Do Not Forget the Past: A Buffer-Aided Framework for Relay Based Key Generation

Rusni Kima Mangang and Harshan Jagadeesh

Abstract—We address relay-assisted key generation wherein two wireless nodes, that have no direct channel between them, seek the assistance of an intermediate relay to generate secret keys. In a celebrated version of the relay-assisted protocol, as applied by Lai *et al.*, Zhou *et al.*, Wang *et al.*, and Waqas *et al.*, the relay node generates pair-wise keys with the two nodes, and then broadcasts an XOR version of the two keys. Although such protocols are simple and effective, we observe that they face reduction in key rates due to two problems. First, for confidentiality, the relay broadcasts an XOR function of the pair-wise keys thereby pruning the length of the shared key to be the minimum of the key lengths of the pair-wise keys. Secondly, the broadcast phase may also experience outages thereby not being able to share the generated key in every round of the protocol. Identifying these issues, we propose a buffer-aided relaying protocol wherein buffer is used at the relay to store unused secret bits generated in the previous rounds of the protocol so as to provide confidentiality in the subsequent rounds of broadcast. On this buffer-aided protocol, we propose a power-allocation strategy between the phases of key generation and broadcast so as to maximize the throughput and key rate. Rigorous analyses show that buffer-aided relay when implemented along with the proposed power-allocation strategy offer remarkable advantages over existing baselines.

Index Terms—Buffers, key generation, power-allocation.

I. INTRODUCTION

IT is well known that eavesdropping over wireless channels can be mitigated through symmetric-key crypto-primitives [1], [2]. Although crypto-primitive based techniques are effective in providing confidentiality, they necessitate the participating nodes to synthesize shared secret-keys at regular intervals. In the context of standard cellular communication, say between a user equipment and a base-station, secret-keys are synthesized using pre-registered subscriber identity module (SIM) based information between the two entities. However, in the context of device-to-device communication, wherein no pre-registered SIM based information are available between the devices, additional dynamic key-generation techniques must be implemented. Among several such key-generation techniques, physical-layer key (PLK) generation methods have received traction in the wireless community. Specifically, in PLK generation, two wireless nodes exploit random fluctuations in their wireless channels to synthesize shared

secret-keys, and subsequently feed the generated keys to the higher-level crypto-blocks [3]–[8].

A. Motivation

In this work, we are interested in developing new strategies for PLK generation particularly addressing practical issues that forbid key generation. For instance, PLK generation is not feasible when the two devices are out-of-coverage due to signal-blockage issues or power-limitations. One possible direction to circumvent this problem is to take the assistance of a trust-worthy neighboring node [12]–[15] that acts as a relay by offering the much needed connectivity and a random channel for the two nodes. To formally explain the relay based PLK generation, consider a wireless communication setting between two nodes, denoted by Node-A and Node-B, as shown in Fig. 1, which would like to harvest shared secret-keys through PLK generation. When the direct channel between Node-A and Node-B is not available, the two nodes use a trusted relay, denoted by Node-R, that can offer wireless channels with significant randomness. With the help of the relay, there are broadly two options for key generation; firstly, the relay can share the common randomness with the legitimate nodes through amplify-and-forward strategy [14], [18]. Secondly, the relay can generate keys with the nodes and broadcast them confidentially [12], [13]. However, among the two options, the amplify-and-forward strategy is not preferred due to higher noise in the common source of randomness as well as loss of key rate due to leakage issues in the common randomness at an eavesdropper. With the help of the relay under the latter class, it is clear that Node-A and Node-R may harvest keys by exchanging pilot symbols during the so-called *key generation phase*. Subsequently, this generated key must be reliably shared with Node-B during a dedicated time called the *broadcast phase*. Note that Node-R must confidentially share the generated key with Node-B, and this implies that the broadcast phase also requires a pre-shared key between Node-R and Node-B. Overall, the relay based PLK generation is such that pair-wise keys must be generated between Node-A and Node-R, and Node-B and Node-R, in the key generation phase, and then, one of the keys is used to securely share the other key in the broadcast phase.

Among the existing relay based PLK generation methods, a state-of-the-art technique [12], [13], [15], [19] that has gathered attention due to its simple and effective implementation, works as follows: **Step 1:** Pair-wise secret-keys are generated between Node-A and Node-R, denoted by $k_{AR} \in \{0,1\}^{N_{AR}}$, and Node-B and Node-R, denoted by

$k_{BR} \in \{0, 1\}^{N_{BR}}$ during the key generation phase, where N_{AR} and N_{BR} denote the lengths of the keys. **Step 2:** In the broadcast phase, an XOR version of pair-wise keys is shared by Node-R so that Node-B can retrieve k_{AR} through self-interference cancellation since k_{BR} is known at Node-B. For this celebrated XOR based idea, we identify two problems:

Problem 1: Although Node-A and Node-R, and Node-B and Node-R generate k_{AR} and k_{BR} in the key generation phase, respectively, the length of the key that is shared with Node-B in the broadcast phase is $\min(N_{AR}, N_{BR})$, which in turn reduces the overall key-rate of the protocol. Note that this limitation arises because of the XOR operation that provides confidentiality from an external eavesdropper listening to the broadcast phase. Motivated by this problem, in this paper, we ask *"How do we circumvent this loss in key-rate due to the XOR operation?"* Given that key-generation protocols are typically executed in multiple rounds in order to update the secret-keys, we explore the possibility of using buffer-aided relay to answer the above question.

Problem 2: We note that the randomness offered by the wireless channel between Node-A (or Node-B) and Node-R depends on its line-of-sight (LOS) component. In other words, higher is the LOS component of the channel, lower is the key length, and vice-versa. On the other hand, since the generated key must be broadcast through the same channel characteristics, we note that higher the LOS component of the channel, higher the reliability. Thus, a lower LOS channel offers conflicting behavior during the key generation phase and the broadcast phase. Moreover, with a given total power budget, allocating majority fraction of power to the key generation phase results in high-rate pair-wise keys; however, this leads to outage events owing to insufficient power to deliver those keys during the broadcast phase. On the other hand, allocating minority fraction of power to probing signals results in low-rate pair-wise secret-keys; however, although this may reduce the fraction of outage events owing to significant power on the broadcast signal, the overall key-rate at Node-A and Node-B might not be maximized. With this observation, we ask *"For a given LOS characteristics of the channel, how should the three nodes distribute their power between the key generation and the broadcast phase so as to maximize number of secret bits that reach Node-B?"*

B. Contributions

(1) We propose buffer-aided relay for PLK generation, and then study its impact on the overall key rate of the protocol. With the buffer at the relay, we show that unused secret bits generated between Node-R and Node-B can be temporarily stored at the relay, and these bits could be used to provide confidentiality for the broadcast phase in the subsequent rounds of key generation. This way, the message length in the broadcast phase would be more than the minimum of the key lengths generated between Node-A and Node-R, and Node-B and Node-R, thereby improving the key rate (see Section II).
(2) When using buffer-aided relay we study power-allocation strategies between the key generation phase and the broadcast phase such that the number of secret bits generated between Node-A and Node-B is maximized as a function of the LOS parameter between Node-A (or Node-B) and Node-R, and the underlying signal-to-noise-ratio (SNR). We first take up the power-allocation problem when optimal key generation algorithms are employed at the three nodes (see Section III). Subsequently, we formulate optimization problems to (i) maximize the *throughput* of the protocol, and to (ii) maximize the *key rate* of the protocol subject to an upper bound on the error-rate, say some $\eta > 0$, of the broadcast phase. The *key rate* metric is useful when the higher-level crypto-primitives of Node-A and Node-B expect shared secret bits through Node-R on at least $1 - \eta$ fraction of the key generation rounds. The number η is however chosen such that the two nodes can manage to garner shared secret bits from some other key generation methods on the residual η fraction. In a different scenario, the *throughput* metric is useful when the crypto-primitives of Node-A and Node-B do not impose strict requirements to generate the shared secret bits as long as the total number of bits generated across several key generation rounds is maximized. We present an extensive analysis on the objective functions and the underlying constraints of the optimization problem to show that standard gradient-descent algorithms can be applied to obtain near-optimal solutions. Through simulation results, we show that the proposed solutions provide significant benefits over standard baselines.
(3) We also extend the power-allocation problem to practical scenarios wherein (i) practical key generation algorithms are employed at the three nodes, and (ii) the buffer size at the beginning of the protocol is empty (see Section IV). In this case, we observe that the key rates offered by the protocol is a correlated process since the buffer also accumulates shared secret bits with Node-B across successive rounds of the key generation protocol. As a result, we capture the update process of the buffer as a function of successive rounds, and then derive closed form expressions on key rate. Finally, owing to short block-length codes for the broadcast phase, we invoke non-asymptotic outage probability results from [30], to pose an optimization problem over the power-allocation variable. Through simulation results, we show that the optimal power-allocation parameter results in substantial benefits in both throughput and key rate over equal power allocation between the key generation phase and the broadcast phase. Finally, we show that the key generation protocol with buffer-aided relay outperforms the one without buffer [12], [13], [15], [19].
(4) Finally, we discuss the application of buffer-aided protocol on relay networks wherein the LOS components between the nodes and the relay are different. We show that the optimization problems discussed in the context of relay networks with equal LOS components continue to apply for the case of unequal LOS components (see Section V).

C. Related Work and Novelty

In Fig. 2, we have shown the novel contributions of our work in contrast to the existing contributions. The idea of using a trusted relay [11] for key generation is closely related to the contributions of [12], [13]. However, unlike [12] and
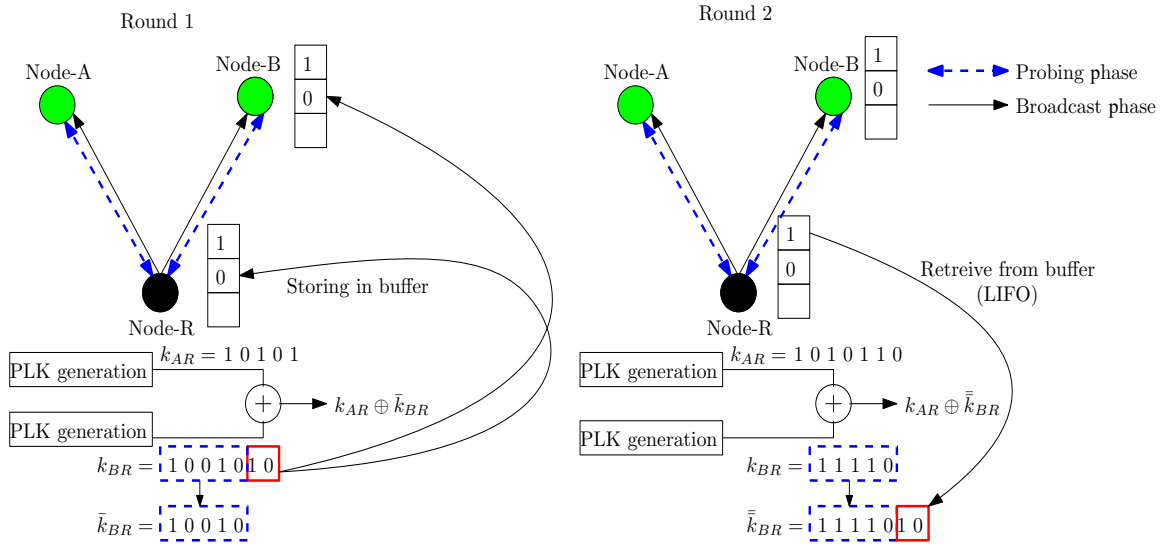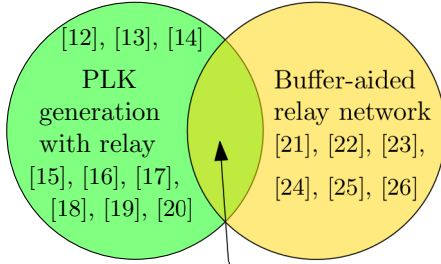
Fig. 1. Network model comprising Node-A and Node-B which intend to harvest secret-keys using their channel with Node-R. We use buffer-aided relay along with a power-allocation strategy between the key generation phase and broadcast phase to improve the throughput and key rates of the protocol. Observe that the unused secret bits of Round 1 are used in Round 2.

