zeta_{J_2D}$, $m_{SR_i} = m_{R_iD} = m_{SD}$, $m_{J_1R_i} = m_{J_1D} = m_{J_2D}$. The SINR threshold $\gamma_0 = 1.6667$ dB is selected matching a packet length of 32 bits [22]. Then, transmit power of all legitimate nodes and jammers are set, e.g. $\alpha = \frac{P_S}{N_D} = \frac{P_S}{N_i} = \frac{P_{R_i}}{N_D}$ in dB and $\alpha_{J_1} = \frac{P_{J_1}}{N_i} = 40$ dB, $\alpha_{J_1D} = \frac{P_{J_1}}{N_D} = 40$ dB, and $\alpha_{J_2D} = \frac{P_{J_2}}{N_D} = 40$ dB during simulation. We first generate channel gains for both phases in line-8. The obtained channel gains are used to decide on the best relayer for RSs 1, 2, and 3 and to calculate the instantaneous SINRs in line-9 to decide on the best relayer for RSs 4, 5, and 6 as well as to check outage condition for each relayer in line-11. For RSs 1-6 and 9, the index of the best relayer is determined before attaining their OPs, respectively, line-16 to line-29. We run **Algorithm 1** using MATLAB. Particularly, we first generate $L = 10^5$ samples of the channel gains following a Gamma distribution and then check the outage conditions for each RS scheme in order to attain p_i for each relayer. For RS 9, the relayer is selected randomly following a uniform distribution. Finally, the overall OPs are then obtained by taking the average of all outage events across 10^5 samples. For RSs 7 and 8, the final OPs are determined as the minimum and maximum among p_i, respectively.

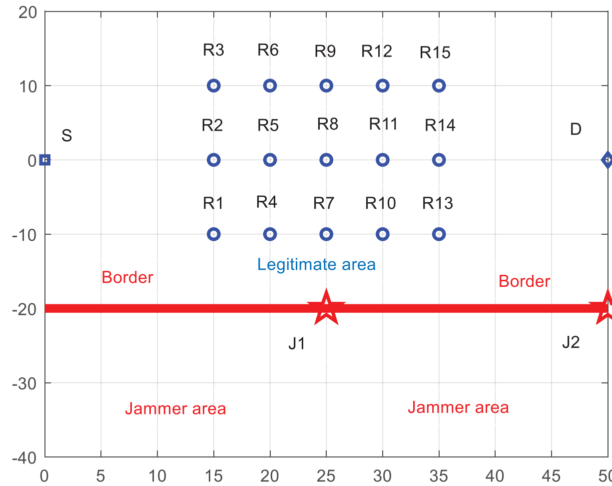

Fig. 2. All nodes' locations.

VI. Results

We consider the worst scenario that all jammers and/or interferers experience the same channel quality as the legitimate nodes, i.e., $\zeta_{SR_i} = \zeta_{R_iD} = \zeta_{SD} = 2$, $\zeta_{J_1R_i} = \zeta_{J_1D} = \zeta_{J_2D} = 2$, $m_{SR_i} = m_{R_iD} = m_{SD} = 3$, $m_{J_1R_i} = m_{J_1D} = m_{J_2D} = 3$. First, we investigate the reliability in terms of OP versus transmit power of the legitimate nodes and channel estimation error without any interferers and/or jammers in Figs. 3-5. As expected, the OP of all RS schemes decreases following an increase of transmit power of the legitimate nodes. However, the probability of outage for both RSs 3 and 6 reduces significantly compared to the others. This is because these two schemes take the information of instantaneous channel gains and instantaneous SINR of both phases into account, and thereby are able to select more appropriate relayers while

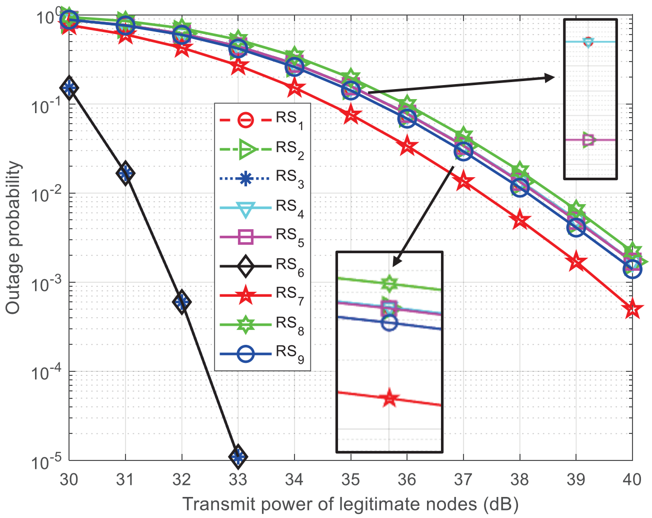

Fig. 3. The OP versus transmit power of legitimate nodes when $\sigma_y^2 = 10^{-4}$.

