End-to-End Secure Multi-Hop Communication with Untrusted Relays

Xiang He, *Member, IEEE,* and Aylin Yener, *Member, IEEE*

***Abstract*—A multi-hop line network is considered, where each node can receive signals transmitted by its two neighbors. As such, the model embodies both the interference and broadcast aspects of wireless networks. The leftmost node wishes to send messages to the rightmost node, while keeping these messages confidential from *all* the intermediate relay nodes. In this setting where any or all of the relay nodes can be eavesdroppers, it is shown that end-to-end secure and reliable communication is possible. Notably, it is shown that an end-to-end secrecy rate that is *independent* of the number of hops, i.e., intermediate eavesdroppers, is achievable by means of a carefully designed transmission schedule, compute-and-forward relaying and coding strategy utilizing nested lattice codes. The achievable rate obtained indicates that imposing secrecy constraints penalizes the capacity by at most 1 bit per channel use. Therefore, it is concluded that information theoretic secrecy can be guaranteed for this model irrespective of eavesdropping relays and a fixed modest cost for the end-to-end rate.**

***Index Terms*—Information theoretic secrecy, nested lattice code, line network, untrusted relays.**

I. Introduction

WIRELESS networking is rapidly becoming the dominant means to communicating any and all information. It is by now clear that guaranteeing secure transfer of all this information is as important as reliability. A prominent concern, as we collectively become a wireless society, is to ensure confidentiality of information communicated in this open medium from unauthorized parties. While information security is currently handled by upper layer protocols that are agnostic to the underlying communication medium, the merit of physical layer aware security solutions are beginning to be noticed for wireless communications [1].

The theoretical foundation of information security dates back to Shannon [2]. In this work, Shannon established confidentiality, i.e., secrecy, to be measured by the mutual information at the unauthorized receiver[1]. Following this framework, Wyner studied the wiretap channel [3] and showed that reliable communication that is secret from an eavesdropper was possible in the setting where the eavesdropper receives a noisy version of that received by the destination. His result and references [4], [5], which guarantee secrecy irrespective of the computational capabilities of the eavesdropper, are a departure from cryptographic approaches, and have established the foundations of information theoretic secrecy.

Recently, there has been a renewed interest in information theoretic secrecy, notably towards identifying the fundamental rate limits of transmitting confidential data in channel models that are building blocks of wireless networks; see for example [6]–[9] and references therein. By nature of network information theoretic building blocks, these works consider small networks of a few nodes and determine upper and lower bounds on secrecy rates.

For networks of arbitrary size, Shannon's notion of information theoretic secrecy, has led to secure network coding [10], [11] where the confidential message must be transmitted over *multiple* hops. This setting is appropriate for wired networks as each link is modeled as a rate-limited noiseless bit pipe.

A wireless network differs fundamentally from a network of noiseless bit pipes. The broadcast nature of the medium results in signals transmitted by a node to be overheard by all, making it easier to eavesdrop. Further, interference results from multiple transmissions overheard by all nodes and fundamentally alters the methods with which information theoretic secrecy can be provided. In fact, interference was shown to be a useful resource to protect confidential messages from being leaked to an eavesdropper, see for example [6]. Hence, a collection of interference free links is not the best representation of a wireless network with secure communication requirements. Finally, in a wireless network, it is more natural to consider the eavesdropper eavesdrops on nodes, rather than on edges. The preceding discussion makes it clear that secure network codes designed for wired networks are not applicable for wireless networks [12], [13].

In this paper, we consider confidential message transfer for wireless networks of arbitrary size within an information theoretic secrecy framework. In order to address this problem with the simplest model which retains the characteristics of a wireless communication medium, namely, broadcast and interference, we consider a line network. The source and the destination in this network are connected by a chain of nodes, any or all of which, despite being a part of the network, and willing to carry out relaying functions, are not to be trusted with the information sent from the source to the destination. To this end, all of these nodes need to be treated as potential eavesdroppers.

Manuscript received July 28, 2010; revised February 20 and October 23, 2011; accepted October 4, 2012. The associate editor coordinating the review of this paper and approving it for publication was T. J. Li.

This work was presented in part at the Allerton Conference on Communication, Control, and Computing, September 2008, and the 42nd Asilomar Conference on Signals, System and Computers, October 2008. This work has been supported in part by the National Science Foundation via Grants CCR-0237727, CCF-051483, CNS-0716325, CIF-0964362 and the DARPA ITMANET Program via Grant W911NF-07-1-0028.

X. He was with the Department of Electrical Engineering at the Pennsylvania State University, University Park, PA 16802. He is now with Microsoft (e-mail: xianghe@microsoft.com).

A. Yener is with the Department of Electrical Engineering, Pennsylvania State University, University Park, PA 16802 (e-mail: yener@ee.psu.edu).

Digital Object Identifier 10.1109/TWC.2012.120412.101358

[1]Here onward this unauthorized party is termed *an eavesdropper*.

We show that, in this network, secure communication is possible between the source and the destination despite the fact that the signals transmitted by the source can reach the destination only through the route using these untrusted nodes. Furthermore, we show that the achievable end-to-end secrecy rate found in this paper is *independent* of the number of hops. This is tantamount to saying that the achievable secrecy rate is constant no matter how many eavesdropping relays are present, and the result holds for an arbitrary size of a line network.

This network can be viewed as a somewhat idealized version of a multi-hop wireless ad-hoc network [2] In particular, the nodes are assumed to be sufficiently far apart that each can only hear from its closest two neighbors. One can also envision some applications, for which this modeling abstraction is more precise. For instance, this can represent a vehicular network on a highway, or a military sensor network which is deployed with the given multi-hop structure, for example for better power efficiency, or with respect to a chain of command. Such multi-hop wireless networks have been studied extensively in the absence of secrecy constraints, see [14] for example. We expect that there is a need for multi-hop secure transmission in the future especially when it is not energy efficient to perform one-hop transmission. That said, we stress that the results provided in this paper is of theoretical nature, worked on a highly idealized system model presenting theoretical achievability.

The line network model is a departure from the three node relay channel that enjoys a direct link [15], [16], and is a generalization of the two-hop model (with one intermediate untrusted relay) considered in [17]–[19]. However, it is easy to see that the relaying scheme utilized in these references, in particular, compress-and-forward, does not lead to non-vanishing secrecy rate with growing number of hops. Instead, we shall follow a compute-and-forward type strategy [20], [21], which, along with the use of nested lattice codes [22], judicious use of structured interference, and a carefully designed transmission protocol, yields the scalable secrecy rate. In computing the secrecy rate, we shall utilize and build upon the recently established framework of equivocation computation with nested lattice codes [23]. As the main result, in this paper, we provide the first end-to-end secure communication guarantee for a network that has an arbitrary number of hops each of which has to be facilitated by a node that is also an eavesdropper.