Fig. 2. Salient features of our work: (i) Multiple rounds of PLK generation, (ii) buffers, and (iii) power-allocation strategy.

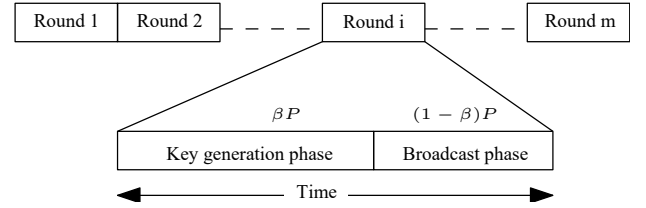| Contributions	Ours	[12]–[20]	[21]–[26]
PLK generation	✓	✓	
Relay	✓	✓	✓
Buffer	✓		✓
Multiple rounds	✓		
Non-asymptotic	✓		
Power allocation	✓		

Fig. 3. A single round of key sharing comprises two phases: The key generation phase and broadcast phase. The optimization parameter $\beta \in (0, 1)$ is used to allocate power between the two phases.

[13], our work is different in the following aspects: (i) The relay is trusted[1] and equipped with a buffer thereby aiding to increase the key rate for every round of key generation, (ii) variable power is considered between the key generation phase and the broadcast phase to deliver maximum number of secret bits within every round of key generation, (iii) the proposed power-allocation strategy is applicable when the two channels are characterized by arbitrary degree of LOS components. As far as the use of buffers is concerned, existing

relay based PLK generation methods have not considered buffers in their model. However, buffer-aided relays have been used to improve secrecy throughput [21], [22], minimize secrecy outage probability [23], [24] or investigate security and delay/QoS trade-off in the presence of eavesdropper [25], [26].

II. BUFFER-AIDED PROTOCOL WITH RELAY

Consider a network model, as shown in Fig. 1, wherein Node-A and Node-B take the assistance of Node-R to generate secret-keys using PLK generation framework. The complex base band channel between Node-A and Node-R is denoted by $h_{AR} = \sqrt{c_R}\left(\frac{1+i}{\sqrt{2}}\right) + \sqrt{1-c_R}g_{AR}$, such that the constant $\sqrt{c_R}\left(\frac{1+i}{\sqrt{2}}\right)$ captures the LOS component with $c_R \in [0, 1]$ and $\sqrt{1-c_R}g_{AR}$ captures the Non-LOS component with $g_{AR} \sim \mathcal{CN}(0, 1)$. As a special case, when $c_R = 0$ and $c_R = 1$, h_{AR} corresponds to a Rayleigh channel and an additive white Gaussian noise (AWGN) channel, respectively.[2] On the other hand, when $c_R \in (0, 1)$, h_{AR} corresponds to a Ricean channel

---

[1]Given that Node-A and Node-B are out of coverage, it is implicit that a relay node would also be needed to forward the payload to Node-B. Thus, the use of trusted relay is natural to the setting. However, as a future direction for research, it would still be interesting to study buffer-aided relaying protocol along with an untrusted relay [16], [17], [18], [20].

[2]In classical Ricean fading models [33], the parameter $K \in [0, \infty]$ is used to capture various degrees of LOS components. Alternatively, in this model, we use c_R for the same purpose, where K can be obtained as $K = \frac{c_R}{1-c_R}$.

with arbitrary degree of LOS as determined by c_R. Along the similar lines, the complex base band channel between Node-B and Node-R is denoted by $h_{BR} = \sqrt{c_R}\left(\frac{1+i}{\sqrt{2}}\right) + \sqrt{1-c_R}g_{BR}$, such that $\sqrt{1-c_R}g_{BR}$ captures the Non-LOS component with $g_{BR} \sim \mathcal{CN}(0,1)$. We assume that both h_{AR} and h_{BR} are quasi-static with a coherence interval of T time-slots, henceforth referred to as a coherence-block. Although identical LOS components are assumed for the two channels, note that their channel realizations are independent owing to their statistically independent Non-LOS components. Along the similar lines of [9], [10], [13], [19], we assume perfect reciprocity in the pair-wise channels.[3] In order to assist buffer-aided key generation, we assume that Node-B and Node-R are equipped with a buffer, using which multiple rounds of relay-assisted key generation protocols are executed, as shown in Fig. 3. To maintain consistency, the two nodes use the buffer as a stack with last-in first-out (LIFO) protocol. To capture successive rounds of key-generation protocols, we use $m \geq 0$ to denote the round number, and then explain the key-generation protocol for the mth round in the next section.

A. Protocol for Key Generation and Distribution

To explain the buffer-aided key generation protocol on the mth round, we assume that the buffers at Node-R and Node-B contain $B(m-1) \geq 0$ number of unused secret bits that were generated from the previous rounds. As shown in Fig. 3, each round of key generation protocol constitutes $L+1$ coherence-blocks, with $T \geq L$ for some $L \in \mathbb{Z}_+$, within which (i) L coherence-blocks are used by the three nodes for the key generation phase to generate pair-wise keys, and (ii) the $(L+1)$th coherence-block is used by Node-R to broadcast the generated key to Node-B. A total power budget of PL units is divided between the key generation phase and the broadcast phase as βPL and $(1-\beta)PL$, for some $0 < \beta < 1$. Subsequently, βPL is equally divided among the three nodes over L coherence-blocks for transmitting the probing symbols, and $(1-\beta)PL$ is used by Node-R to distribute the generated keys to Node-B during the $(L+1)$th coherence-block. This way, we use β as the underlying optimization parameter to distribute the power between the key generation phase and the broadcast phase. Note that this framework of power-allocation requires the total power at the relay to be higher than that of the other nodes since it has to execute both the probing phase and the broadcast phase. We do not consider power-allocation for the consensus-phase of key generation as it is proportional to the power needed for probing signals. By using $l \in \{1, 2, \cdots, L+1\}$ to denote the coherence-block index, the two channels in the network are represented as $h_{AR}(l)$ and $h_{BR}(l)$. To keep the notations simple, we do not use the round index m in the signal model, however, we use it when referring to the key lengths and the buffer size. First, we present a description of the key generation phase of the protocol within

a coherence-block index l, for $1 \leq l \leq L$, and then describe the broadcast phase in the $(L+1)$th coherence-block.

1) Key Generation Phase: In the key generation phase, Node-A, Node-B, and Node-R take turns to broadcast a symbol $x = \sqrt{\beta P/3}$ during the 1st, 2nd, and 3rd slots of the lth coherence-block.
Slot 1: Node-A transmits a probing signal $x = \sqrt{\beta P/3}$, which is used by Node-R to receive a noisy version of $h_{AR}(l)$. In particular, the corresponding received signal is

$$y_R^{(1)}(l) = \sqrt{\frac{\beta P}{3}}h_{AR}(l) + n_R^{(1)}(l), \qquad (1)$$

where $n_R^{(1)}(l)$ represents the AWGN, distributed as $\mathcal{CN}(0,\gamma)$. Here, the superscript denotes the slot number of the coherence-block.
Slot 2: Node-B transmits a probing signal $x = \sqrt{\beta P/3}$, which is used by Node-R to receive a noisy version of $h_{BR}(l)$. In particular, the corresponding received signal is

$$y_R^{(2)}(l) = \sqrt{\frac{\beta P}{3}}h_{BR}(l) + n_R^{(2)}(l), \qquad (2)$$

where $n_R^{(2)}(l)$ represents the AWGN, distributed as $\mathcal{CN}(0,\gamma)$.
Slot 3: Node-R transmits a probing signal $x = \sqrt{\beta P/3}$, which is used by Node-A and Node-B to receive a noisy version of $h_{AR}(l)$ and $h_{BR}(l)$, respectively. In particular, the corresponding received signals are

$$y_A^{(3)}(l) = \sqrt{\tfrac{\beta P}{3}}h_{AR}(l) + n_A^{(3)}(l) \;\&\; y_B^{(3)}(l) = \sqrt{\tfrac{\beta P}{3}}h_{BR}(l) + n_B^{(3)}(l), \tag{3}$$

where $n_A^{(3)}(l)$ and $n_B^{(3)}(l)$ represent the AWGN, distributed as $\mathcal{CN}(0,\gamma)$. Using the first L coherence-blocks of the mth round, Node-A and Node-R use their observations $\{y_R^{(1)}(l), 1 \leq l \leq L\}$ and $\{y_A^{(3)}(l), 1 \leq l \leq L\}$, respectively, to apply a pair-wise key generation algorithm to synthesize $N_{AR}(m)$ secret bits, denoted by $k_{AR}(m) \in \{0,1\}^{N_{AR}(m)}$. Similarly, Node-B and Node-R generate $N_{BR}(m)$ secret bits, denoted by $k_{BR}(m) \in \{0,1\}^{N_{BR}(m)}$, using their observations $\{y_R^{(2)}(l), 1 \leq l \leq L\}$ and $\{y_B^{(3)}(l), 1 \leq l \leq L\}$, respectively. The process of pair wise key generation involves an appropriate consensus algorithm to ensure that keys generated separately are identical. The specific consensus algorithm applied in our work would be discussed in Section III and Section IV.

2) Broadcast Phase: In the $(L+1)$th coherence-block, Node-R intends to confidentially share $k_{AR}(m)$ with Node-B, using their secret-key $k_{BR}(m)$. Since the lengths of $k_{AR}(m)$ and $k_{BR}(m)$ are potentially different, the protocol for generating the broadcast message must be carefully designed. If $N_{AR}(m) < N_{BR}(m)$, then all the bits of $k_{AR}(m)$ can be confidentially shared with Node-B by XORing it with the corresponding number of bits in $k_{BR}(m)$. On the other hand, if $N_{AR}(m) > N_{BR}(m)$, then only $N_{AR}(m) - N_{BR}(m)$ bits of k_{AR} can be shared due to lack of padding bits from $k_{BR}(m)$ to provide confidentiality. To circumvent this loss in key length, our buffer-aided protocol uses the pre-shared bits in the buffer $B(m-1)$ to generate a new sequence $k_{XOR}(m) \in \{0,1\}^{N_{XOR}(m)}$ defined as in (4),

---

[3]Pair-wise key generation protocol is still applicable for imperfect channel reciprocity [15], [32]. Although the key-rate reduces due to imperfect reciprocity, the difference in the key length of the two channels persists, and therefore, buffers are applicable.