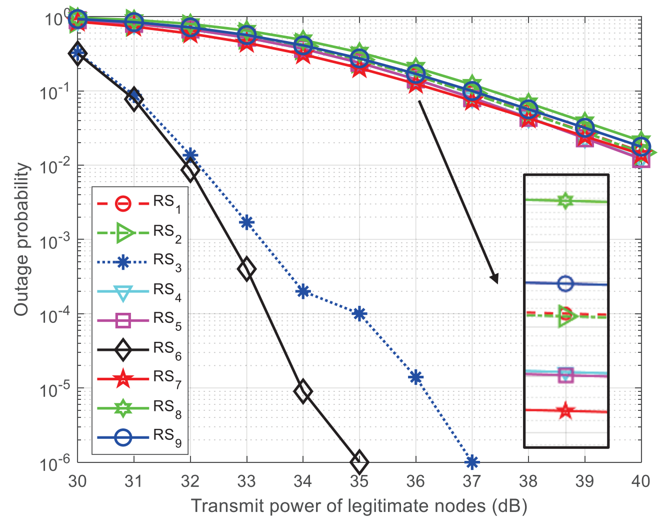

Fig. 4. The OP versus transmit power of legitimate nodes when $\sigma_y^2 = 0.1$.

TABLE I

FREQUENCY OF EACH RELAYER BEING SELECTED IN FIG. 3 (IN %).

	RS1	RS2	RS3	RS4	RS5	RS6	RS7	RS8
R1	**17.6704**	0.0129	3.0087	**17.6713**	0.0129	3.0092	0	**100**
R2	**43.6126**	0.0217	4.7752	**43.6008**	0.0218	4.7756	0	0
R3	**17.6516**	0.0142	3.0247	**17.6533**	0.0142	3.0251	0	0
R4	**4.1357**	0.1048	6.3657	**4.1383**	0.1050	6.3661	0	0
R5	**9.3073**	0.2089	10.7830	**9.3092**	0.2092	10.7826	0	0
R6	**4.1354**	0.1058	6.4057	**4.1370**	0.1060	6.4053	0	0
R7	0.7382	0.7455	8.2842	0.7387	0.7460	8.2836	0	0
R8	**1.5501**	**1.5589**	14.6235	**1.5513**	**1.5600**	14.6230	**100**	0
R9	0.7325	0.7373	8.2871	0.7330	0.7383	8.2866	0	0
R10	0.1087	**4.1138**	6.4028	0.1087	**4.1158**	6.4029	0	0
R11	0.2101	**9.3283**	10.8015	0.2107	**9.3309**	10.8009	0	0
R12	0.1004	**4.1105**	6.3152	0.1006	**4.1121**	6.3147	0	0
R13	0.0125	**17.6599**	3.0408	0.0125	**17.6623**	3.0418	0	0
R14	0.0229	**43.6076**	4.8301	0.0230	**43.5959**	4.8305	0	0
R15	0.0116	**17.6699**	3.0518	0.0116	**17.6696**	3.0521	0	0

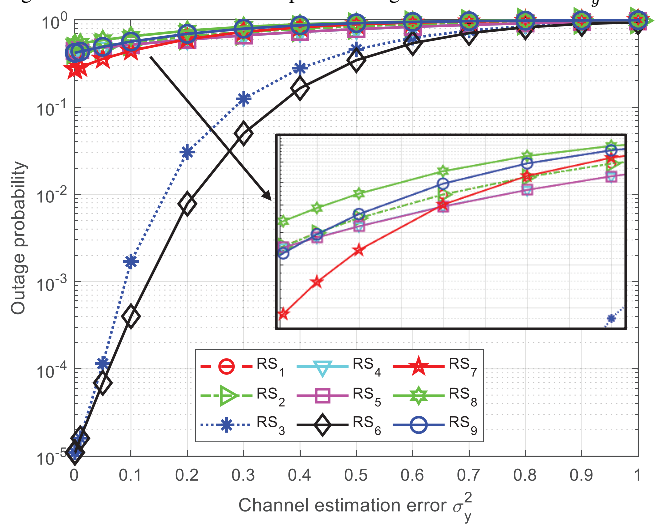

Fig. 5. The OP versus channel estimation error.

the other schemes consider only partial information either from the first hop or the second hop.