The remainder of the paper is organized as follows: In section II, we describe the system model. Section III describes some results on lattice codes that are useful for establishing the main result of this work. Section IV states the main result. Section V, VI and VII describe the details of the transmission strategy. Section VIII describes the secrecy rate calculation. Section IX concludes the paper.

II. System Model

The system model is shown in Figure 1. The network is composed of K nodes on a line. The source and the destination

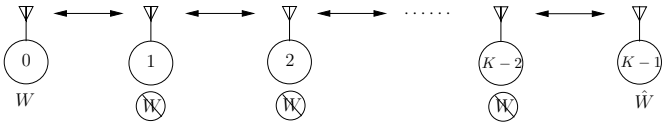


Fig. 1. A line network composed of K nodes. Node 0 is the source, node $K-1$ is the destination. Nodes $1, ..., K-2$ are *untrusted* relays who help forward the message, but are prevented from being able to decode it.

are labeled by 0 and $K-1$ respectively. The relay nodes are labeled by $1, ..., K-2$. We assume that, while these nodes participate in forwarding signals, any or all of them are simply nodes of lower security clearance, and cannot be trusted with the message. Thus, the message W that the source wishes to send to the destination must be kept secret from all of these relay nodes.

Each node is half-duplex, i.e., can either receive or transmit at a time, but not both. Each node can receive signals from its two nearest neighbors[3]. In addition, without loss of generality, we normalize the channel gain from each node to its nearest neighbors to unity. That is, we use transmission power control and combine the effect of the channel gain into the received power constraint. The channel gain from node i to node j is denoted by $h_{i,j}$, $i \neq j, 0 \leq i, j \leq K-1$

$$h_{i,j} = \begin{cases} 1, |i-j| = 1 \\ 0, \text{otherwise.} \end{cases} \tag{1}$$

Let X_i and Y_i be the transmitted and received signal of the ith relay node respectively, $0 \leq i \leq K-1$. Then, we have

$$Y_0 = h_{1,0}X_1 + Z_0 \tag{2}$$

$$Y_i = h_{i-1,i}X_{i-1} + h_{i,i+1}X_{i+1} + Z_i, \quad i = 1, ..., K-2 \tag{3}$$

$$Y_{K-1} = h_{K-2,K-1}X_{K-2} + Z_{K-1} \tag{4}$$

where Z_is are independent, zero-mean Gaussian random variables with unit variance.

Let n be the total number of channel uses. Let $X_{i,k}$ be the signal transmitted by node i during the kth channel use. We assume that the average power constraint of each node is $\bar{P}$:

$$\frac{1}{n}\sum_{k=1}^{n} E\left[X_{i,k}^2\right] \leq \bar{P}. \tag{5}$$

Let $\hat{W}$ be the estimate of W at the destination. For reliable communication [24], we require

$$\lim_{n\to\infty} \Pr\left(W \neq \hat{W}\right) = 0. \tag{6}$$

Let I_i denote all information available to the ith node. Since any or all of the relay nodes are untrusted, W should not be leaked to any of them. This means that we require

$$\lim_{n\to\infty} \frac{1}{n} H\left(W|I_i\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W\right), i = 1, ..., K-2. \tag{7}$$

where $H(X)$ denotes Shannon entropy of the random variable X [24]. The performance metric we will concentrate on is *secrecy rate*, i.e., the communication rate that is reliable

[2]The secrecy capacity of a wireless network of arbitrary topology, just like its counterpart without secrecy constraints, is a challenging open problem.

[3]The source and the destination receive only from their right and left neighboring node respectively.

TABLE I
SUMMARY OF NOTATIONS

Λ	lattice in $\mathcal{R}^N$
$\mathcal{V}(\Lambda)$	the fundamental region of a lattice
$x^N \bmod \Lambda$	modulus operation (9)
(Λ_f, Λ_c)	nested lattice pair, $\Lambda_c \subset \Lambda_f$
$\Lambda_f \cap \mathcal{V}(\Lambda_c)$	nested lattice codebook
t^N	a lattice point
$t_1^N \oplus t_2^N$	$(t_1^N + t_2^N) \bmod \Lambda_c$
d^N	dithering vector
R_L	rate of the lattice codebook
P_L	average power of the lattice codebook
T	the $N \log_2 K$ bit information that can recover the real sum from the modulus sum of K lattice points. See Theorem 3.

and secure, denoted by R_s and is defined as

$$R_s = \lim_{n\to\infty} \frac{1}{n} H(W) \tag{8}$$

such that both (6) and (7) hold.

Remark 1: The use of unit channel gains per Equation (1) is for clarity of exposition. The achievable scheme in Section VI is applicable for any $h_{i,j}$ when $|i-j| = 1$. When the channel gains are not unity, all each node needs to do is to properly scale its transmit power, i.e., employ transmit power control. In particular, the achievability scheme requires the received power from neighboring hops to be equal which can be satisfied by scaling X_{i-1} and X_{i+1}, for all i. □

III. PRELIMINARIES

In this section, we provide the definitions and results which will be useful in the sequel. The notation used is summarized in Table I for the reader's convenience.

We denote the dimensionality of the vectors with subscripts, i.e., x^N denotes the N-dimensional vector x. Let Λ denote a lattice in $\mathcal{R}^N$ [22], i.e., a set of points which is a group closed with respect to real vector addition. The modulo operation $x^N \bmod \Lambda$ is defined as

$$x^N \bmod \Lambda = x^N - \arg\min_{y^N \in \Lambda} d(x^N, y^N) \tag{9}$$

where $d(x^N, y^N)$ is the Euclidean distance between x^N and y^N. The fundamental region of a lattice Λ is denoted by $\mathcal{V}(\Lambda)$ and is defined as

$$\mathcal{V}(\Lambda) = \{x^N : x^N \bmod \Lambda = x^N\}. \tag{10}$$

Consider two lattices: a fine lattice Λ_f and a coarse lattice Λ_c such that $\Lambda_c \subset \Lambda_f$. The codebook of a nested lattice code, denoted by (Λ_f, Λ_c), is composed of all lattice points in the set $\Lambda_f \cap \mathcal{V}(\Lambda_c)$ [22]. Let t^N be a lattice point in the nested lattice codebook. Let d_i^N denote the dithering vector used in error probability analysis of lattice decoders [22]. A lattice decoder computes the point in the fine lattice that is closest to the received signal in terms of Euclidean distance. The transmitted signal over N channel uses, X^N is related to t^N as follows:

$$X^N = (t^N + d^N) \bmod \Lambda_c. \tag{11}$$

Let $|A|$ be the cardinality of the set A. The rate of the nested lattice codebook, R_L, is given by

$$R_L = \frac{1}{N} \log_2 |\Lambda_f \cap \mathcal{V}(\Lambda_c)|. \tag{12}$$

Let $t_i^N, i = 1, 2$ be two independent lattice points taken from the same lattice codebook $\Lambda_f \cap \mathcal{V}(\Lambda_c)$. Let $d_i^N, i = 1, 2$ be the corresponding dithering vectors. Let

$$X_i^N = (t_i^N + d_i^N) \bmod \Lambda_c. \tag{13}$$

Let $\left\|X_i^N\right\|$ be the Euclidean norm of vector X_i^N. Let P_L be the average power of X_i^N when $N \to \infty$. We rely on the following result from [25] to meet the reliability requirement given by (6). Suppose that a receiver, given $X_1^N + X_2^N$, wishes to decode $(t_1^N + t_2^N) \bmod \Lambda_c$. Suppose further that the receiver knows d_1^N, d_2^N. Let $\hat{t}^N$ be its decoder output. Then, we have:

Theorem 1: [25] For any positive R_L, such that

$$R_L < \frac{1}{2} \log_2 (\frac{1}{2} + P_L) \tag{14}$$

and for each N, there exists a pair of nested lattice Λ_f, Λ_c, such that

$$\lim_{N\to\infty} -\frac{1}{N} \log_2 \Pr\left(\left(t_1^N + t_2^N\right) \bmod \Lambda_c \neq \hat{t}^N\right) > 0. \tag{15}$$

The nested lattice code offers a natural algebraic structure, which we will utilize to satisfy the secrecy requirement given by (7). First, it can be verified that $\Lambda_f \cap \mathcal{V}(\Lambda_c)$ forms a finite abelian group with the addition operation defined by $(x^N + y^N) \bmod \Lambda_c$ for $x^N, y^N \in \Lambda_f \cap \mathcal{V}(\Lambda_c)$. For a finite abelian group, the following lemma holds:

Lemma 1: [26] Let t_A, t_B be two independent random variables distributed over a compact abelian group, t_B has a uniform distribution, then $t_A \oplus t_B$ is independent from t_A. Here $\oplus$ is the addition over the group.

In the sequel, we shall use $t_1^N \oplus t_2^N$ to denote $(t_1^N + t_2^N) \bmod \Lambda_c$. The lemma implies that $t_1^N \oplus t_2^N$ is independent from t_1^N, if t_2^N is uniformly distributed over $\Lambda_f \cap \mathcal{V}(\Lambda_c)$ and is independent from t_1^N. This was utilized in [26] for the modulus channel. On the other hand, if the addition is not defined over the group, the lemma no longer holds.

IV. MAIN RESULT

In this section, we state the main result of this work:

Theorem 2: Define $C(\gamma)$ as $C(\gamma) = \frac{1}{2}\log_2(1+\gamma)$. For any $\varepsilon > 0$, a secrecy rate of *at least*

$$R_s = 0.5(C(2\bar{P} - 0.5) - 1) - \varepsilon \tag{16}$$

bits per channel use is achievable regardless of the number of hops.

Proof: The proof of Theorem 2 is provided in Section VIII-B. ■

Remark 2: As shown by Theorem 2, the achievable secrecy rate is not a function of the number of nodes in the line network. □

Remark 3: When there is no secrecy constraint, an achievable rate is $0.5C(2\bar{P} - 0.5)$ [25]. Hence only 0.5 bit per channel use is lost due to the presence of the eavesdropper. This is a remarkably different conclusion than that in [10]

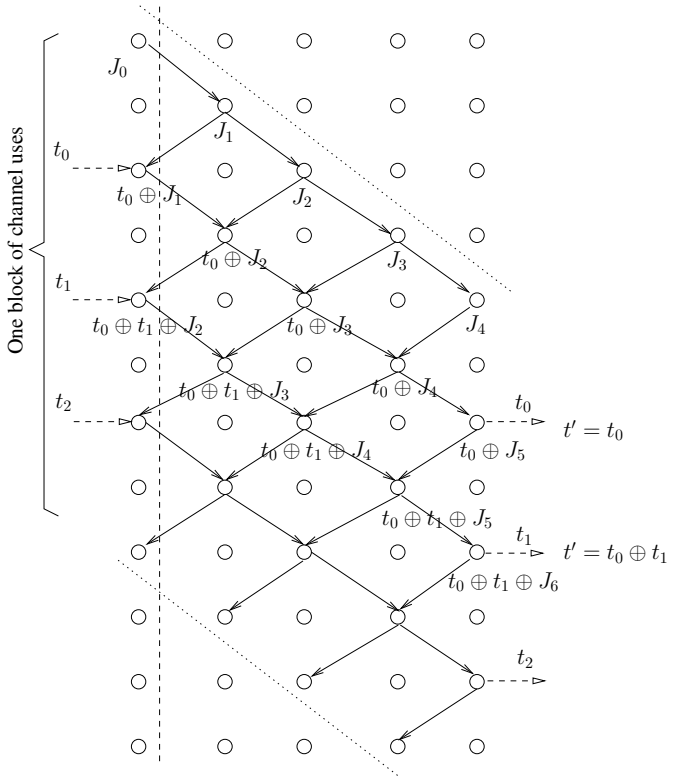


Fig. 2. One block of channel uses in the proposed transmission scheme. The labels denote the transmitted lattice points calculated according to the inner code summarized in Table II. For clarity, the superscript ^{N} is omitted. $\oplus$ denotes the modulus sum operation over the lattice codebook.

TABLE II
TRANSMISSION STRATEGY OF THE INNER CODE IN A BLOCK

Node Type	First Phase	Other Phases
Source	J^N	$t^N \oplus J^N$
Relay	J^N	$\hat{t}^N \oplus (-x'^N)$
Destination	J^N	$t'^N \oplus J^N$

Notation	Meaning
$\hat{t}^N$	the lattice point decoded by the relay in the previous phase.
x'^N	the previous lattice point transmitted by the relay.
t'^N	the modulus sum of source-transmitted t^Ns that has been recovered by the destination up to this phase in this block.
J^N	a random lattice point

where the loss is proportional to the capacity of a single edge of the network. We obtain this result by benefiting from having interference in this network and utilizing it to provide secrecy. □

Remark 4: Without the secrecy constraints, the achievable rate offered by lattice codes is within 0.5 bits/channel use of the channel capacity [25]. The secrecy rate derived in this work is within 0.5 bits/channel use of the rate in [25], and thus is *at most* 1 bit/channel use away from the channel capacity. □

V. OVERVIEW OF THE CODING SCHEME

In this section, we describe the coding scheme. To do so, we begin with an alternative representation of the network, as shown in Figure 2. In this representation, each column of nodes corresponds to a single node in the line network. Each row corresponds to a phase. A phase is composed of N channel uses, which will be used to transmit a lattice point, i.e., the signal X^N given by (11). A node in a row has an outgoing edge if it transmits during this phase. The node in that row has an incoming edge if it receives signals during the previous phase. Since we assume all nodes are half duplex, a node can not transmit and receive simultaneously in the same phase. Therefore, each edge always connects nodes from different columns in this representation. For clarity, the details of the underlying communication channel are omitted from the figure. For example, it is understood, though not explicitly shown in Figure 2, that the signal received by the node is a superposition of the signals over all incoming edges corrupted by the additive Gaussian noise.