where $B(0) = 0$, $\bar{k}_{BR}(m)$ constitutes the first $N_{AR}(m)$ components of $k_{BR}(m)$ and $\bar{k}_{AR}(m)$ constitutes the first $N_{BR}(m)$ components of $k_{AR}(m)$, and finally, $\bar{\bar{k}}_{BR}(m)$ constitutes the concatenation of $N_{BR}(m)$ and the additional $N_{AR}(m) - N_{BR}(m)$ bits from the buffer. With the use of the buffer it is clear that the length of the key is shortened only if sufficient number of padding bits is not available in the buffer (as captured in the third case of (4)). Concurrently, in order to enhance the key length for the subsequent rounds, the buffer gets updated as in (5), where $B(0) = 0$. Since $k_{AR}(m)$ and $k_{BR}(m)$ are uniformly distributed and statistically independent, the XOR operation in (4) provides confidentiality to the underlying secret-key $k_{AR}(m)$ from an external eavesdropper [12], [13]. As the last part of the broadcast phase, $k_{XOR}(m)$ is mapped to an L-length codeword $\mathbf{c} \in \mathcal{S} \subset \mathbb{C}^L$, and then sent to Node-B in the $(L + 1)$th coherence-block. Here, $\mathcal{S}$ denotes the chosen channel code of block-length L in order to provide reliability. Assuming $\frac{1}{L}\mathbb{E}[|\mathbf{c}|^2] = 1$, Node-B receives

$$\mathbf{y}_B = \sqrt{(1-\beta)P}h_{BR}(L+1)\mathbf{c} + \mathbf{n}_B \in \mathbb{C}^L, \quad (7)$$

where $\mathbf{n}_B$ represents the AWGN, distributed as $\mathcal{CN}(\mathbf{0}_L, \gamma\mathbf{I}_L)$. In addition to sending the codeword, Node-R also shares the length of $k_{XOR}(m)$ through a control channel. Then, Node-B decodes to $\hat{\mathbf{c}} \in \mathcal{S}$ using an appropriate decoder, and then recovers $\hat{k}_{XOR}(m)$. Using $N_{XOR}(m)$ (that is sent by Node-R) and $N_{BR}(m)$ (that is known during the pair-wise key generation process), the shared secret-key $\hat{k}_{AR}(m)$ is extracted as in (6), where $\bar{k}_{BR}(m)$ constitutes the first $N_{AR}(m)$ components of $k_{BR}(m)$, and $u_{BR}(m)$ are the $N_{XOR}(m) - N_{BR}(m)$ bits retrieved from the buffer $B(m-1)$ at Node-B. The XOR operation in (6) can be viewed as successive interference cancellation (SIC) as $k_{BR}(m)$ and $u_{BR}(m)$ are perfectly known at Node-B. We highlight that $u_{BR}(m)$ was known since Node-R maintains an identical buffer as that at Node-B. After the recovery process, the buffer at Node-B also gets updated to obtain $B(m)$ identically at Node-R. Thus, due to the proposed buffer-aided relay, $N_{XOR}(m)$ bits are communicated to Node-B during the $L+1$ coherence-blocks of one round. However, due to the channel conditions in the $(L + 1)$th coherence-block, $\hat{k}_{XOR}(m)$ is likely to be in error despite using the channel code $\mathcal{S}$. As a result, we need to study the fraction of times $\hat{k}_{XOR}(m)$ is correctly decoded at Node-B.

From the description of relay-assisted protocol, it is clear that the length of the secret-key that is correctly generated between Node-A and Node-B at the mth round depends on the power-allocation factor $\beta \in (0, 1)$, the LOS component $c_R \in [0, 1]$, the signal-to-noise ratio of the two channels, and the buffer-size $B(m - 1)$ at the end of the $(m - 1)$th key generation round. To characterize the best-case benefits of the buffer-aided protocol on the mth round, in the next section, we present the throughput and key rate analysis when optimal key generation algorithms are employed for pair-wise key generation between Node-A and Node-R, and Node-B and Node-R. Throughout the next section, we drop the reference to m, when referring to the keys and their lengths.

III. PERFORMANCE ANALYSIS WITH OPTIMAL KEY GENERATION ALGORITHMS

During the key generation phase of the protocol in Section II-A, Node-A and Node-R collect the set $\{y_A^{(3)}(l), 1 \le l \le L\}$ and $\{y_R^{(1)}(l), 1 \le l \le L\}$, wherein $y_A^{(3)}(l)$ is correlated with $y_R^{(1)}(l)$ for each l due to channel reciprocity. On this batch of samples, we assume that an optimal key generation algorithm [35] is applied to obtain k_{AR}, wherein optimality is measured in terms of maximizing the average key-rate, which is $I\left(y_A^{(3)}(l); y_R^{(1)}(l)\right)$ bits per coherence-block. Note that the consensus methodology used is as per Section IV of [35]. Similarly, Node-B and Node-R collect the set $\{y_B^{(3)}(l), 1 \le l \le L\}$ and $\{y_R^{(2)}(l), 1 \le l \le L\}$, and then apply an optimal key generation algorithm [35] to obtain k_{BR}, with average key rate $I\left(y_B^{(3)}(l); y_R^{(2)}(l)\right)$ per coherence-block. Since we have considered same LOS parameter c_R for both channels, i.e., channel between Node-A and Node-R, and channel between Node-B and Node-R, both the channels are identically distributed. With the same noise variances associated with the channels, the signals observed by all nodes are identically distributed. Since the optimal key rate is obtained by computing the mutual information of pair wise observations which provides identical results for identical distributions, key lengths generated between two pairs of nodes are identical, i.e., $N_{AR} = N_{BR}$.

After the XOR operation in (4), where the first condition is always satisfied, the sequence k_{XOR} has to be broadcast to Node-B in L channel-uses in the $(L + 1)$th coherence-block. Given that the entropy of the source is $I\left(y_A^{(3)}(l); y_R^{(1)}(l)\right)$ bits per coherence-block, and these bits are communicated over L channel-uses, we represent the rate of communication in bits per channel-use for the broadcast phase as

$$M \triangleq \frac{1}{L}\log_2\left(2^{N_{AR}}\right) = I\left(y_A^{(3)}(l); y_R^{(1)}(l)\right)$$
$$= \log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right), \quad (8)$$

where the last equality is computed using the joint distribution of $y_A^{(3)}(l)$ and $y_R^{(1)}(l)$ [12], [19]. In (8), we define $\rho \triangleq P/\gamma$. From the joint source-channel coding theorem [34], it is well known that a source with entropy $I\left(y_A^{(3)}(l); y_R^{(1)}(l)\right)$ bits per sample cannot be reliably communicated over a channel with mutual information less than its entropy. Applying these results in our case, information-theoretic outage event will occur when the instantaneous mutual information of the channel between Node-B and Node-R in the $(L+1)$th coherence-block is less than M. In other words, the probability that the channel $h_{BR}(L + 1)$ is in outage is given by

$$P_{\text{out}}^{(BR)} = \text{Prob}\left(M \ge \log_2\left(1 + |h_{BR}(L+1)|^2(1-\beta)\rho\right)\right),$$
$$= \text{Prob}\left(|h_{BR}(L+1)|^2 \le \left(\frac{1}{(1-\beta)\rho}\right)\frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right),$$
$$(9)$$

where $\log_2\left(1 + |h_{BR}(L+1)|^2(1-\beta)\rho\right)$ is the mutual information of the channel from Node-R to Node-B. Since

$$k_{XOR}(m) = \begin{cases} k_{AR}(m) \oplus k_{BR}(m), & \text{if } N_{AR}(m) = N_{BR}(m); \\ k_{AR}(m) \oplus \bar{k}_{BR}(m), & \text{if } N_{AR}(m) < N_{BR}(m); \\ \bar{k}_{AR}(m) \oplus k_{BR}(m), & \text{if } N_{AR}(m) - N_{BR}(m) > B(m-1); \\ k_{AR}(m) \oplus \bar{\bar{k}}_{BR}(m), & \text{if } N_{AR}(m) - N_{BR}(m) \le B(m-1); \end{cases} \tag{4}$$

$$B(m) = \begin{cases} B(m-1), & \text{if } N_{AR}(m) = N_{BR}(m); \\ B(m-1) + N_{BR}(m) - N_{AR}(m), & \text{if } N_{AR}(m) < N_{BR}(m); \\ B(m-1), & \text{if } N_{AR}(m) - N_{BR}(m) > B(m-1); \\ B(m-1) - (N_{AR}(m) - N_{BR}(m)), & \text{if } N_{AR}(m) - N_{BR}(m) \le B(m-1). \end{cases} \tag{5}$$

$$\hat{k}_{AR}(m) = \begin{cases} \hat{k}_{XOR}(m) \oplus k_{BR}(m), & \text{if } N_{XOR}(m) = N_{BR}(m); \\ \hat{k}_{XOR}(m) \oplus \bar{k}_{BR}(m), & \text{if } N_{XOR}(m) < N_{BR}(m); \\ \hat{k}_{XOR}(m) \oplus [k_{BR}(m) \ u_{BR}(m)], & \text{otherwise.} \end{cases} \tag{6}$$

$|h_{BR}(L+1)|$ is Rician distributed, the corresponding outage-probability $P_{\text{out}}^{(BR)}$ given in (9) can be computed in closed form. Specifically, using the cumulative distribution function (CDF) of a non-central chi-square random variable, we can write $\text{Prob}(|h_{BR}(L+1)|^2 \le h)$, for $h \ge 0$, as

$$\text{Prob}\left(|h_{BR}(L+1)|^2 \le h\right) = 1 - Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right), \tag{10}$$

where $Q_1(\cdot, \cdot)$ is a first-order Marcum-Q function expressed as

$$Q_1(\alpha, \lambda) = e^{-\frac{(\alpha^2+\lambda^2)}{2}} \sum_{n=0}^{\infty} \left(\frac{\alpha}{\lambda}\right)^n I_n(\alpha\lambda), \tag{11}$$

such that $I_n(\cdot)$ is the nth order modified Bessel function. In the next section, we formally define a throughput metric, which captures the fraction of secret bits that are correctly recovered at Node-B.

A. Throughput Analysis

Over the $L+1$ coherence-blocks, Node-B recovers LM secret bits through the relay channel whenever the channel from Node-R to Node-B is not in outage. On the other hand, Node-B recovers zero bits when the channel from Node-R to Node-B is in outage. Therefore, the average number of secret bits generated through the relay channel over $L+1$ coherence-blocks is $ML\left(1 - P_{\text{out}}^{(BR)}\right)$.

Definition 1: To capture the fraction of secret bits that reach Node-B from Node-R, we formally define the throughput of the scheme as

$$\Theta \triangleq M\left(1 - P_{\text{out}}^{(BR)}\right), \tag{12}$$

where M is given in (8) and $P_{\text{out}}^{(BR)}$ is given in (9). Note that we have discarded L in the throughput expression since the latency-interval is fixed.

In the above definition, we have assumed that k_{XOR} can be accurately recovered at Node-B when $h_{BR}(L+1)$ is not in outage, assuming that the channel code $\mathcal{S}$ is appropriately designed. By using (10) in (12), we get

$$\Theta = M \times Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right), \tag{13}$$

where

$$h = \left(\frac{1}{(1-\beta)\rho}\right) \frac{(\frac{1-c_R}{2})^2 \beta^2 \rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}. \tag{14}$$

Note that Θ is a function of β, c_R and ρ. For a given $\rho > 0$ and a given $c_R \in [0, 1]$, our goal is to solve [4]

$$\beta_{opt} = \max_{\beta \in (0,1)} \Theta. \tag{15}$$

It is easy to verify that $\Theta \ge 0$ over the domain $\beta \in [0, 1]$ with equality when $\beta = 0$ and $\beta = 1$. This is because M and $Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right)$ evaluate to zero when $\beta = 0$ and $\beta = 1$, respectively. Before solving (15), we need to understand the behavior of Θ as a function of β. We immediately note that M is non-concave in β and $Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right)$ is the sum of infinite Bessel functions. Although the Marcum-Q function has been shown to exhibit monotonous and log-concave properties [28], the function $Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right)$ is not log-concave in β since the parameter h in the second variable of the Marcum-Q function is a non-linear function of β, as shown in (14). Furthermore, we also note that the Marcum-Q function is typically expressed as an infinite sum of the modified Bessel functions of the first kind. Thus, owing to the non-concave structure of M and $Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right)$, we are unable to characterize the structure of their product as a function of β. As a result, the throughput expression is mathematically intractable to derive results on the optimal power-allocation factor.