In Fig. 3, we can see that the OP of RS1, RS2, and RS3 experience the same behavior and performance differences as RS4, RS5 and RS6 when the channel estimation error is small enough, $\sigma_y^2 = 10^{-4}$. The reason is that the residual channel estimation error can be ignored when at this level, leading to the same relayer being selected, Table I. Looking at Table I, we can also see that the relayers located close to the source node are selected more often than others for both RSs 1 and 4, while RSs 2 and 5 select relayers close to the destination, as can be predicted intuitively. It can be seen that the relay selection made by RSs 3 and 6 is the same. Moreover, a relayer in the middle between the source and the destination is chosen with the highest probability as suggested by the result in [23]. For RS7, the best relayer is also in the middle between the source and destination. However, RS8 shows that the first relayer is the worst one. This also matches the obtained results in [24], which states that the relayer closer to the destination can help to improve the communication reliability more given that it manages to receive a correct packet.

In Fig. 4, when the channel estimation error is higher, $\sigma_y^2 = 0.1$, the gap of the OP between RS3 and RS6 grows dramatically with an increase of transmit power of the legitimate nodes. This is because the three RSs 1, 2, and 3 keep the same best relayers for both cases, Tables I and II. However, the residual noise in terms of channel estimation error increases, e.g. relayers closer to the source node may experience a higher residual noise due to channel estimation error. As seen in Table II, the three RSs 4, 5, and 6 adapt to the residual noise to improve reliability. In Fig. 5, we can see how the OP of all schemes changes following an increase of channel estimation error. When the channel estimation error is very high, all schemes eventually reach the same OP due to very strong residual interference.

In the presence of interferers and/or jammers, we first consider the worst case scenario in which both jammers are located at the border, $\{J_1\left(x_{J_1}, -20\right), J_2\left(50, -20\right)\}$, and then change x_{J_1} to see how position of the jammer 1 affects the OP in Figs. 6, 7 and 8. From the figures, we can see that RS6 always performs best and the gap between the OP of RS6 and the others is very high. We also can see that RS3 offers higher reliability compared to the remaining ones, even though it is not taking the jamming attack into account to decide on

TABLE II
FREQUENCY OF EACH RELAYER BEING SELECTED IN FIG. 4 (IN %).

	RS1	RS2	RS3	RS4	RS5	RS6	RS7	RS8
R1	**17.6704**	0.0129	3.0087	**14.7101**	0.6463	4.6810	0	**100**
R2	**43.6126**	0.0217	4.7752	**20.4839**	0.8736	6.3017	0	0
R3	**17.6516**	0.0142	3.0247	**14.7047**	0.6409	4.6673	0	0
R4	**4.1357**	0.1048	6.3657	**8.4013**	**1.7015**	6.5574	0	0
R5	**9.3073**	0.2089	10.7830	**11.5537**	**2.3439**	8.8818	0	0
R6	**4.1354**	0.1058	6.4057	**8.3939**	**1.7367**	6.5619	0	0
R7	0.7382	0.7455	8.2842	**4.1004**	**4.0607**	7.3209	0	0
R8	**1.5501**	**1.5589**	14.6235	**5.5893**	**5.6395**	10.0864	**100**	0
R9	0.7325	0.7373	8.2871	**4.0727**	**4.1047**	7.3250	0	0
R10	0.1087	**4.1138**	6.4028	**1.7293**	**8.3708**	6.5667	0	0
R11	0.2101	**9.3283**	10.8015	**2.3720**	**11.5375**	8.8755	0	0
R12	0.1004	**4.1105**	6.3152	**1.7451**	**8.3896**	6.4891	0	0
R13	0.0125	**17.6599**	3.0408	0.6383	**14.7216**	4.6494	0	0
R14	0.0229	**43.6076**	4.8301	0.8657	**20.5389**	6.3311	0	0
R15	0.0116	**17.6699**	3.0518	0.6396	**14.6938**	4.7048	0	0