A number of consecutive phases are collectively called one *block*. As shown in Figure 2, a block starts at different phases for different nodes. As a rule, a block always starts one phase later at a node compared to its left neighbor. The boundary of a block is depicted by the dotted line in Figure 2. The communication will span over a number of blocks.

The main idea behind the achievability scheme is simple. We utilize the fact that the network has interference, and purposefully, and in a structured way, create interference for each relay node from its next hop neighbor while it simultaneously receives the signal containing the confidential message from its previous hop neighbor. Each relay is able to remove the channel noise from its received signal, which alleviates the degradation in rate due to noise accumulation over the hops, but cannot separate the confidential message from the structured interference.

The coding scheme is composed of two parts: an inner code using nested lattices and an outer code which uses a stochastic encoder. Figure 3 is an example with only one relay node that illustrates this architecture. The encoder of the inner code takes inputs as sequence of lattice points and computes the lattice points to transmit in the next phase based on the rule in Section VI-A. The relay nodes and the destination node receives a superposition of the signals transmitted by its neighbor and decodes the modulus sum of the lattice points contained in the received signals. Each node then either forwards the decoded lattice points or transmits jamming signals according to the protocol in Section VI-B and Section VI-C.

The outer code is also essential to provide the stated secrecy rate. The signals received by each relay node is a superposition, i.e., real sum -*not* the modulo sum- of two N-dimensional vectors transmitted by its two neighbors. Thus, Lemma 1 does not hold and there will still be some information leaked to the relay node from the signals it receives. The outer code, which is a random binning scheme [5], is used to eliminate this leakage. This outer code, which we shall describe in Section VII, uses a stochastic encoder which provides sufficient randomness to confuse the eavesdropper. In the next two sections, we describe the details of the inner code and the outer code.

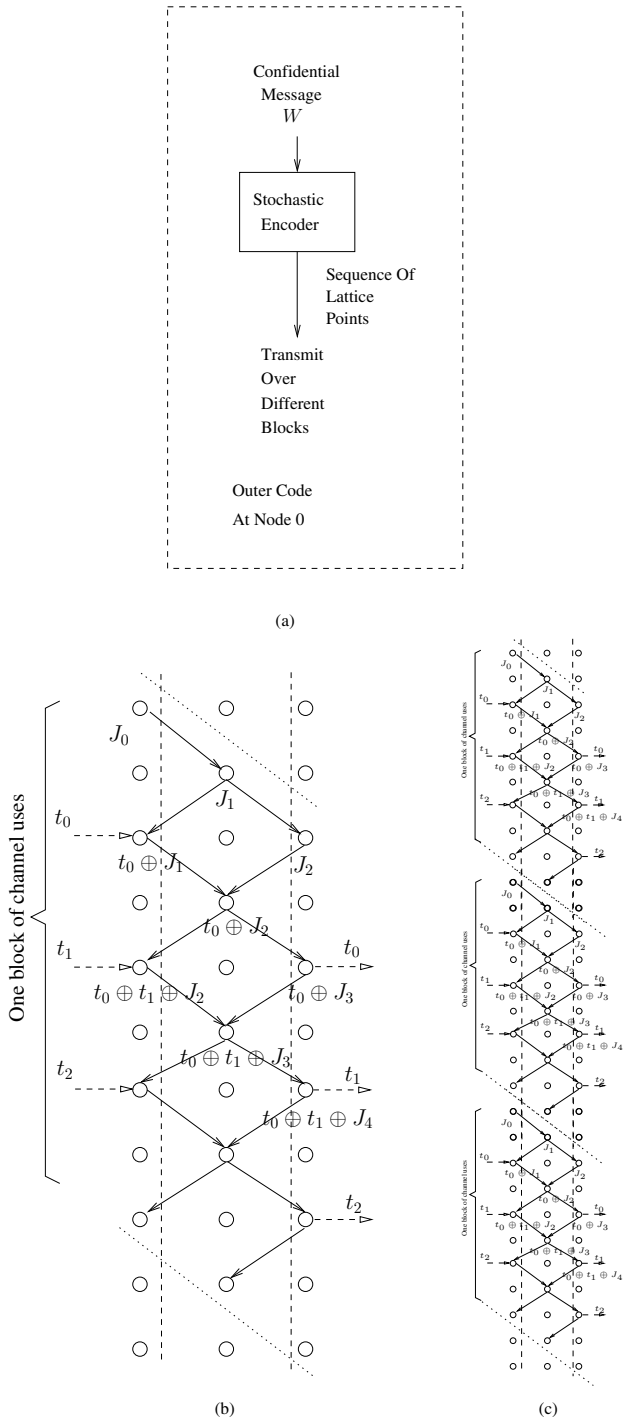


Fig. 3. Overview of the coding scheme. Assume we have only one relay node. (a) Outer code at node 0, which uses a stochastic encoder. Its output is encoded with the inner code and transmitted over multiple blocks. (b) One block of channel use. (c) Multiple blocks of channel use. The label denotes the lattice points transmitted by each node. t_i, J_i are lattice points. $\oplus$ denotes the modulus sum operation over the lattice codebook.

VI. Inner Code

In this section, we describe the inner code, which includes physical layer network coding, structured interference, and careful scheduling of transmissions. The coding scheme is summarized in Table II.

A. The Source Node

In each phase, the signals transmitted by the source node takes the form:

$$t^N \oplus J^N \oplus d^N \tag{17}$$

where d^N is the dithering vector, t^N and J^N are lattice points from the nested lattice codebook. t^N and J^N are determined as follows:

1) In the first phase within a block during which the source node transmits, $t^N = 0$. J^N is chosen randomly from the nested lattice codebook according to a uniform distribution.

2) Otherwise, t^N is chosen by an stochastic encoder, which will be described in Section VII. J^N is chosen to be the output of the lattice decoder [22] whose inputs are the signals received by the source node during the previous phase.

B. The Relay Node

Within each phase, the relay node labeled by k in Figure 1 transmits signals in the form of

$$t_k^N \oplus d_k^N, \quad k = 2, ..., K-1 \tag{18}$$

where d_k^N is the dithering vector. t_k^N is a lattice point chosen as follows:

1) If this is the first phase the relay transmits during this block, then t_k^N is drawn from a uniform distribution over the nested lattice codebook. This t_k^N does not convey any information, but is transmitted with the sole aim of jamming the neighboring eavesdropper (relay).