To circumvent this issue, we present a lower bound on Θ, and then analyze its behavior with respect to β. Subsequently, we will show that searching for β that maximizes this lower bound on Θ will provide throughput values close to that when maximizing the exact throughput expression.

---

[4] We consider β only for key generation and broadcast phases; consensus power is not considered in the optimization problem because as in lemma 4.3 of [35] power required to achieve consensus is function of β or directly proportional to power allocated for key generation phase.

B. Lower Bound on Throughput

In this section, we present a lower bound on Θ, and then prove that the lower bound is unimodal over $\beta \in (0, 1)$ under some constraints on c_R and ρ.

Theorem 1: The throughput expression given in (13) is lower bounded by (16) shown at the top of next page.

Proof: In (11), the infinite series of $I_n(\alpha\lambda)$ can be lower bounded by considering the first dominant term as $Q_1(\alpha, \lambda) > e^{-\frac{\alpha^2+\lambda^2}{2}} I_0(\alpha\lambda) > e^{-\frac{\alpha^2+\lambda^2}{2}}$, where the last inequality is applicable because of the bound $I_0(\alpha\lambda) > 1$ given in [27]. Using the above lower bound on the Marcum-Q function in (13), and by substituting $\alpha = \sqrt{c_R/(\frac{1-c_R}{2})}$ and $\lambda = \sqrt{\frac{2^M-1}{(\frac{1-c_R}{2})(1-\beta)\rho}}$, the throughput expression is lower bounded as

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{(\frac{1-c_R}{2})\beta^2\rho}{2(9+6(\frac{1-c_R}{2})\beta\rho)(1-\beta)}}.$$

Since $9 + 6(\frac{1-c_R}{2})\beta\rho$ is lower bounded by $6(\frac{1-c_R}{2})\beta\rho$, we further bound the third term in the above product to get

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}}. \quad (17)$$

With this lower bound, we now split the domain $\beta \in (0, 1)$ into two parts, namely: (i) $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$ and (ii) $9/(6(\frac{1-c_R}{2})\rho) < \beta < 1$, provided the constants ρ and $(1-c_R)$ are such that $9/(6(\frac{1-c_R}{2})\rho) < 1$. In the latter case, when $9/(6(\frac{1-c_R}{2})\rho) < \beta$, we have

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right) > \log_2\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right).$$

By substituting the above bound in (17), we get

$$\Theta > \log_2\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}},$$

when $9/(6(\frac{1-c_R}{2})\rho) < \beta < 1$. Similarly, when $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$, we have the inequality

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right) \ge \log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right).$$

By substituting the above bound in (17), we get

$$\Theta \ge \log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}},$$

when $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$. Combining the above two cases, we obtain the lower bound on the throughput given in (16). This completes the proof. ∎

In the rest of this section, we present three lemmas to show that the proposed lower bound in (16) is unimodal in β. This result ensures that we can apply a gradient descent algorithm of suitable step-size to find β that maximizes (16), i.e., to solve the problem:

$$\beta^* = \arg \max_{\beta \in (0,1)} \Theta_{LB}. \quad (18)$$

Our approach to prove the unimodal property is to partition the interval $(0, 1)$ into three regions, namely: $\mathcal{R}_1 = (0, \beta_{\min}], \mathcal{R}_2 = (\beta_{\min}, 23/24)$, and $\mathcal{R}_3 = [23/24, 1)$, where $\beta_{\min} = 9/(6(\frac{1-c_R}{2})\rho)$ provided c_R and ρ satisfy an appropriate constraint. Subsequently, we prove that Θ_{LB} is (i). an increasing function in $\mathcal{R}_1$ (given in Lemma 1), (ii). concave in $\mathcal{R}_2$ (given in Lemma 2), and (iii). a decreasing function in $\mathcal{R}_3$ (given in Lemma 3).

Lemma 1: Θ_{LB} is an increasing function of β in the interval $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$ provided $(1-c_R)$ and ρ are such that $(\frac{1-c_R}{2})\rho > 1.862$.

Proof: When $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$, Θ_{LB} is of the form (from (16))

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}}.$$

Since the second term in the above product does not contain β, we need to show that

$$\frac{d}{d\beta}\left(\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right) e^{-\frac{\beta}{12(1-\beta)}}\right) > 0,$$

when $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$. After differentiating the above and rearranging terms, we must prove the following equivalent inequality

$$\frac{(\frac{1-c_R}{2})^2\beta\rho^2}{9} 12(1-\beta)^2 > \log\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right) \quad (19)$$
$$\times \left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right).$$

Applying the inequality $\log(1 + x) \le x$ on the first term of the right hand side (RHS) of (19), it suffices to show that

$$\frac{(\frac{1-c_R}{2})^2\beta\rho^2}{9} 12(1-\beta)^2 > \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18} \times \left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right).$$

By again rearranging the above, we need to show

$$24(1+\beta^2) - \frac{(\frac{1-c_R}{2})^2\rho^2\beta^3}{18} - 49\beta > 0, \quad (20)$$

in the interval $0 < \beta \le 9/(6(\frac{1-c_R}{2})\rho)$. We substitute $\beta = 9/(6(\frac{1-c_R}{2})\rho)$ in the left hand side (LHS) of (20), and then find the range of values of $(\frac{1-c_R}{2})\rho$ such that the inequality in (20) is satisfied. This implies we need to find the range of values of $(\frac{1-c_R}{2})\rho$ such that

$$384\left(\left(\frac{1-c_R}{2}\right)\rho\right)^2 - 1179\left(\left(\frac{1-c_R}{2}\right)\rho\right) + 864 > 0. \quad (21)$$

The roots of the above quadratic equation are $(\frac{1-c_R}{2})\rho = 1.21$ and $(\frac{1-c_R}{2})\rho = 1.862$. It is easy to note that the inequality in (21) is satisfied when $0 \le (\frac{1-c_R}{2})\rho < 1.21$ and $(\frac{1-c_R}{2})\rho > 1.862$. Out of the two regions, note that $(\frac{1-c_R}{2})\rho < 1.21$ leads to $\beta > 1$, and therefore this range is not applicable. On the other hand, the range $(\frac{1-c_R}{2})\rho > 1.862$ implies $\beta < 0.805$, and therefore this region is applicable. Thus, if $(\frac{1-c_R}{2})\rho > 1.862$, the extreme ends of the interval

$$\Theta_{LB} = \begin{cases} \log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{18}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}}, & \text{if } 0 < \beta \leq \frac{9}{6(\frac{1-c_R}{2})\rho}; \\ \log_2\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right) e^{-\frac{c_R}{2(\frac{1-c_R}{2})}} e^{-\frac{\beta}{12(1-\beta)}}, & \text{if } \frac{9}{6(\frac{1-c_R}{2})\rho} < \beta < 1. \end{cases} \tag{16}$$

$\beta \in (0, 9/(6(\frac{1-c_R}{2}))\rho)$ satisfy (20). Finally, since the LHS of (20) is a deceasing function of β, the inequality in (20) is satisfied when β takes interior points of the interval $(0, 9/(6(\frac{1-c_R}{2})\rho))$. Thus, Θ_{LB} is an increasing function of β in the interval $0 < \beta \leq \beta_{\min}$, where $\beta_{\min} = 9/(6(\frac{1-c_R}{2})\rho)$ provided $(\frac{1-c_R}{2})\rho > 1.862$. ∎

Lemma 2: Θ_{LB} is a concave function when $\frac{9}{6(1-c_R)\rho} < \beta < 23/24$ provided c_R and ρ are such that $9/(6(1-c_R)\rho) < 23/24$.

Proof: From (16), we have $\Theta_{LB} = \log_2\left(1 + (\frac{1-c_R}{2})\beta\rho/12\right) e^{-c_R/(2(\frac{1-c_R}{2}))} e^{-\frac{\beta}{12(1-\beta)}}$. Since the second term does not contain β, we represent $\log_2\left(1 + (\frac{1-c_R}{2})\beta\rho/12\right)$ and $e^{-\frac{\beta}{12(1-\beta)}}$ as $f(\beta)$ and $t(\beta)$, respectively. Subsequently, we prove that the second derivative of $f(\beta)t(\beta)$ is negative, i.e.,

$$\frac{d^2 f(\beta)}{d\beta^2}t(\beta) + 2\frac{df(\beta)}{d\beta}\frac{dt(\beta)}{d\beta} + f(\beta)\frac{d^2 t(\beta)}{d\beta^2} < 0. \tag{22}$$

Taking the first and the second derivatives of $t(\beta)$ and $f(\beta)$, we get

$$\frac{dt\beta}{d\beta} = \frac{-t(\beta)}{12(1-\beta)^2}, \frac{dt^2(\beta)}{\beta^2} = t(\beta)\frac{24\beta - 23}{12^2(1-\beta)^4},$$

$$\frac{df(\beta)}{d\beta} = (\log_2 e)\frac{1}{1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}}\frac{(\frac{1-c_R}{2})\rho}{12},$$

$$\frac{df^2(\beta)}{d\beta^2} = -(\log_2 e)\left(\frac{\frac{(\frac{1-c_R}{2})\rho}{12}}{1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}}\right)^2.$$

Since $\frac{df^2(\beta)}{d\beta^2}$ and $t(\beta)$ are always negative and positive, respectively, in the region of interest, the first term in (22) is always negative and so is the second term. Since $\frac{d^2 t(\beta)}{d\beta^2} < 0$ for $\beta < 23/24$, and $f(\beta)$ is non-negative, it is straightforward to observe that (22) is negative in the region $\beta < 23/24$. Furthermore, since the lower bound is applicable when $\beta > 9/(6(\frac{1-c_R}{2})\rho)$, we deduce that Θ_{LB} is a concave function in the interval $9/(6(\frac{1-c_R}{2})\rho) < \beta < 23/24$. This completes the proof. ∎

Lemma 3: When c_R and ρ are such that $9/(6(\frac{1-c_R}{2})\rho) < 23/24$, the lower bound on throughput given in (16) is a decreasing function of β in the interval $23/24 \leq \beta < 1$.

Proof: The expression for Θ_{LB} is a product of three terms, where the second term is not a function of β. As a result, it suffices to prove that

$$\frac{d}{d\beta}\left(\log_2\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right) e^{-\frac{\beta}{12(1-\beta)}}\right) < 0,$$

in the interval $23/24 < \beta < 1$. After differentiating the above with respect to β, we have to prove that

$$\log_2\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right)\frac{-e^{-\frac{\beta}{12(1-\beta)}}}{12(1-\beta)^2}$$

$$+(\log_2 e)\left(\frac{\frac{(\frac{1-c_R}{2})\rho}{12}}{1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}}\right) e^{-\frac{\beta}{12(1-\beta)}} < 0.$$

After rearranging the above terms, it suffices to prove that

$$\left(\frac{1-c_R}{2}\right)\rho(1-\beta)^2 < \left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right)\log\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right).$$

Applying the bound $\log(x) \geq 1 - 1/x$ on the RHS of the above equation, we get

$$\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right)\log\left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right)$$

$$\geq \left(1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}\right)\left(\frac{\frac{(\frac{1-c_R}{2})\beta\rho}{12}}{1 + \frac{(\frac{1-c_R}{2})\beta\rho}{12}}\right).$$

As a result proving the below inequality suffices.

$$\left(\frac{1-c_R}{2}\right)\rho(1-\beta)^2 < \frac{(\frac{1-c_R}{2})\beta\rho}{12},$$
$$12(1-\beta)^2 < \beta.$$

This further implies that we need to prove $12 - 25\beta + 12\beta^2 < 0$. It can be verified that the roots of the quadratic equation $12 - 25\beta + 12\beta^2 = 0$ are $3/4$ and $4/3$. Therefore, $12 - 25\beta + 12\beta^2 > 0$ for $\beta < 3/4$ and $\beta > 4/3$, and also $12 - 25\beta + 12\beta^2 < 0$ for $3/4 < \beta < 4/3$. The interval $23/24 \leq \beta \leq 1$ falls inside the interval $3/4 < \beta < 4/3$, and hence, the lower bound on throughput Θ_{LB} is a decreasing function of β in the interval $23/24 \leq \beta < 1$. ∎

Theorem 2: Θ_{LB} given in (16) is unimodal provided c_R and ρ are such that $(\frac{1-c_R}{2})\rho > 1.862$.