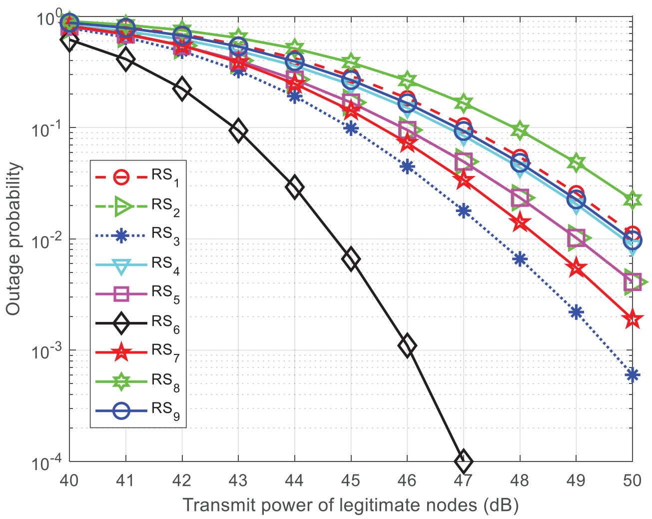

Fig. 6. The OP versus transmit power of legitimate nodes when $x_{J_1} = 15$.

the best relayer. Considering Tables III, IV, and V, we note that the three schemes RSs 1, 2, and 3 still keep the same best relayers as in previous scenarios. In contrast, both RSs 4 and 6 change their best relayers, while RS5 keeps the same relayers due to the second jammer position being fixed, and jammer 1 not affecting the SINR in the second hop. This is why the OP of RS4 is better than that of RS5. The best relayer of the RS7 is R15 for both $x_{J_1} = 15$ and 25, and then changes to R12 when $x_{J_1} = 35$ to reduce the effect of strong interference from jammer 1 while still selecting a relay close to the destination.

TABLE III
FREQUENCY OF EACH RELAYER BEING SELECTED IN FIG. 6 (IN %).

	RS1	RS2	RS3	RS4	RS5	RS6	RS7	RS8
R1	17.6872	0.0125	3.0061	0.3952	0.0125	0.1448	0	100
R2	43.6786	0.0238	4.7779	17.8958	0.0240	1.8033	0	0
R3	17.6682	0.0139	3.0359	33.6166	0.0142	1.6923	0	0
R4	4.1354	0.1101	6.4220	0.2176	0.1107	0.2824	0	0
R5	9.2773	0.2093	10.8211	6.3982	0.2103	3.3427	0	0
R6	4.0987	0.1079	6.3839	16.3453	0.1085	3.6084	0	0
R7	0.7257	0.7373	8.3016	0.2436	0.7406	0.8436	0	0
R8	1.5457	1.5454	14.5076	3.1943	1.5522	6.3176	0	0
R9	0.7284	0.7440	8.2910	8.7798	0.7461	7.3858	0	0
R10	0.1036	4.1190	6.3852	0.3389	4.1300	2.4883	0	0
R11	0.2013	9.2789	10.8534	2.0575	9.2883	11.7155	0	0
R12	0.1048	4.0976	6.3666	5.1904	4.1092	13.7214	0	0
R13	0.0103	17.6774	3.0052	0.4038	17.6826	5.7333	0	0
R14	0.0216	43.6060	4.7778	1.5468	43.5495	18.8986	0	0
R15	0.0132	17.7169	3.0647	3.3762	17.7213	22.0220	100	0

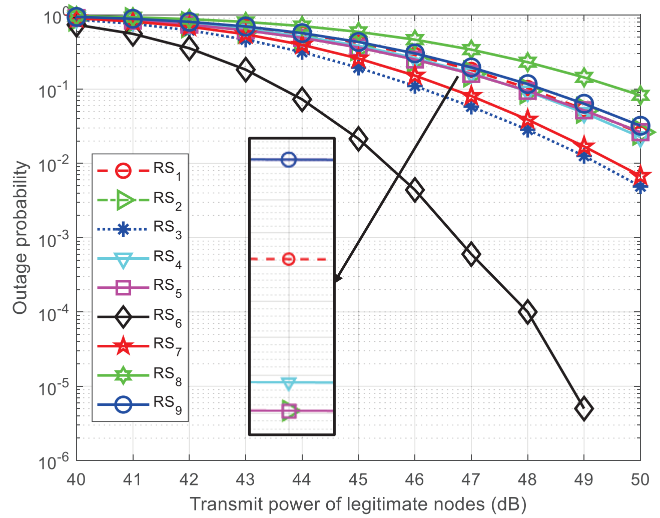

Fig. 7. The OP versus transmit power of legitimate nodes when $x_{J_1} = 25$.

TABLE IV
FREQUENCY OF EACH RELAYER BEING SELECTED IN FIG. 7 (IN %).