2) Otherwise, t_k^N depends on the signal the relay receives during the previous phase, as we will explain shortly, and is expressed in (19).

The signals received by the relay within a block can be categorized into the following three cases. Let z^N denote the Gaussian channel noise. Let t_A^N, t_B^N denote lattice points, and d_A^N, d_B^N denote the dithering vectors.

1) If this is the first phase during which the relay receives signals during this block, then the received signal takes the form $(t_A^N \oplus d_A^N) + z^N$. It only contains interference from its left neighbor. This is because, as noted earlier, a block starts one phase earlier at a node compared to its right.

2) Similarly, if this is the last phase the relay receives signals during this block, then the received signal takes the form $(t_B^N \oplus d_B^N) + z^N$. It only contains interference from its right neighbor, since a block ends one phase earlier at a node compared to the node to its right. In this case, the block terminates and the relay does not transmit signals in the ensuing phases until a new block starts.

3) Otherwise the signals received by the relay take the form $y_k^N = (t_A^N \oplus d_A^N) + (t_B^N \oplus d_B^N) + z^N$, which contains the superposition of signals from its left and right neighbors.

We next explain how the relay computes t_k^N in (18) in ensuing phases within a block.

Observe that, the signals received by the relay falls into the category of case 3) described above. Since the rate of the nested lattice codebook is chosen according to (14) in Theorem 1, for case 3), the relay, with the knowledge of d_A^N, d_B^N, will be able to decode $t_A^N \oplus t_B^N$ reliably using the

lattice decoder in [25]. We use $\hat{t}^N$ to denote the decoder output.

Let the signal transmitted by the relay node during the previous phase be $x'^N \oplus d_k'^N$, where x'^N is a point from the nested lattice code book and $d_k'^N$ be the dithering vector. Then t_k^N in (18) is computed as follows:

$$t_k^N = \hat{t}^N \oplus (-x'^N). \tag{19}$$

Here $-$ is the inverse operation defined over the abelian group $\mathcal{V}(\Lambda_c) \cap \Lambda_f$.

C. The Destination

1) Transmitter: The destination can be viewed as a relay node without a neighbor to its right hence it must simulate its effect when computing its transmitted signals. The signals it transmitted still takes the form (18). Like a relay node, the destination transmits a random lattice point during the first phase in a block. In the ensuing phase, one by one, the destination recovers t^N in (17) as described in the next section: Section VI-C2. Let t'^N be the modulus sum of the t^Ns it has recovered so far in this block. Then the lattice point transmitted by the destination is given by:

$$t'^N \oplus J^N \tag{20}$$

where J^N is a lattice point randomly chosen from the lattice codebook according to a uniform distribution. It can be verified from Figure 2 that this is the lattice point the destination would transmit if it had a neighbor to its right.

2) Decoder: The decoder at the destination wishes to recover t^N in (17), i.e., the lattice point transmitted by the source node.

Since the destination node does not have a right neighbor, the signals it receives during one phase, i.e., N channel uses, always take the form

$$Y^N = (t_A^N \oplus d_A^N) + z^N \tag{21}$$

where $t_A^N \in \Lambda_f$, d_A^N is the dithering vector and z^N is the channel noise. The decoder then obtains the output $\hat{t}^N$ using the lattice decoder in [25].

The decoder at the destination starts producing outputs at the end of the second phase in a block, in a way similar to the relay node: Let the signal transmitted by the destination node during the previous phase be $x'^N \oplus d_k'^N$, where x'^N is a point from the nested lattice code book and $d_k'^N$ be the dithering vector. Then the decoder outputs:

$$\hat{t}^N \oplus (-x'^N) \tag{22}$$

By this operation, the destination subtracts the interference caused by itself to their left neighbor. Hence the only remaining lattice point observable from the output of the decoder at the destination is the one transmitted by the source node, which, with the rate chosen, the destination is able to decode reliably.

VII. Outer Code

The stochastic encoder of the outer code uses a random binning scheme proposed in [5]: Let Q denote the number of nested lattice points transmitted in a block. Then, the codebook used by the encoder is composed of independent and identically distributed (i.i.d.) sequences whose components are sampled from a uniform distribution by a Q-fold Cartesian product of the nested lattice codes. These sequences are then randomly binned into bins of equal size. The size of the bin is determined by the entropy of the secret message conditioned on the observation of the eavesdropper, i.e., the *equivocation* [5], which we shall compute in Section VIII. The encoder determines which bin to use based on the value of the secret message, and outputs a codeword randomly chosen from that bin, which, in this work, corresponds to a sequence of lattice points. These lattice points then form t^N in (17), that is used to compute the signals transmitted by the source node in different phases.

As shown in Section VI-C2, at the destination, with high probability, the decoder can recover this sequence of lattice points, i.e., the codeword in the wiretap codebook transmitted by the source node. The destination then produces the value of the message corresponds to the bin that contains the codeword in the wiretap codebook, which equals the confidential message transmitted by the source node.

We next compute the equivocation, and prove the secrecy rate claimed in Theorem 2.

VIII. Secrecy Rate

A. Supporting Results

We have seen that Lemma 1 is not sufficient to guarantee secrecy since the signals received by the relay node is not modulus sum of lattice points transmitted by its neighbors.

To overcome this difficulty, we use the following representation theorem from [23] and "genie bound" from [27].

Theorem 3: [23] Let $u_1^N, u_2^N, ..., u_K^N$ be K vectors taken from $\mathcal{V}(\Lambda_c)$. There exists an integer T, such that $1 \leq T \leq K^N$, and $\sum_{k=1}^{K} u_k^N$ is uniquely determined by $\{T, \sum_{k=1}^{K} u_k^N \bmod \Lambda_c\}$.

Lemma 2: [27] For random variables A and B, and discrete random variable T, we have $H(A|B,T) \geq H(A|B) - H(T)$.