Proof: The proof follows from the conjunction of results in Lemma 1, Lemma 2, and Lemma 3. ∎

C. Simulation Results on Throughput Optimization

In this section, we present simulation results on throughput optimization when the channel offered by Node-R experiences LOS values of $c_R \in \{0, 0.1, \cdots, 0.9\}$, and when the underlying SNR values are $\rho \in \{5, 10, 15, 20, 25, 30\}$ in dB. For each combination of c_R and ρ, the power-allocation parameter β is obtained using the following methods: (i) Maximizing Θ in (13) using a brute-force search over $\beta \in (0, 1)$ in steps of 0.001, (ii) applying a gradient descent method to maximize Θ_{LB} in (16) with step-size of 0.001, (iii) using

TABLE I
COMPARISON OF OPTIMIZED POWER-ALLOCATION PARAMETERS β_{opt} AND β^*, WHICH ARE OBTAINED BY MAXIMIZING THE EXACT EXPRESSION OF
THROUGHPUT IN (12) AND THE LOWER BOUND IN (16), RESPECTIVELY.

$c_R \setminus \rho$	5 dB		10 dB		15 dB		20 dB		25 dB		30 dB	
	β_{opt}	β^*	β_{opt}	β^*	β_{opt}	β^*	β_{opt}	β^*	β_{opt}	β^*	β_{opt}	β^*
0	0.807	0.74	0.746	0.725	0.687	0.695	0.633	0.653	0.586	0.609	0.545	0.567
0.1	0.817	0.741	0.757	0.727	0.698	0.698	0.644	0.657	0.597	0.613	0.557	0.571
0.2	0.828	0.742	0.77	0.729	0.712	0.702	0.658	0.662	0.611	0.618	0.571	0.575
0.3	0.841	0.743	0.784	0.731	0.728	0.706	0.675	0.667	0.628	0.623	0.588	0.58
0.4	0.856	0.79	0.802	0.733	0.747	0.71	0.696	0.673	0.649	0.629	0.61	0.585
0.5	0.873	0.812	0.822	0.736	0.771	0.715	0.721	0.679	0.676	0.636	0.637	0.592
0.6	0.894	0.813	0.848	0.738	0.8	0.72	0.753	0.687	0.711	0.644	0.674	0.6
0.7	0.918	0.814	0.879	0.741	0.837	0.726	0.796	0.696	0.758	0.655	0.725	0.611
0.8	0.948	0.815	0.918	0.75	0.885	0.733	0.854	0.708	0.824	0.671	0.798	0.627
0.9	0.981	0.815	0.966	0.814	0.948	0.74	0.93	0.725	0.914	0.695	0.901	0.653

$\beta = 3/4$, which corresponds to equal power-allocation for key generation and broadcast phase. In Table I, we list the values of β_{opt} and β^*, which maximize the exact throughput expression and its lower bound, respectively. Table I highlights that the absolute values of β offered by solving the optimization problem are different from that of uniform distribution, i.e., $\beta = 3/4$.

In Fig. 4, we present the plots on Θ , which are obtained by substituting β from (i), (ii), and (iii). The plots highlight that at $\rho = 15$ dB, the throughput values of all the three schemes are approximately same. However, at $\rho = 20$, 25, and 30 dB, the plots show that instead of allocating equal power to key generation and broadcast phase, the choice of β must be made by solving the proposed optimization problem as a function of c_R and ρ. In particular, Fig. 4 indicates that the gains over equal power-allocation is maximum when ρ is high and $c_R = 0$, which corresponds to Rayleigh channel between Node-R and Node-B. Furthermore, the plots show that the throughput values obtained by maximizing the lower bound is approximately same as that when optimizing the exact throughput expression.

D. Key Rate Analysis

In this section, we consider the metric of maximizing the key rate subject to an upper bound on the outage probability of the broadcast phase, given by $P_{out}^{(BR)} \leq \eta$, for some $\eta > 0$. The key rate maximization problem for a given $\eta > 0$ can be formally defined as below,

$$\arg \max_{\beta \in (0,1)} \log_2 \left(1 + \frac{(\frac{1-c_R}{2})^2 \beta^2 \rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right), \qquad (23)$$
$$\text{such that } P_{out}^{(BR)} \leq \eta.$$

We consider the following lemmas to solve the optimization problem in (23).

Lemma 4: The key rate in (8) is an increasing function of β.

Proof: Taking the first derivative of (8) w.r.t β, we get

$$\frac{d}{d\beta}M = \frac{d}{d\beta}\log_2\left(1 + \frac{(\frac{1-c_R}{2})^2\beta^2\rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right),$$
$$= \log_2 e \frac{1}{9 + 6(\frac{1-c_R}{2})\beta\rho + (\frac{1-c_R}{2})^2\beta^2\rho^2}$$
$$\times \frac{18(\frac{1-c_R}{2})^2\beta\rho + 12(\frac{1-c_R}{2})^3\beta^2\rho^3}{9 + 6(\frac{1-c_R}{2})\beta\rho}.$$

For $c_R \in [0,1]$, $\beta \in (0,1)$, and $\rho > 0$, $\frac{d}{d\beta}M$ is always positive, and thus the key rate, M is an increasing function of β. ∎

Lemma 5: The outage probability in (10) is an increasing function of β.

Proof: Taking the first derivative of (10) w.r.t β, gives

$$\frac{d}{d\beta}P_{out}^{(BR)} = -\frac{d}{d\beta}Q_1\left(\frac{\sqrt{c_R}}{\sqrt{\frac{1-c_R}{2}}}, \frac{\sqrt{h}}{\sqrt{\frac{1-c_R}{2}}}\right)$$
$$= \frac{1}{1-c_R}I_o\left(\frac{2\sqrt{c_R h}}{1-c_R}\right)e^{-\frac{c_R+h}{(1-c_R)}}$$
$$\times \frac{(\frac{1-c_R}{2})^2\beta\rho\left(18 - 9\beta + 6(\frac{1-c_R}{2})\beta\rho\right)}{\left(9 + 6(\frac{1-c_R}{2})\rho\beta - 9\beta - 6(\frac{1-c_R}{2})\beta^2\rho\right)^2}.$$

In the RHS on the above equation, the term $I_o(\frac{2\sqrt{c_R h}}{1-c_R}) > 1$ as given in [27]. The denominator of $\frac{d}{d\beta}P_{out}^{(BR)}$ is always positive. Furthermore, for $\beta \in (0,1)$, the numerator of the last product term is also always positive. Thus, $P_{out}^{(BR)}$ is an increasing function of β. ∎

With the above two lemmas, the optimization problem in (23) can be transformed into an equivalent problem, as given in the following theorem.

Theorem 3: The optimization problem in (23) has same optimal solution as that of the following problem.

$$\arg \max_{\beta \in (0,1)} \log_2 \left(1 + \frac{(\frac{1-c_R}{2})^2 \beta^2 \rho^2}{9 + 6(\frac{1-c_R}{2})\beta\rho}\right), \qquad (24)$$
$$\text{such that } P_{out}^{(BR)} = \eta.$$

Proof: Suppose that $\beta^\dagger$ is the solution that satisfies the outage probability equation in (24) for a given value of η. Since the outage probability is an increasing function of β by

Lemma 5, the solutions for the outage probability inequality equation in (23) for the same value of η will be in the interval $(0, \beta^\dagger]$. Furthermore, since the key rate expression (which is the objective function of (23) and (24)) is an increasing function of β by Lemma 4, the optimal solution for the optimization problem in (23) will also be $\beta^\dagger$. Thus, the optimal solution to (23) and (24) are the same.   ∎

Note that the outage probability, $P_{\text{out}}^{(BR)}$ is the complement of the first order Marcum Q-function, which is mathematically intractable. Thus, solving the root of the equality in (24) for a given η, requires a numerical approach. As a naive approach to numerically solve this problem, we need to plot the key rate along with the corresponding outage probability expression as a function of β for a given ρ and c_R (as shown in Fig. 4). Subsequently, to determine the maximum key rate with the outage probability constraint, we should draw a horizontal line $P_{\text{out}}^{(BR)} = \eta$ on the plots and then determine the point at which this line intersects the outage probability curve. The corresponding x-coordinate of this point of intersection gives the β value that maximizes the key rate under the constraint. However, as a formal approach to solve (24), a possible strategy is to use the well-known Newton-Raphson method [38], wherein the function $P_{\text{out}}^{(BR)} - \eta$ is used to iteratively compute the root by choosing a suitable step-size for β in the range $(0, 1)$.

IV. PERFORMANCE ANALYSIS WITH PRACTICAL KEY GENERATION ALGORITHMS

In this section, we discuss the buffer-aided protocol of Section II from an implementation viewpoint by considering practical key generation algorithms at the three nodes, and an empty buffer at the start of the key generation protocol.

A. Buffer-aided Relay Protocol

In this section, we adopt the relay-assisted key generation protocol discussed in Section II-A, with the exception that practical key generation algorithms are used to optimize the throughput and the key rate yard-sticks. Adopting the state-of-the art key generation protocol [29] on their observations, Node-A and Node-R, unfold each complex number into two real values. Subsequently, a two-level crossing algorithm is applied on the samples by choosing an appropriate guard band, denoted by q^- and q^+, such that the key miss-match rate is less than or equal to ϵ, for some $\epsilon > 0$. After applying the algorithm in [29], Node-R generates a key k_{AR} of length N_{AR} with Node-A, and also generates a key k_{BR} of length N_{BR} along with Node-B. Since N_{AR} and N_{BR} are random variables, we are interested in characterizing the average key lengths $\mathbb{E}[N_{AR}]$ and $\mathbb{E}[N_{BR}]$. Towards that direction, the following lemma is straightforward to prove.

Lemma 6: With y_A and y_R denoting the real sample of a coherence-block between Node-A and Node-R, the probability that the two samples are in consensus is $p_\epsilon = \iint\limits_{y_A, y_R \notin (q-, q+)} f(y_A, y_R) dy_A dy_R$, where $f(y_A, y_R)$ denotes the joint density function of y_A and y_R, and $q+$ and $q-$

represent the threshold levels of the guard band of the two-level crossing algorithm.

The consensus probability for samples between Node-B and Node-R is also p_ϵ since the two channels are identically distributed. With $2L$ real samples subject to the two-level key generation algorithm, and since each real sample is statistically identical and independent, the key length between a pair of nodes is equal to the number of real samples in consensus. Thus, we note that both N_{AR} and N_{BR} are independent Binomial random variables defined as $N_{AR} \sim \mathcal{B}in(2L, p_\epsilon)$, and $N_{BR} \sim \mathcal{B}in(2L, p_\epsilon)$, and therefore, we have $\mathbb{E}[N_{AR}] = \mathbb{E}[N_{BR}] = 2Lp_\epsilon$. In case, a multi-level crossing algorithm is used for key generation [31], the average key length will be multiplied by f, where 2^f is the number of levels of the quantizer. From the buffer-aided relay model, the length of k_{XOR} depends on the difference between N_{AR} and N_{BR}, and the size of the buffer at that point. In practice, the buffer may not have sufficient bits, and therefore, we expect N_{XOR} to be less than N_{AR} in some rounds of the key generation protocol. In the next section, we revisit the broadcast phase of the relay model in order to compute $\mathbb{E}[N_{XOR}]$ with buffer constraints.