	RS1	RS2	RS3	RS4	RS5	RS6	RS7	RS8
R1	17.6872	0.0125	3.0061	1.9989	0.0125	0.8519	0	0
R2	43.6786	0.0238	4.7779	24.2297	0.0240	3.2593	0	0
R3	17.6682	0.0139	3.0359	36.8733	0.0142	2.7505	0	0
R4	4.1354	0.1101	6.4220	0.2093	0.1107	0.5454	0	0
R5	9.2773	0.2093	10.8211	6.0240	0.2103	5.3790	0	0
R6	4.0987	0.1079	6.3839	15.4393	0.1085	5.6704	0	0
R7	0.7257	0.7373	8.3016	0.0367	0.7406	0.3779	0	0
R8	1.5457	1.5454	14.5076	1.8680	1.5522	7.4875	0	0
R9	0.7284	0.7440	8.2910	6.7884	0.7461	10.3449	0	0
R10	0.1036	4.1190	6.3852	0.0256	4.1300	0.5905	0	100
R11	0.2013	9.2789	10.8534	0.8131	9.2883	9.9651	0	0
R12	0.1048	4.0976	6.3666	3.3154	4.1092	16.4063	0	0
R13	0.0103	17.6774	3.0052	0.0357	17.6826	1.4194	0	0
R14	0.0216	43.6060	4.7778	0.4893	43.5495	12.5325	0	0
R15	0.0132	17.7169	3.0647	1.8533	17.7213	22.4194	100	0

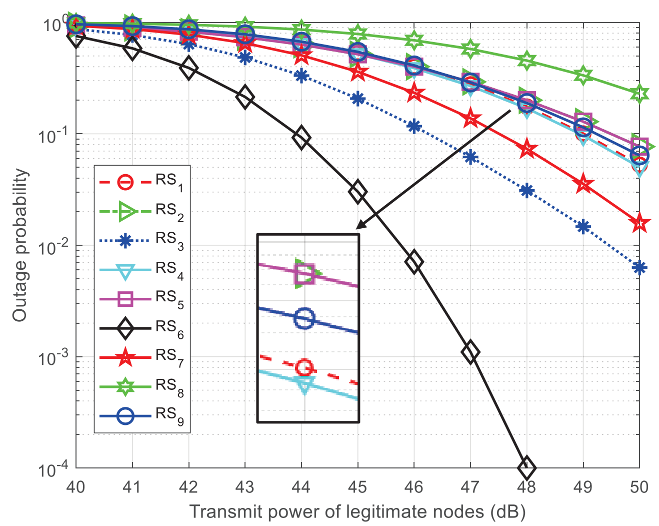

Fig. 8. The OP versus transmit power of legitimate nodes when $x_{J_1} = 35$.

TABLE V
FREQUENCY OF EACH RELAYER BEING SELECTED IN FIG. 8 (IN %).

	RS1	RS2	RS3	RS4	RS5	RS6	RS7	RS8
R1	17.6872	0.0125	3.0061	6.9986	0.0125	1.7217	0	0
R2	43.6786	0.0238	4.7779	30.7957	0.0240	3.3726	0	0
R3	17.6682	0.0139	3.0359	33.6467	0.0142	2.5528	0	0
R4	4.1354	0.1101	6.4220	1.0051	0.1107	2.1961	0	0
R5	9.2773	0.2093	10.8211	6.8441	0.2103	6.6883	0	0
R6	4.0987	0.1079	6.3839	12.1757	0.1085	5.7529	0	0
R7	0.7257	0.7373	8.3016	0.0966	0.7406	1.4774	0	0
R8	1.5457	1.5454	14.5076	1.4671	1.5522	9.5083	0	0
R9	0.7284	0.7440	8.2910	4.2901	0.7461	10.7697	0	0
R10	0.1036	4.1190	6.3852	0.0077	4.1300	0.6004	0	0
R11	0.2013	9.2789	10.8534	0.3590	9.2883	10.0529	0	0
R12	0.1048	4.0976	6.3666	1.5516	4.1092	16.3198	100	0
R13	0.0103	17.6774	3.0052	0.0015	17.6826	0.2856	0	100
R14	0.0216	43.6060	4.7778	0.1141	43.5495	8.7829	0	0
R15	0.0132	17.7169	3.0647	0.6464	17.7213	19.9186	0	0