Let X_1^N, X_2^N be defined as in (13). Using Lemma 2 and Theorem 3, when eavesdropper observes $X_1^N + X_2^N$ and has side information d_1^N, d_2^N, we can write [23]:

$$\begin{aligned}
&H\left(t_1^N | X_1^N + X_2^N, d_1^N, d_2^N\right) && (23)\\
=&H\left(t_1^N | \left(X_1^N + X_2^N\right) \bmod \Lambda_c, T, d_1^N, d_2^N\right) && (24)\\
=&H\left(t_1^N | \left(t_1^N + t_2^N\right) \bmod \Lambda_c, T, d_1^N, d_2^N\right) && (25)\\
\geq&H\left(t_1^N | \left(t_1^N + t_2^N\right) \bmod \Lambda_c, d_1^N, d_2^N\right) - H(T) && (26)\\
=&H\left(t_1^N\right) - H(T) \geq H\left(t_1^N\right) - N && (27)
\end{aligned}$$

In (25), we use Theorem 3 for $K = 2$. In (26), we apply Lemma 2. In (27) we use Lemma 1. From (23)-(27), it follows that

$$\lim_{N\to\infty} \frac{1}{N} I\left(t_1^N; X_1^N + X_2^N, d_1^N, d_2^N\right) \leq 1 \tag{28}$$

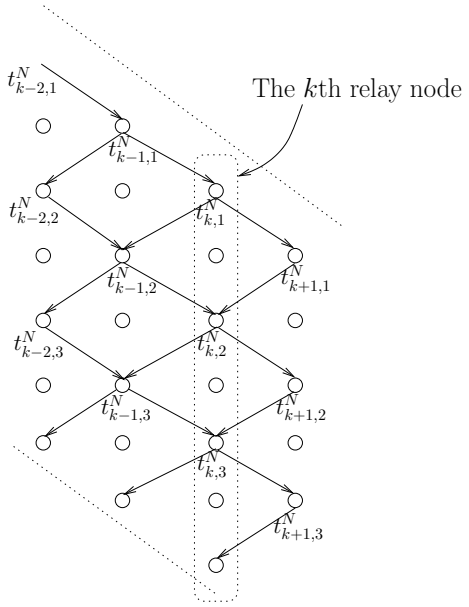


Fig. 4. Notations for lattice points transmitted over different edges. The number of lattice points sent by the wiretap encoder within a block, $Q = 2$.

This means that the information leaked to the eavesdropper regarding the value of t_1^N cannot exceed 1 bit per channel use [23], which can be eliminated using the stochastic encoder described in Section VII.

As we shall see in Section VIII-B, since the message is transmitted over multiple hops and the network has cycles, the eavesdropper at a certain relay node may receive more than one set of signals with the form $X_1^N + X_2^N$ and the final expression we shall use to compute the secrecy rate will be more complicated than given in (23). However, as we shall see shortly, the steps we use to compute the secrecy rate are similar to (23)-(27).

B. Secrecy Rate Calculation

Given that there are Q lattice points from the wiretap encoder sent out during a block, we observe, from Section VI-A, that the source transmits during $Q+1$ phases within a block. Each relay node receives signals during $Q+2$ phases within the block. The one additional phase is caused by transmission from its right neighbor, where a block terminates one phase later. Then each relay node has the following side information regarding the source input within one block:
i) the signals received during $Q+2$ phases.
ii) the dithering vectors $\{d_{k,i}\}$ for the kth node and the ith phases, $k = 0, ..., K-1$, $i = 1...Q+2$.
iii) the signals transmitted from the relay node during this block. Note that only signals it transmitted during the first phase may provide information because all subsequent transmitted signals are computed from signals received in the phases before them and the corresponding dithering vectors.

Recall that W is the secret message. Assume that the transmission spans over M blocks. Let $t_{k,i}^N$ and $d_{k,i}^N$ be the lattice point and dithering vector respectively used by the kth node's transmitter during the ith phase. Similarly, Let $t_{k,i}^{NM}$ and $d_{k,i}^{NM}$ be these signals used by the kth node during the ith phase in each block of the M blocks. The superscript shows the dimension of each signal. Then for the kth relay node, the equivocation can be written as:

$$\begin{aligned}\mathcal{H}_k = \frac{1}{NM} H(W | & t_{k,1}^{NM} \oplus d_{k,1}^{NM} + z_1^{NM}, d_{k,1}^{NM}, \\ & t_{k-1,i}^{NM} \oplus d_{k-1,i}^{NM} + t_{k+1,i-1}^{NM} \oplus d_{k+1,i-1}^{NM} + z_i^{NM}, \\ & d_{k-1,i}^{NM}, d_{k+1,i-1}^{NM}, i = 2, ..., Q+1, \\ & t_{k+1,Q+1}^{NM} \oplus d_{k+1,Q+1}^{NM} + z_{Q+2}^{NM}, d_{k+1,Q+1}^{NM}, \\ & t_{k,1}^{NM}, d_{k,1}^{NM}) \end{aligned} \tag{29}$$

where on the condition term of the entropy expression, the first line represents the signals received during the first phase in M blocks and the corresponding dithering vector. The second line represents these signals received during phases $2, ..., Q+1$. The third line is for phase $Q+2$. The last line is the lattice point transmitted by the kth relay node in the first phase and the corresponding dithering vectors. These terms are demonstrated in Figure 4 for $Q = 2$ for the reader's convenience. The value of $t_{k,i}^N$ depends on the outputs of the lattice decoder and hence is subject to channel noise. $t_{k,i}^N$ is *in error* if it deviates from the correct value observed when the same network coding scheme is used in a noiseless line network. Then we can define the block error probability $\bar{P}_e$ as

$$\begin{aligned}\Pr(\exists i \in \{2, ..., Q+1\}, & \\ \text{s.t. } t_{k-1,i}^N & \text{ is in error, or } t_{k+1,i-1}^N \text{ is in error,} \\ \text{or } t_{k+1,Q+1}^N & \text{ is in error.)} \end{aligned} \tag{30}$$

The lattice decoder of the kth node is in error if its output does not equal the $\oplus$-sum of the lattice points in its incoming edges. Then we can define $P_e(k,i)$ as the probability of decoding error of the lattice decoder from [25] used by the kth node during ith phase. With these definitions, $\bar{P}_e$ is related to $P_e(i,k)$ as

$$\bar{P}_e \leq 1 - \prod_{k,i} (1 - P_e(k,i)) \tag{31}$$

where the subscript in the product includes the indices of all the relay nodes and the indices of all the phases within one block. According to [25] and stated in Theorem 1, $P_e(k,i)$ decreases to 0 exponentially fast with respect to N. Hence for any given block that spans over $Q+2$ phases, we have $\lim_{N\to\infty} \bar{P}_e = 0$.

We define the *error-free equivocation* as

$$\begin{aligned}\bar{\mathcal{H}}_k = \frac{1}{NM} H(W | & t_{k,1}^{NM} \oplus d_{k,1}^{NM} + z_1^{NM}, d_{k,1}^{NM}, \\ & \bar{t}_{k-1,i}^{NM} \oplus d_{k-1,i}^{NM} + \bar{t}_{k+1,i-1}^{NM} \oplus d_{k+1,i-1}^{NM} + z_i^{NM}, \\ & d_{k-1,i}^{NM}, d_{k+1,i-1}^{NM}, i = 2, ..., Q+1, \\ & \bar{t}_{k+1,Q+1}^{NM} \oplus d_{k+1,Q+1}^{NM} + z_{Q+2}^{NM}, d_{k+1,Q+1}^{NM}, \\ & t_{k,1}^{NM}, d_{k,1}^{NM}) \end{aligned} \tag{32}$$

where $\bar{t}_{k,i}^{NM}$ corresponds to the value of $t_{k,i}^{NM}$ in a noise-free network. Then we have the following lemma:

Lemma 3: For a given Q,

$$\bar{\mathcal{H}}_k + \varepsilon_2 \geq \mathcal{H}_k \geq \bar{\mathcal{H}}_k - \varepsilon_1 \tag{33}$$

where $\varepsilon_i, i = 1, 2$ go to 0 as $N, M \to \infty$.