B. Broadcast Phase with Buffer Constraints

We recollect from Section II-A that the buffer bits at Node-R are the unused bits in consensus between Node-B and Node-R from the previous *rounds* of the key generation protocol. To incorporate practical constraints on the buffer for analyzing the throughput and key rate, we incorporate the round number $m \geq 0$ when referring to the buffer size, keys and their lengths. Consequently, $B(m), N_{AR}(m), N_{BR}(m), N_{XOR}(m)$ denote the buffer size, the pair-wise key lengths, and the length of the sequence $k_{XOR}(m)$ broadcast to Node-B at the end of the mth round. With these definitions, we immediately note that $N_{AR}(m), N_{BR}(m)$ are statistically independent across m, whereas $B(m)$ and $N_{XOR}(m)$ are statistically dependent across m because the latter numbers depend on $B(m-1)$, $N_{AR}(m)$ and $N_{BR}(m)$. In particular, with the updates in (4) and (5), we broadly have three types of schemes, namely:

- The optimal scheme, wherein $B(m) = \infty, \forall m$,
- The min-scheme, wherein $B(m) = 0, \forall m$, and
- The intermediate scheme, where $B(0) = 0$ for $m = 0$.

We note that the optimal scheme is such that $\mathbb{E}[N_{XOR}(m)] = \mathbb{E}[N_{AR}(m)] = 2Lp_\epsilon$, for all m, whereas the min-scheme is such that $\mathbb{E}[N_{XOR}(m)] = \mathbb{E}[\min(N_{AR}(m), N_{BR}(m))]$ for all m. Given that the intermediate scheme makes use of the buffer as and when available, it is intuitive that $\mathbb{E}[N_{XOR}(m)]$ of the intermediate scheme should lie in between that of the optimal scheme and the min-scheme. Moreover, unlike the optimal scheme and the min-scheme, we expect that $\mathbb{E}[N_{XOR}(m)]$ for the intermediate scheme changes as a function of m since $\{B(m) \mid m \geq 0\}$ is a non-stationary random process. Towards understanding the behavior of $\mathbb{E}[N_{XOR}(m)]$ of the three schemes, we present simulation results to compute the average key lengths of their broadcast phase, i.e., $\mathbb{E}[N_{XOR}(m)]$ for various values of m. In Fig. 5, we plot the average key lengths of all the three schemes as a function of m for the
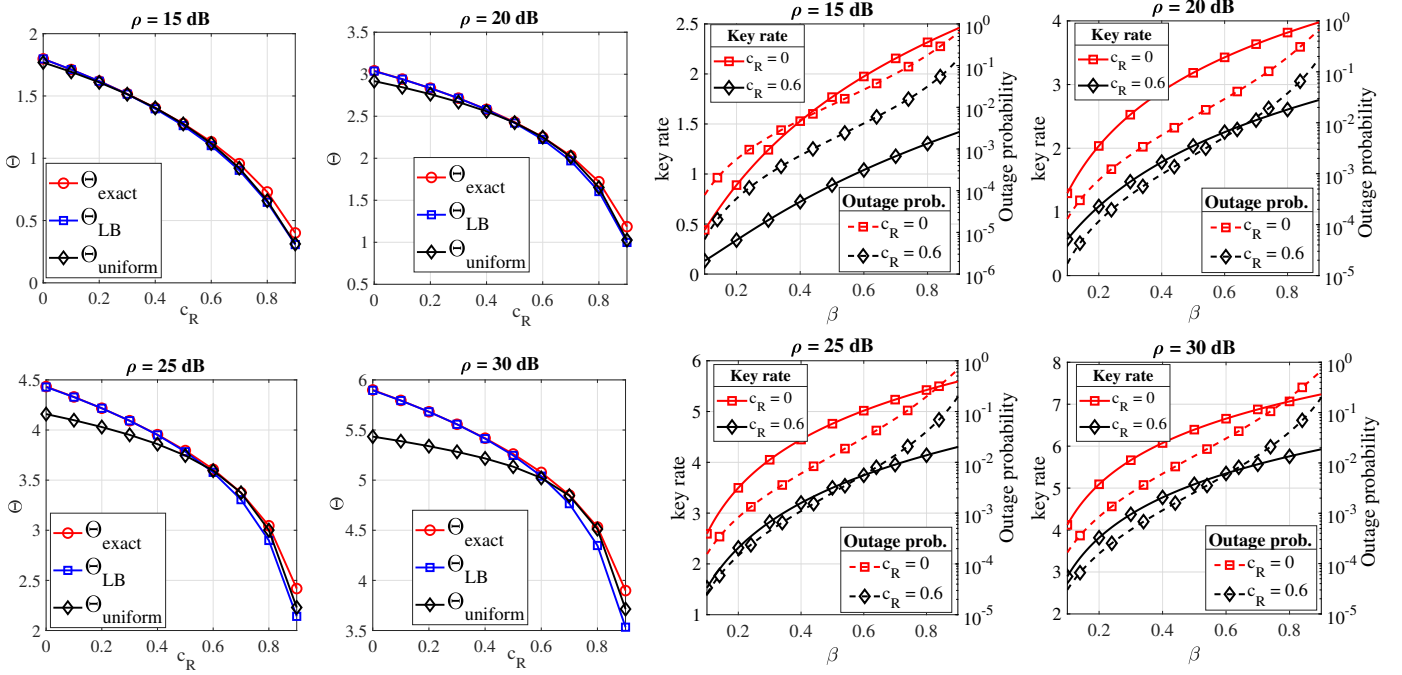
Fig. 4. **On the left:** Plots of throughput when β is optimized using (i) Θ_{exact}, the exact throughput expression in (12), (ii) the lower bound Θ_{LB} given in (16), and (iii) Θ_{uniform}, which corresponds to equal power-allocation for the key generation phase and the broadcast phase. **On the right:** Plots of key rate and its outage probability as a function of β with various values of ρ and c_R, while considering that block length is asymptotically large.

channel condition $\rho = 20$ dB, $\beta = 0.6$, and $c_R = 0.2$. Furthermore, under the intermediate scheme, we plot the average key lengths for various buffer switch-on time-instants. In this context, the buffer switch-on time is the round index of the key generation protocol until which the min-scheme is active, i.e., the buffer is allowed to grow from $m = 0$ till the switch-on instant whenever $N_{AR}(m) < N_{BR}(m)$. To generate the simulation results, the buffer switch-on time were $\{0, 10, 30, 50, 100, 150\}$. From the simulation results, we observe that the intermediate scheme achieves the optimal scheme when the buffer is switched-on at $\{100, 150\}$, and it is apparent that we do not need to wait longer than $m = 100$ to achieve the optimal key length. Inspired by the observations made in Fig. 5, we would like to theoretically analyze the key lengths, i.e., $\mathbb{E}[N_{XOR}(m)]$ for any given m, offered by the three variants. Note that the average key lengths of these regimes are different from that of the asymptotic case because these average key lengths are from using a practical key generation algorithm as opposed to the optimal one as discussed in Section III. In order to characterize $\mathbb{E}[N_{XOR}(m)]$, we need to understand the probability mass function (PMF) on the difference between $N_{AR}(m)$ and $N_{BR}(m)$ (which are individually binomially distributed and statistically independent), and also the PMF on $B(m)$. In the following lemma, we present the PMF on $D(m) \triangleq N_{AB}(m) - N_{BR}(m)$ by dropping the index m since $D(m)$ is identically distributed across m.

Lemma 7: Given $N_{AR}, N_{BR} \sim \mathcal{B}in(2L, p_\epsilon)$ and are statistically independent, the PMF on $D = N_{AR} - N_{BR}$, i.e., $P(D = d)$, for $-2L \leq d \leq 2L$, can be computed as in (25).

In the following lemma, we provide a way to construct the PMF on $B(m)$ for any $m \geq 1$.

Lemma 8: Assuming that the buffer is switched-on at round m', the PMF on $B(m)$ can be computed in closed-form for any $m > m'$.

Proof: Throughout the proof, we use $n = 2L$. Let $B(m') = B_0 < n$ be the size of buffer at the time when buffer is switched on. At the $(m'+1)$th round of key generation, we have

$$B(m'+1) = \begin{cases} B(m') - D(m'+1), & \text{if } D(m'+1) \leq B(m'); \\ B(m'), & \text{if } D(m'+1) > B(m'); \end{cases}$$

$$(25)$$

where $B(m'+1) = N_{AR}(m'+1) - N_{BR}(m'+1)$ is a random variable which has a support set, $\mathcal{S}upp(B(m'+1)) = [0, B(m') + n]$. Since $B(m')$ is a constant, the PMF of $B(m'+1)$ can be easily determined using the PMF of $D(m'+1)$ as in (26), where b_1 is a realization of $B(m'+1)$. At the $(m'+j)^{th}$ round of key generation, for $j \geq 2$, the buffer size is updated using the distribution on $B(m'+j-1)$ as given in (27), where $\mathcal{S}upp(B(m'+j)) = [0, B(m') + jn]$. Defining a new random variable $Y(m'+j) = B(m'+j-1) - D(m'+j)$ whose PMF can be determined, the PMF of $B(m'+j)$ can be determined as below by using b_j as a realization of $B(m'+j)$.

Case 1: $0 \leq b_j \leq B(m') + (j-1)n$:

$$P(B(m'+j) = b_j)$$
$$= P(B(m'+j-1) = b_j)P(D(m'+j) > b_j) \qquad (28)$$
$$+ P(Y(m'+j) = b_j).$$

Case 2: $B(m') + (j-1)n + 1 \leq b_j \leq B(m') + jn$:

$$P(B(m'+j) = b_j) = P(Y(m'+j) = b_j). \qquad (29)$$

This completes the proof. ∎

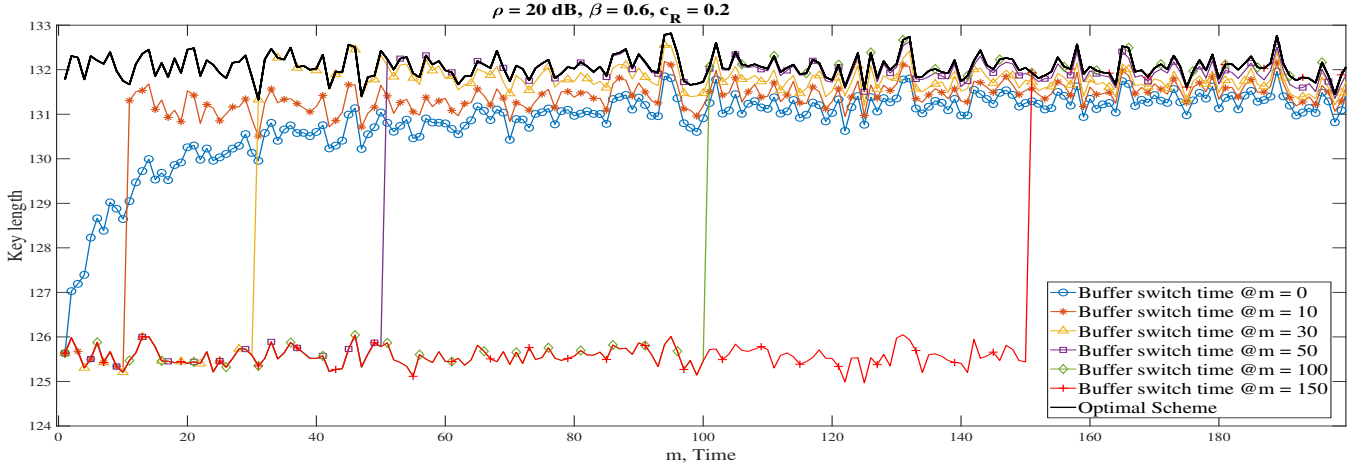Using the PMFs on $D(m)$ and $B(m)$, in the following theorem, we provide a closed form expression on the average