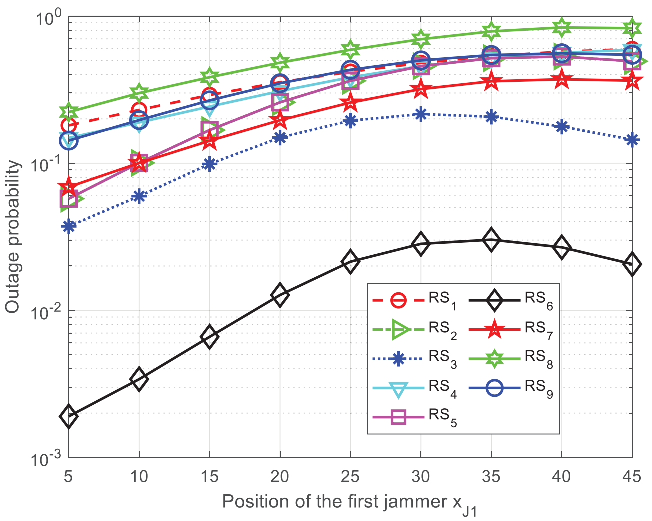

Fig. 9. The OP versus x_{J_1}, $y_{J_1} = -20$ and $J_2\,(50, -20)$, $\alpha = 45$dB.

In Figs. 9, 10 and 11, we fix the position of one jammer and change the position of the other one to investigate the OP of all schemes. Here, RS6 offers the best reliability. When both jammers are located at the border, the OP of RS3 is better than the others, with the exception of for RS6, Fig. 9. However, when jammer 2 is far away from the border and experiences as free interference in the second phase, the OP of the RS4 is much better than the others, only inferior than that of RS6, Fig. 10. Both RSs 2 and 5 can enhance the communication reliability much better than others, except for RS6 when jammer 1 almost disappears, Fig. 11. This is because the relayers close to the destination should be selected to deal with interference from jammer 2.

VII. DISCUSSIONS AND GUIDELINES

From the obtained results, we can see that various schemes can offer better performance in different scenarios. However, we need to consider each scheme's complexity to see if the gained performance is worth it compared to its complexity, Table VI and VII. RSs 1-6 need to recalculate the OP for every slot to select the best relayer, while RS7 only calculates the OP once to decide on the best relayer. From the tables, we can see that the complexity of RS6 is the highest, followed by RSs 3, 4, and 5, and then RSs 1, 2, and 7, 8 while RS9 has the lowest complexity. This is because RS9 just selects a random

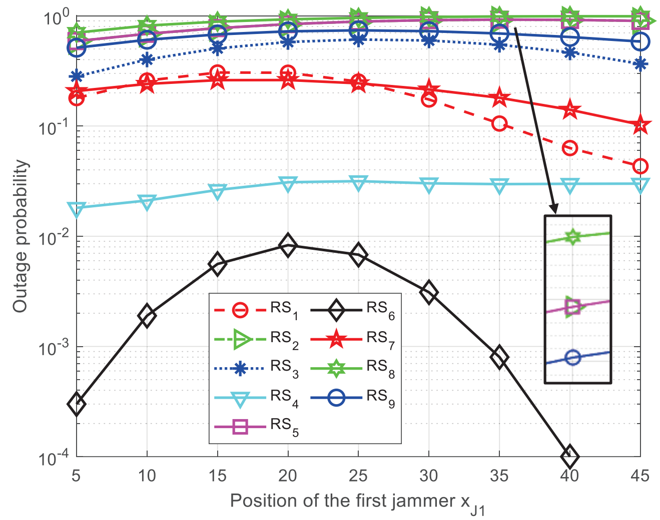

Fig. 10. The OP versus x_{J_1}, $y_{J_1} = -20$ and $J_2\,(50, -200)$, $\alpha = 40$dB.

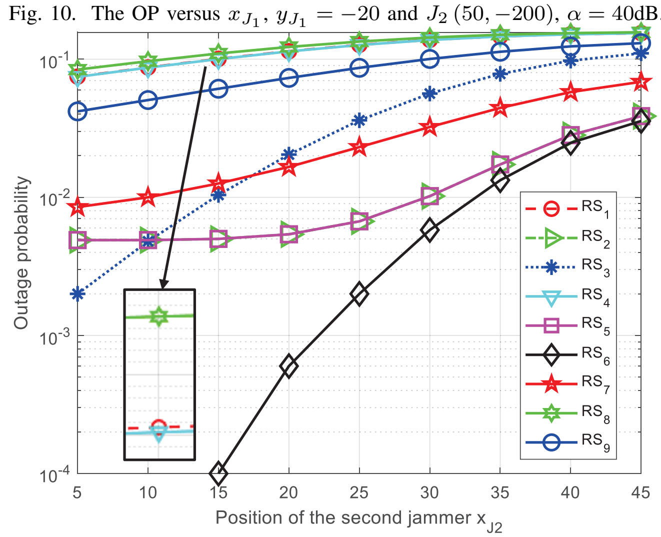

Fig. 11. The OP versus x_{J_2}, $y_{J_2} = -20$ and $J_1\,(25, -200)$, $\alpha = 40$dB.