Proof: The proof is provided in Appendix A. ■

Remark 5: The proof of Lemma 3 uses the condition that the error probability of all the lattice decoders decreases exponentially fast with respect to the lattice dimension N. If this condition holds, Lemma 3 claims that if a particular equivocation value is achievable for the kth relay node with all the other nodes producing the correct values as observed in a noise-free line network, then the same equivocation value is achievable in a Gaussian noisy line network.□

Lemma 4: $\bar{\mathcal{H}}_k$ is the same for all relay nodes.

Proof: The proof is provided in Appendix B. ■

With this lemma, we can drop the subscript k and write $\bar{\mathcal{H}}_k$ as $\bar{\mathcal{H}}$. After these preparations, we are now ready to compute the secrecy rate.

Proof of Theorem 2: According to Lemma 3 and Lemma 4, it is sufficient to compute $\bar{\mathcal{H}}_k$ for one relay node. We focus on one block of channel uses as shown in Figure 4. Let $V(j)$ to denote the condition term in $\bar{\mathcal{H}}_k$. We start by lower bounding $H(t_0^{NQ}|V(j))$, where t_0^{NQ} are the lattice points transmitted by the source node as described in Section VI-A within this block. Then $H(t_0^{NQ}|V(j))$ can be written as:

$$\begin{aligned} H(t_0^{NQ}|V(j)) = H(t_0^{NQ}|&(\bar{t}_{k-1,i}^N \oplus d_{k-1,i}^N)+ \\ &(\bar{t}_{k+1,i-1}^N \oplus d_{k+1,i-1}^N) + z_i^N, \\ d_{k-1,i}^N, d_{k+1,i-1}^N, &i = 2, ..., Q+1, t_{k,1}^N, d_{k,1}^N) \end{aligned} \quad (34)$$

Comparing (34) with the condition terms in (32), we see that we have removed the signals received during the first and the last phase within a block from the condition terms. This is because these signals are independent from all the other signals on the condition terms and t_0^{NQ}:

1) The lattice point contained in the signals received during the last phase is given in (74). It is randomly chosen by the left neighbor of the relay node which is ignored by the relay node and hence never propagates to its right neighbor.

2) The lattice point contained in the signals received during the last phase is given in (75). Note that it includes a fresh lattice point J_{k+Q}^N, which has never been observed by the relay node before in its previous phases. The independence from the other terms hence follows from Lemma 1.

We then assume that there is a genie which reveals the channel noise z^N to the eavesdropper residing at the relay node. This means that (34) can be lower bounded by:

$$\begin{aligned} H(t_0^{NQ}|&(\bar{t}_{k-1,i}^N \oplus d_{k-1,i}^N)+ \\ &(\bar{t}_{k+1,i-1}^N \oplus d_{k+1,i-1}^N), d_{k-1,i}^N, d_{k+1,i-1}^N, \\ &i = 2, ..., Q+1, t_{k,1}^N, d_{k,1}^N) \end{aligned} \quad (35)$$

Next, we reuse the steps described earlier in (23)-(27). We first use Theorem 3 and lower bound (35) as:

$$\begin{aligned} H(t_0^{NQ}|&\bar{t}_{k-1,i}^N \oplus d_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N \oplus d_{k+1,i-1}^N, T_i, \\ &d_{k-1,i}^N, d_{k+1,i-1}^N, i = 2, ..., Q+1, t_{k,1}^N, d_{k,1}^N) \end{aligned} \quad (36)$$

where T_i is the integer in Theorem 3 and can be represented with N bits. We then apply the genie lower bound in Lemma 2 to (36) and find that it is lower bounded by:

$$\begin{aligned} &H(t_0^{NQ}|\bar{t}_{k-1,i}^N \oplus d_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N \oplus d_{k+1,i-1}^N, \\ &\quad d_{k-1,i}^N, d_{k+1,i-1}^N, i = 2, ..., Q+1, t_{k,1}^N, d_{k,1}^N) \\ &\quad - H(T_i, i = 2, ..., Q+1) \end{aligned} \quad (37)$$

$$\begin{aligned} =&H(t_0^{NQ}|\bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., Q+1, t_{k,1}^N) \\ &- H(T_i, i = 2, ..., Q+1) \end{aligned} \quad (38)$$

For the first term in (38), we have

$$H(t_0^{NQ}|\bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., Q+1, t_{k,1}^N) = H(t_0^{NQ}) \quad (39)$$

This is because, as shown in (74)-(75), $\bar{t}_{k+1,i-1}^N$ contains J_{k+i-1}^N, which is a new lattice point not contained in previous $\bar{t}_{k-1,j}^N$ or $\bar{t}_{k+1,j-1}^N$, $2 \le j < i$. Hence $\bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N$ can be expressed as $U_i^N \oplus J_{k+i-1}^N$, where $U_i^N = \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N \oplus (-J_{k+i-1}^N)$ is independent from J_{k+i-1}^N. Then, we have

$$I\left(t_0^{NQ}; \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., Q+1, t_{k,1}^N\right) \quad (40)$$

$$= \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(t_0^{NQ}; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \quad (41)$$

$$\le \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(t_0^{NQ}, U_j^N; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \quad (42)$$

$$= \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(t_0^{NQ}; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad U_j^N, \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \\ +I(U_j^N; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \quad (43)$$

$$= \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(t_0^{NQ}; J_{k+j-1}^N | \\ \quad U_j^N, \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \\ +I(U_j^N; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \quad (44)$$

$$\begin{aligned} &= \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(U_j^N; \bar{t}_{k-1,j}^N \oplus \bar{t}_{k+1,j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \\ &= \sum_{j=2}^{Q+1} \left\{ \begin{array}{l} I(U_j^N; U_j^N \oplus J_{k+j-1}^N | \\ \quad \bar{t}_{k-1,i}^N \oplus \bar{t}_{k+1,i-1}^N, i = 2, ..., j-1, t_{k,1}^N) \end{array} \right\} \\ &\le \sum_{j=2}^{Q+1} I\left(U_j^N; U_j^N \oplus J_{k+j-1}^N\right) = 0 \end{aligned} \quad (45)$$

The first term in (44) is 0 because J_{k+j-1}^N is independent from everything else in that term. (45) follows from Lemma 1.