Fig. 5. Plots of average key lengths as a function of time for SNR $\rho = 20$ dB, power optimization parameter, $\beta = 0.6$, LOS parameter, $c_R = 0.2$, and number of coherence-blocks, $L = 100$ for variable bits available in the buffer at different instants of time.

$$P(D = d) = \begin{cases} \sum_{t=0}^{2L+d} \binom{2L}{t} p^t (1-p)^{(2L-t)} \binom{2L}{t-d} p^{(t-d)} (1-p)^{(2L-t+d)}, & \text{if } -2L \le d < 0; \\ \sum_{t=0}^{2L-d} \binom{2L}{t+d} p^{(t+d)} (1-p)^{(2L-t-d)} \binom{2L}{t} p^t (1-p)^{(2L-t)}, & \text{if } 0 \le d \le 2L. \end{cases} \tag{25}$$

$$P(B(m'+1) = b_1) = \begin{cases} P(D(m'+1) > B(m')) + P(D(m'+1) = 0), & \text{if } b_1 = B(m'); \\ P(D(m'+1) = B(m') - b_1), & \text{if } 0 \le b_1 \le B(m') + n \ \& \ b_1 \ne B(m'); \end{cases} \tag{26}$$

$$B(m'+j) = \begin{cases} B(m'+j-1) - D(m'+j) & \text{if } D(m'+j) \le B(m'+j-1); \\ B(m'+j-1), & \text{if } D(m'+j) > B(m'+j-1); \end{cases} \tag{27}$$

key length of the intermediate that has $B(m-1) = b_{m-1}$ bits in the buffer for the mth round.

Theorem 4: Given that $B(m-1) = b_{m-1}$, for some fixed $b_{m-1} > 0$, the average key length of the buffer-aided practical key generation scheme for the mth round is given by (30), where $P_{N_{AR}(m)}(\cdot)$ and $P_{N_{BR}(m)}(\cdot)$ denote the evaluation of PMF of $N_{AR}(m)$ and $N_{BR}(m)$ at a particular realization, respectively.

Proof: By definition, $N_{XOR}(m)$ is given by

$$N_{XOR}(m) = \begin{cases} N_{AR}(m), & \text{if } N_{AR}(m) - N_{BR}(m) \le b_{m-1}; \\ N_{BR}(m), & \text{if } N_{AR}(m) - N_{BR}(m) > b_{m-1}. \end{cases} \tag{31}$$

Since b_{m-1} is a constant, we can use the joint probability mass function of $N_{AR}(m)$ and $N_{BR}(m)$, denoted by $P_{N_{AR}(m), N_{BR}(m)}(\cdot, \cdot)$, to compute $\mathbb{E}[N_{XOR}(m) \mid B(m-1) = b_{m-1}]$ as below:

$$\begin{aligned} & \mathbb{E}[N_{XOR}(m)/B(m-1) = b_{m-1}] \\ &= \sum_{z_2} \sum_{z_1} z P_{N_{AR}(m), N_{BR}(m)}(z_1, z_2), \\ &= \sum_{z_2} \sum_{z_1} z P_{N_{AR}(m)}(z_1) P_{N_{BR}(m)}(z_2), \\ &= \sum_{z_2=0}^{n-b_{m-1}} \left\{ \sum_{z_1=0}^{b_{m-1}+z_2} z_1 P_{N_{AR}(m)}(z_1) \right\} P_{N_{BR}(m)}(z_2) \\ &\quad + \sum_{z_1=b_k+1}^{n} \left\{ \sum_{z_2=0}^{z_1-b_k-1} z_2 P_{N_{BR}(m)}(z_2) \right\} P_{N_{AR}(m)}(z_1), \end{aligned} \tag{32}$$

wherein z_1 and z_2 run through different realizations of $N_{AR}(m)$ and $N_{BR}(m)$, while z takes the appropriate value depending on z_1, z_2 and b_{m-1}, as defined in (31). This completes the proof. ■

Finally, using the above result, the overall average key length for the mth round can be computed as in (33). As a special case of the above expression, we can also obtain average key length of the optimal scheme and min-scheme. In particular, to obtain the optimal scheme as a special case, applying $B(m) = \infty, \forall m$ in (4), we observe that $N_{AR}(m) - N_{BR}(m) > B(m-1)$ never happens, and therefore, we have

$$\mathbb{E}[N_{XOR}(m)] = \mathbb{E}[N_{AR}(m)] = \sum_{z_1=0}^{n} z_1 P_{N_{AR}(m)}(z_1). \tag{34}$$

Note that the above expression corresponds to the black curve in Fig. 5. Similarly, we can also obtain the average key length of the min-scheme by using $B(m) = 0, \forall m$. As a result, we get (34). We now need to use $\mathbb{E}[N_{XOR}(m)]$, for $m \ge 1$, to compute the power-allocation parameter β such that the throughput is maximized or the key rate is maximized subject to the outage probability constraint in the broadcast phase.

C. Throughput and Key Rate Analysis

Based on our protocol for the mth round, the key generation phase is executed with $\beta \in (0,1)$, after which Node-R has an average of $\mathbb{E}[N_{XOR}(m)]$ secret bits from the first L

$$
\mathbb{E}[N_{XOR}(m) \mid B(m-1) = b_{m-1}]
$$

$$
= \sum_{z_1=b_{m-1}+1}^{n} \left\{ \sum_{z_2=0}^{z_1-b_{m-1}-1} z_2 P_{N_{BR}(m)}(z_2) \right\} P_{N_{AR}(m)}(z_1) + \sum_{z_2=0}^{n-b_{m-1}} \left\{ \sum_{z_1=0}^{b_{m-1}+z_2} z_1 P_{N_{AR}(m)}(z_1) \right\} P_{N_{BR}(m)}(z_2), \tag{30}
$$

$$
\mathbb{E}[N_{XOR}(m)] = \sum_{b_{m-1} \in \mathbb{S}upp(B(m-1))} P(B(m-1) = b_{m-1})\mathbb{E}[N_{XOR}(m)|B(m-1) = b_{m-1}]. \tag{33}
$$

$$
\mathbb{E}[N_{XOR}(m)] = \sum_{z_1=1}^{n} \left\{ \sum_{z_2=0}^{z_1-1} z_2 P_{N_{BR}(m)}(z_2) \right\} P_{N_{AR}(m)}(z_1) + \sum_{z_2=0}^{n} \left\{ \sum_{z_1=0}^{z_2} z_1 P_{N_{AR}(m)}(z_1) \right\} P_{N_{BR}(m)}(z_2). \tag{34}
$$

---

coherence-blocks. In the $(L + 1)$th coherence-block, Node-R communicates this message using a code of block-length L with rate $R = \frac{\mathbb{E}[N_{XOR}(m)]}{L}$, such that the average power per channel use is $(1 - \beta)P$. Towards studying the error performance of the code used for the broadcast phase, the outage probability expression of Section III is no longer applicable since L need not be large in practice. As a result, we apply the corresponding non-asymptotic outage probability results of [30] to compute $P_{\text{out}}^{(BR)}(m)$ as a function of β. Formally, $P_{\text{out}}^{(BR)}(m)$ can be computed as

$$
P_{\text{out}}^{(BR)}(m) = \int_{\mathbb{R}} Q\left(\sqrt{\frac{L}{V(\Gamma)}}(C(\Gamma) - R) \right) f_{\Gamma}(\Gamma)d\Gamma, \tag{36}
$$

where $\Gamma = |h_{BR}|^2(1 - \beta)\frac{P}{\gamma}$ is the instantaneous SNR of the wireless channel, $(1 - \beta)P$ is the average power per channel use, R is the code rate, $f_{\Gamma}(.)$ is the probability density of the instantaneous SNR Γ, $C(\Gamma) = log_2(1 + \Gamma)$ is the Shannon channel capacity, $V(\Gamma) = \frac{\Gamma}{2}\frac{\Gamma+2}{(\Gamma+1)^2}log_2^2 e$ is the back-off factor for finite block-length, and finally, $Q(x) = \frac{1}{2\pi}\int_x^{\infty} e^{-\frac{u^2}{2}} du$. When using a practical key generation algorithm along with finite block length code, we observe that both the average key length $\mathbb{E}[N_{XOR}(m)]$ and the outage probability $P_{\text{out}}^{(BR)}(m)$ are not available in closed-form, and therefore, we solve the optimization problem $\arg\max_{\beta \in (0,1)} \mathbb{E}[N_{XOR}(m)](1 - P_{\text{out}}^{(BR)}(m))$ using simulation results.[5]

To generate the simulation results, we fix $L = 100$, and then vary the value of $\beta \in (0, 1)$ at discrete steps to compute $\mathbb{E}[N_{XOR}(m)](1 - P_{\text{out}}^{(BR)}(m))$ for both the optimal scheme and the min-scheme. These simulations are presented in Fig. 6 for the LOS parameters $c_R = [0, 0.6]$ and SNR, $\rho = [15, 20, 25, 30]$ in dB. We observe that the optimal value of β that maximizes the throughput is close to $\beta = 0.9$, and this behavior is unlike the throughput analysis for the asymptotic case. This difference is because of two factors: first, in the broadcast phase the generated key is encoded using a strong channel code of block-length L, and second, the rate of increase of $\mathbb{E}[N_{XOR}(m)]$ as β increases is low due to two-level quantizer employed in key generation process. In general, when either a multi-level crossing algorithm is used

for key generation, or when the codes used for the broadcast is uncoded, we expect the optimal value of β to reduce. We also observe from the plots that the optimal scheme outperforms the min-scheme in throughput [12], [13], [15], [19]. For instance, in Fig. 6 when $\rho = 15$ dB and $c_R = 0$, optimal scheme with optimal power allocation yields 8% increase in throughput, in comparison to min-scheme with equal power allocation.

Similar to the key rate analysis for the asymptotic case in Section III-D, in Fig. 6, we plot the average key length and outage probability for the case of short block-lengths. We observe that both the average key length and the outage probability increase as β increases. To determine the optimal value of β that provides maximum key rate subject to given outage probability, we suggest drawing a horizontal line which corresponds to the given outage probability constraint, and then the x-coordinate of the intersection point of the line gives the optimal β value. The plots in Fig. 6 show that for a given outage probability constraint, the optimal scheme provides higher key rate compared to the min-scheme, which is none other than the existing buffer-less key generation method [12], [13], [15], [19]. This behavior can be attributed to the fact that although the optimal scheme provides higher values of $\mathbb{E}[N_{XOR}(m)]$, the corresponding difference in the rate does not result in significant changes in the outage probability. For instance, in Fig. 6 when $\rho = 15$ dB, $c_R = 0$, optimal scheme yields 9% increase in average key length, in comparison to min-scheme subject to outage probability, $P_{\text{out}}^{(BR)} = 10^{-2}$. Overall, the simulation results of this section have shown that the optimal scheme with the help of the buffer outperforms the min-scheme [12], [13], [15], [19].