relayer without any criteria. Note that RSs 1-6 need a center to collect all necessary information as presented in Table VII to select the best relayer for every slot before informing which relayer is chosen to act as the best one. This procedure can lead to higher latency and overhead problems when the number of relay nodes N is large. In contrast, RS7 needs several trials in order to obtain the long term statistics of the CSI needed to select the best relayer. This means when the channel conditions do not vary much, the best relayer does not vary much either. In this case, RS7 should be adopted to reduce the complexity.

Based on the complexity of each RS scheme above, we

TABLE VI
COMPLEXITY OF RSS 1-7.

	γ_i^R	γ_i^D	OP once	OP each slot	Min operator	Max operator
RS1				x		1
RS2				x		1
RS3				x	N	1
RS4	N			x		1
RS5		N		x		1
RS6	N	N		x	N	1
RS7			x		1	

TABLE VII
COMPARISON OF CRITERION TO SELECT THE BEST RELAYER OF ALL RSS.

Criterion	Group A	Group B	Group C
Statistic estimated channel gains			x
Instantaneous estimated channel gains	x	x	
Estimated transmit power of jammers	x	x	x
Estimated jammers' position	x	x	x
Instantaneous SINRs		x	

provide several guidelines for selecting RS as follows:

- When the system resources can satisfy all complex requirements for RS6, we should use RS6 to obtain the highest reliability as presented in section VI. However, RS3 also can offer a similar reliability level in systems with no interference and low channel estimation error, Fig. 3. Then, the legitimate system should have the capability to detect the presence of jammers and/or interferers, e.g. as in [25] and switch to RS6 when needed.
- When J_2 almost disappears, a lower complexity than provided by the RS6 scheme, such as RS4, can offer quite good reliability as presented in Fig. 10. Therefore, this scheme should be selected instead of RS6 if the system cannot satisfy the RS6 requirements.
- When J_1 is located far away from the border, RSs 2 and 5 can provide the same good reliability level, Fig. 11. Considering the system resources, RS2 can be adopted to reduce the complexity of the protocol.
- When the wireless channels do not vary much, RS7 is useful and offers lower complexity. Moreover, RS7 is also useful when the interference comes from static jammers and/or co-located clusters. When the legitimate system can detect the presence of interference and the root of interference, the legitimate system should be able to select a proper RS improving the communication reliability.

VIII. CONCLUSION

In this paper, we evaluate how interference from jamming attacks and/or interferers affect the communication reliability when using typical RS schemes. OP is selected as the reliability metric to evaluate the RS schemes. We consider several RS schemes from the literature and also random RS, minimum, and maximum OP as benchmarks. By conducting an extensive comparison of the attained OP of all RS schemes considering different jammers' positions for both relayers and destination in different phases, we have found three RS schemes that offer good reliability with relatively low complexity. Based on the obtained results, we discuss the achievable performance and complexity of each RS scheme to provide several guidelines for choosing the best scheme or combination of schemes in various scenarios with more or less stationary nodes and ability to estimate the channel state.

REFERENCES

[1] S. Diggavi, N. Al-Dhahir, A. Stamoulis, and A. Calderbank, "Great expectations: the value of spatial diversity in wireless networks," *Proc. IEEE*, vol. 92, no. 2, pp. 219–270, 2004.

[2] A. V. and B. A. V., "Performance analysis of NOMA-based underlay cognitive radio networks with partial relay selection," *IEEE TVT*, vol. 70, no. 5, pp. 4615–4630, 2021.

[3] J. S. Yeom, Y.-B. Kim, and B. C. Jung, "Spectrally efficient uplink cooperative NOMA with joint decoding for relay-assisted iot networks," *IEEE IoT-J*, vol. 10, no. 1, pp. 210–223, 2023.

[4] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, Y. Li, and J. Wang, "Security-reliability trade-off analysis of an-aided relay selection for full-duplex relay networks," *IEEE TVT*, vol. 70, no. 3, pp. 2362–2377, 2021.

[5] T. N. Nguyen, L.-T. Tu, D.-H. Tran, V.-D. Phan, M. Voznak, S. Chatzinotas, and Z. Ding, "Outage performance of satellite terrestrial full-duplex relaying networks with co-channel interference," *IEEE WCL*, vol. 11, no. 7, pp. 1478–1482, 2022.

[6] M. Dimitropoulou, C. Psomas, and I. Krikidis, "Generalized selection in wireless powered networks with non-linear energy harvesting," *IEEE TCOM*, vol. 69, no. 8, pp. 5634–5648, 2021.

[7] M. Xie, J. Gong, and X. Ma, "Age and energy tradeoff for short packet based two-hop decode-and-forward relaying networks," in *IEEE WCNC*, 2021, pp. 1–6.

[8] M. Xu, F. Liu, H. Xu, H. Zhu, and B. Wang, "On maximum of energy-efficiency in amplify-and-forward relay networks under channel estimation errors," *IEEE Access*, vol. 7, pp. 149 641–149 648, 2019.

[9] L.-N. Hoang, E. Uhlemann, and M. Jonsson, "Low complexity algorithm for efficient relay assignment in unicast/broadcast wireless networks," in *IEEE VTC Spring*, Sydney, NSW, Australia, 2017, pp. 1–6.

[10] S. Yan, X. Cao, Z. Liu, and X. Liu, "Interference management in 6G space and terrestrial integrated networks: Challenges and approaches," *Intell. and Converged Netw.*, vol. 1, no. 3, pp. 271–280, 2020.

[11] V.-L. Dao, L.-N. Hoang, S. Girs, and E. Uhlemann, "Defeating jamming using outage performance aware joint power allocation and access point placement in uplink pairwise NOMA," *IEEE OJ-COMS*, vol. 2, pp. 1957–1979, 2021.

[12] A. Goldsmith, *Wireless communications*. CUP, 2005.

[13] K. M. Eshteiwi, "Outage performance of relay selection in cooperative wireless networks over rayleigh fading channels," in *IEEE CCECE*, Regina, SK, Canada, 2013, pp. 1–5.

[14] S. Al-Zoubi, R. Mohaisen, M. F. Al-Mistarihi, S. M. Khatalin, and M. A. Khodeir, "On the outage probability in DF relay selection cooperative wireless networks over nakagami-m fading channels," in *ICICS*, Irbid, Jordan, 2016, pp. 186–189.

[15] T. T. Duy, T. Q. Duong, D. B. da Costa, V. N. Q. Bao, and M. Elkashlan, "Proactive relay selection with joint impact of hardware impairment and co-channel interference," *TCOM*, vol. 63, no. 5, pp. 1594–1606, 2015.

[16] J. Si, Z. Li, and Z. Liu, "Threshold based relay selection protocol for wireless relay networks with interference," in *IEEE ICC*, Cape Town, South Africa, 2010, pp. 1–5.

[17] F. Pan, Z. Pang, M. Luvisotto, M. Xiao, and H. Wen, "Physical-layer security for industrial wireless control systems: Basics and future directions," *IEEE IEM*, vol. 12, no. 4, pp. 18–27, 2018.

[18] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 767–809, 2022.

[19] P. Angueira, I. Val, J. Montalban, O. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surv. Tutor.*, vol. 24, no. 2, pp. 810–838, 2022.

[20] CISCO. (2020, March) Cisco annual internet report (2018–2023). [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[21] D. Jiang, Q. Chen, and L. Delgrossi, "Optimal data rate selection for vehicle safety communications," ser. VANET '08. New York, NY, USA: ACM, 2008, p. 30–38.

[22] J. García-Morales, M. C. Lucas-Estañ, and J. Gozalvez, "Latency-sensitive 5G RAN slicing for industry 4.0," *IEEE Access*, vol. 7, pp. 143 139–143 159, 2019.

[23] S. Girs, E. Uhlemann, and M. Björkman, "The effects of relay behavior and position in wireless industrial networks," in *IEEE WFCS*, Lemgo, Germany, 2012, pp. 183–190.

[24] L.-N. Hoang, E. Uhlemann, and M. Jonsson, "Relay grouping to guarantee timeliness and reliability in wireless networks," *IEEE COMML*, vol. 23, no. 9, pp. 1661–1664, 2019.

[25] V.-L. Dao and B. Leander, "Anomaly attack detection in wireless networks using DCNN," in *IEEE WFIoT*, Yokohama, Japan, October 2022.