V. BUFFER-AIDED PROTOCOL WITH ASYMMETRIC LOS CHARACTERISTICS

In Section II, we introduced a network model wherein the LOS parameters of the channels between Node-A and Node-R, and Node-B and Node-R are identical (denoted by $c_R \in [0, 1]$). As a result, without loss of generality, the key generated between Node-A and Node-R during the key generation phase is broadcast to Node-B, although the roles of Node-A and Node-B could have been swapped. However, if a relay network is such that the channels between Node-A (or Node-B) and Node-R have different LOS parameters, then

---

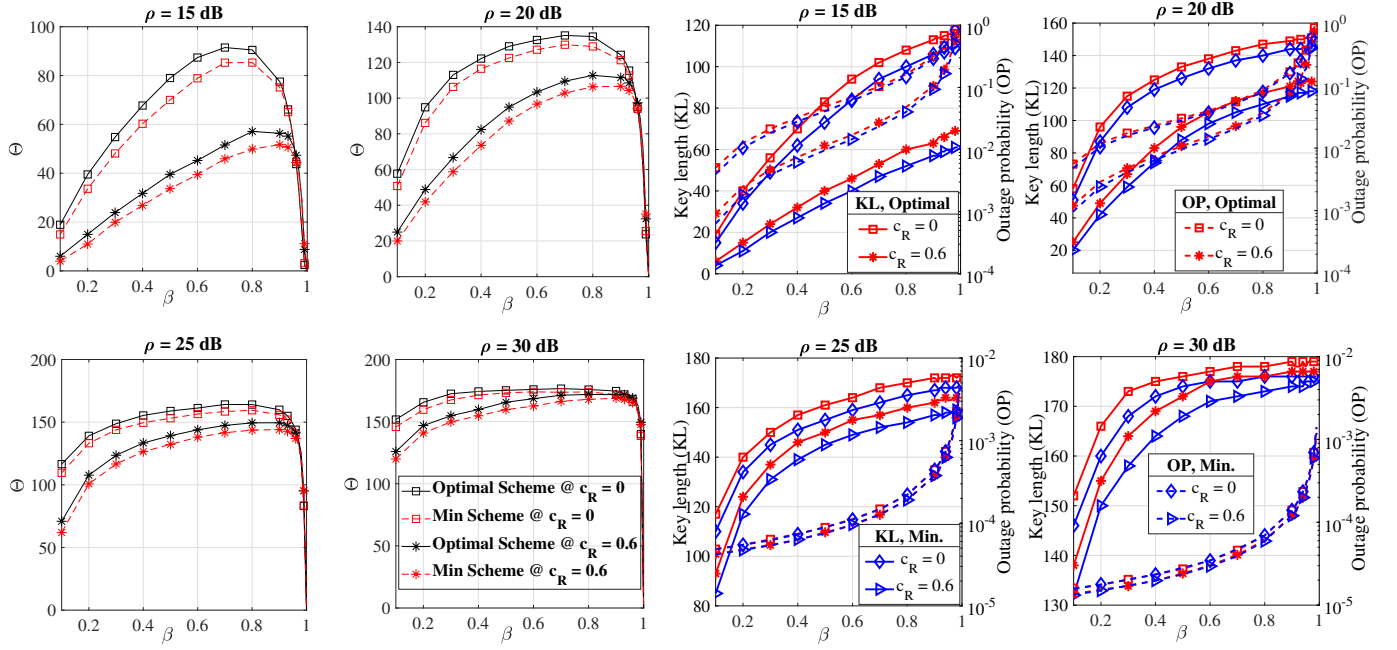[5]Consensus power is not considered in the optimization problem as in the similar case of asymptotic analysis.

Fig. 6. **On the left:** Plots of throughput as a function of β with various values of ρ and c_R. The legend in the fourth subplot applies to all subplots of left side. **On the right:** Plots of average key length and its outage probability as a function of β with various values of ρ and c_R. Note that four legends in each subplot apply to all subplots.

appropriate modifications on the buffer-aided protocol must be discussed. Towards that direction, the following proposition states that higher the LOS parameter of the channel, lower is the key rate offered by the PLK generation.

Proposition 1: The mutual information $I(y_A^{(3)}(l); y_R^{(1)}(l))$ in (8) is a decreasing function of $c_R \in [0, 1]$.

To formally discuss the modifications needed on the buffer-aided protocol, let $c_{AR} \in [0, 1]$ and $c_{BR} \in [0, 1]$ represent the LOS components of h_{AR} and h_{BR}, respectively. Furthermore, suppose that $c_{AR} < c_{BR}$. During the key generation phase of the protocol, it is clear from Proposition 1 that the pair-wise keys k_{AR} and k_{BR} are such that $N_{BR} < N_{AR}$ with high probability in each round of the protocol. As a result, even if the relay assisted key generation is executed over several rounds to fill the buffer with unused bits of k_{BR}, there will not be sufficient bits to provide confidentiality to achieve N_{AR} as the key length. Thus, choosing k_{BR} as the key for broadcast is the best strategy, and hence, buffers are no longer useful. Note that the key k_{BR} should not be broadcast to Node-A through h_{AR} because transmitting a message over lower LOS channel results in higher values of outage probability compared to transmitting over a channel with higher LOS parameter. Because of this result, we propose that Node-R uses the first N_{BR} bits of k_{AR}, and then broadcast an XOR version to Node-B. This way, both the key-rate of the key generation phase as well as the outage probability of the broadcast phase are functions of the LOS parameter c_{BR}. Consequently, the optimization problems for throughput and key rate for this case can be solved by applying the techniques in Section III and Section IV, however, by replacing c_R with c_{BR}. Overall, we have shown that the power-allocation strategies proposed in this work are also applicable to a relay network when the LOS components of the two channels are different.

VI. SUMMARY

We addressed a key generation scenario wherein two wireless devices seek the assistance of a trusted relay to generate secret-keys. To handle the reduction in key rate due to XOR based broadcast, we have proposed buffer-aided key generation protocol at the relay wherein the unused secret bits generated between the relay and one of the nodes can be temporarily stored in a buffer before using them to provide the confidentiality feature for the broadcast phase in the subsequent rounds. We have also proposed power allocation policies between the key generation phase and broadcast phase by optimizing the overall key rate and throughput in different scenarios: (i) Optimal or practical key generation methods and (ii) empty buffer at the start of algorithm. Simulation results show that using buffer results in remarkable benefits when the LOS of the two channels are close.

Towards implementing the strategies proposed in this work, the knowledge of the LOS component is required for choosing an appropriate value of the power-allocation factor. In practice, we believe that this could be achieved in the following way. Before a pair of nodes initiates the key generation process, each node processes to detect the LOS component by estimating the fading channel characteristics. For instance, the techniques mentioned in [36], [37] could be used since LOS component is usually a long-term characteristic of the channel. Subsequently, for every round of secret key generation, each node could use the corresponding optimal power allocation parameter (solved using our proposed scheme) against the detected LOS component. One way to implement this in practice is to store a table of the power allocation parameter values and the LOS values a priori in the memory of the devices. With this stored information, in the subsequent rounds

of secret key generation and distribution, the three nodes could allocate the power for their transmission by looking up the table in the memory.

REFERENCES

[1] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

[4] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[5] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1779–1790, Sep. 2013.

[6] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Channel frequency response-based secret key generation in underwater acoustic systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5875–5888, Sep. 2016.

[7] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[8] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[9] R. Wilson, D. Tse, and Robert A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[10] F. Rottenberg, T. Nguyen, J. Dricot, F. Horlin, and J. Louveaux, "CSI-based versus RSS-based secret-key generation under correlated eavesdropping," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1868–1881, Mar. 2021.

[11] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[12] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[13] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 3, pp. 476–488, Mar. 2014.

[14] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 650–660, Sep. 2011.

[15] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[16] P. Xu, Z. Ding, X. Dai, and G. K. Karagiannidis, "Simultaneously generating secret and private keys in a cooperative pairwise-independent network," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 6, pp. 1139–1150, Jun. 2016.

[17] R. Guillaume, S. Ludwig, A. Müller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in *Proc. IEEE WiMob*, 2015.

[18] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 02, pp. 1517–1530, Feb. 2016.

[19] M. Waqas, M. Ahmed, Y. Li, D. Jin, and S. Chen, "Social-aware secret key generation for secure device-to-device communication via trusted and non-trusted relays," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3918–3930, Jun. 2018.

[20] Nasser Aldaghri and Hessam Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2692–2705, Feb. 2020.

[21] Jing Huang and A. Lee Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.

[22] Jing Wan, Deli Qiao, Hui-Ming Wang, and Haifeng Qian, "Buffer-aided two-hop secure communications with power control and link selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635–7647, Nov. 2018.

[23] R. Nakai and S. Sugiura, "Physical layer security in buffer-state-based max-ratio relay selection exploiting broadcasting with cooperative beamforming and jamming," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 431–444, Feb. 2019.

[24] X. Tang *et al.*, "Secrecy outage analysis of buffer-aided cooperative mimo relaying systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2018.

[25] X. Liao *et al.*, "On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1893–1906, Mar. 2018.

[26] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Link selection for security-qos tradeoffs in buffer-aided relaying networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1347–1362, Sep. 2019.

[27] Y. L. Luke, "Inequalities for generalized hypergeometric functions," *J. Approximation Theory*, vol. 5, no. 1, pp. 41–65, Jan. 1972.

[28] Y. Sun, A. Baricz, and S. Zhou, "On the monotonicity, log-concavity, and tight bounds of the generalized Marcum and Nuttall Q-functions," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1166–1186, Mar. 2010.

[29] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. ACM MobiCom*, Sep. 2008.

[30] Y. Polyanskiy, H. Vincent Poor, and S. Verdu, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[31] H. Jagadeesh, R. Joshi, and M. Rao, "Group secret-key generation using algebraic rings in wireless networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1538–1553, Feb. 2021.

[32] H. M. Furqan , J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 59–63, Jan. 2021.

[33] A. Abdi, C. Tepedelenlioglu, M. Kaveh, and G. Giannakis, "On the estimation of the K parameter for the Rice fading distribution," *IEEE Commun. Lett.*, vol. 5, no. 3, pp. 92–94, Mar. 2001.

[34] T. M. Cover and J. A. Thomas, *Elements of information theory*. New York: Wiley, 1991.

[35] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.

[36] D. L. Hall, M. J. Brandsema, and R. M. Narayanan, "Derivation of K-factor detection statistics to discriminate between LOS and NLOS scenarios," *IEEE Trans. Wireless Commun.*, Early Access, 2021

[37] F. Benedetto, G. Giunta, and L. Vandendorpe "LOS/NLOS detection by the normalized Rayleigh-ness test," in *Proc. IEEE EUSIPCO*, 2009.

[38] M. W. Hirsch and S. Smale, "On algorithms for solving $f(x) = 0$," *Commun. Pure Appl. Math.*, vol. 32, no. 3, pp. 281–312, 1979.

Rusni Kima Mangang received the B.E. degree with honours in Electronics and Communication Engineering from Manipur University, India, in 2005, securing the first rank in Electronics and Communication Engineering. He obtained the M.E. degree in Applied Electronics from Anna Univeriity in 2008. He is currently pursuing a Ph.D. degree in the Department of Electrical Engineering, IIT Delhi, Delhi, India. Since December 2009, he has been a faculty member with the Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology, Itanagar, India. His current research interests information-theoretic security and key generation.

Harshan Jagadeesh is an Assistant Professor in the Department of Electrical Engineering, Indian Institute of Technology Delhi. Prior to joining IIT Delhi, he worked as a Researcher in the CyberSecurity group at Advanced Digital Sciences Center, Singapore. Before that he worked as a Research Fellow in the Division of Mathematical Sciences, Nanyang Technological University, Singapore and in the Department of Electrical and Computer Systems Engineering at Monash University, Australia. He obtained the Ph.D. degree from the Department of Electrical Communication Engineering, Indian Institute of Science, India in 2010. His research interests are in the broad areas of security, wireless networks, and applications of information theory and coding theory to communication and storage.