Applying (39) to (38), we find that (38) equals $H(t_0^{NQ}) - H(T_i, i = 2, ..., Q+1)$. Hence we have proved

$$I(t_0^{NQ}; V(j)) \le H(T_i, i = 2, ..., Q+1) \quad (46)$$

By Theorem 3, T_i can take at most 2^N values. Hence $H(T_i, i = 2, ..., Q+1) < NQ$. Define

$$c = \frac{1}{NQ} I(t_0^{NQ}; V(j)) \quad (47)$$

Then from (46), we have $0 \le c \le 1$.

We next describe the wiretap encoder, which will perform coding across M blocks. The codebook is constructed as follows: The codebook contains $2^{\lfloor MNQR_L \rfloor}$ codewords. Each codeword is a length MQ sequence. Each component of the

sequence is an N-dimensional lattice point sampled in an i.i.d. fashion from the uniform distribution over the nested lattice codebook with rate R_L. The codebook is then randomly binned into several bins, each of which contains $2^{\lfloor MNQc \rfloor}$ codewords, with c given by (47).

Each block has $2(Q+1)$ phases, which equals $2(Q+1)N$ channel uses. We also use an additional phase to separate different blocks. Hence transmitting a codeword from a wiretap codebook takes $(2Q+3)NM$ channel uses. Therefore the rate of the codebook is given by:

$$\lim_{M\to\infty} \frac{1}{MNQ} H(W) = \frac{Q}{2Q+3}(R_L - c) \tag{48}$$

The transmitted codeword is chosen as described in Section VII. Let this codeword be u^{MNQ}. Let $V = \{V(j), j = 1...M\}$. Then, we have:

$$\begin{aligned}
\bar{\mathcal{H}} =& H(W|V) && (49)\\
=& H\left(W|u^{MNQ}, V\right) + H\left(u^{MNQ}|V\right) - H\left(u^{MNQ}|W, V\right) && (50)\\
\geq& H\left(u^{MNQ}|V\right) - MNQ\varepsilon && (51)\\
=& H\left(u^{MNQ}\right) - I\left(u^{MNQ}; V\right) - MNQ\varepsilon && (52)\\
\geq& H\left(u^{MNQ}\right) - \sum_{j=1}^{M} I\left(u^{MNQ}(j); V(j)\right) - MNQ\varepsilon && (53)\\
=& H\left(u^{MNQ}\right) - MNQc - MNQ\varepsilon && (54)
\end{aligned}$$

In (51), we use the fact that $H\left(u^{MNQ}|W,V\right) \leq MNQ\varepsilon$, where $\varepsilon > 0$ and $\lim_{M\to\infty}\varepsilon = 0$. This is because the size of the bin in the codebook is chosen according to the rate of information leaked to the eavesdropper. Hence given W, the bin index and V, with high probability the eavesdropper can determine the codeword that was transmitted. (51) follows from Fano's inequality. (53) is because, as explained in Section VII, if a block is viewed as one big channel use, the channel is memoryless.

Dividing (49) and (54) by MNQ and letting $M \to \infty$, we have

$$\lim_{M\to\infty} \frac{1}{MNQ}\bar{\mathcal{H}} = \lim_{M\to\infty} \frac{1}{MNQ} H(W) = \frac{Q}{2Q+3}(R_L - c) \tag{55}$$

Therefore a secrecy rate of $R_L - c$ bits per channel use is achieved. Then, according to Lemma 3, we can replace $\bar{\mathcal{H}}$ with $\mathcal{H}$ and write:

$$\begin{aligned}
\lim_{N,M\to\infty} \frac{1}{MNQ}\mathcal{H} &= \lim_{N,M\to\infty} \frac{1}{MNQ} H(W)\\
&= \frac{Q}{2Q+3}(R_L - c) && (56)
\end{aligned}$$

Next we use Theorem 1, which states R_L can be made arbitrarily close to $C(P - 0.5)$ as $N \to \infty$, where P is the average power per channel use to transmit a lattice point. For a given node, during $2Q+3$ phases, it only transmits in $Q+1$ phases. Hence we can choose R_L to be arbitrarily close to $\frac{Q}{2Q+3}(C(\frac{2Q+3}{Q+1}\bar{P} - 0.5))$. Taking the limit $Q \to \infty$, we find that a secrecy rate of $\max\{\frac{1}{2}(C(2\bar{P} - 0.5) - c), 0\}$ bits per channel use is achievable.

Finally, we can always set part of the bin index to be random bits. This is equivalent to increasing the size of the bin in the wiretap codebook. Since we know that minimum size of the bin is $2^{\lfloor MNQc \rfloor}$ codewords, where $0 \leq c \leq 1$, we can use a bin size of $2^{\lfloor MNQ \rfloor}$. The achievable secrecy rate then becomes $\max\{\frac{1}{2}(C(2\bar{P} - 0.5) - 1), 0\}$, which is the result claimed in Theorem 2. ∎

IX. Conclusion

In this work, we have considered a source destination pair which can communicate only over a chain of untrusted relay nodes, and showed that, information theoretically secure end-to-end communication is possible via a careful joint use of wiretap codes, lattice codes, and a network coding scheme. We have proved that this achievable secrecy rate is independent of the number of hops, and incurs only a modest penalty as compared to the case where no secrecy constraint is present. We conclude by noting that construction of channel codes for secure communication is needed for bringing these theoretical findings into practical communication networks.

Appendix A
Proof of Lemma 3

Let $c^j, \hat{c}^j$ denote the part of signals received by the kth relay node within the jth block excluding the first and the last phase. More specifically, this means:

$$\begin{aligned}
\hat{c}^j = \{&t^N_{k-1,i}(j) \oplus d^N_{k-1,i}(j) +\\
&t^N_{k+1,i-1}(j) \oplus d^N_{k+1,i-1}(j) + z^N_i(j), i = 2, ..., Q+1\}
\end{aligned} \tag{57}$$

$$\begin{aligned}
c^j = \{&\bar{t}^N_{k-1,i}(j) \oplus d^N_{k-1,i}(j) +\\
&\bar{t}^N_{k+1,i-1}(j) \oplus d^N_{k+1,i-1}(j) + z^N_i(j), i = 2, ..., Q+1\}
\end{aligned} \tag{58}$$

The signals received during the first phase of a block do not undergo any decoding operation and hence have the same expression in $\mathcal{H}_k$ and $\bar{\mathcal{H}}_k$. The signals received during the last block can be written as:

$$\hat{f}^j = (t^N_{k+1,Q+1}(j) \oplus d^N_{k+1,Q+1}(j)) + z^N_{Q+2}(j) \tag{59}$$

$$f^j = (\bar{t}^N_{k+1,Q+1}(j) \oplus d^N_{k+1,Q+1}(j)) + z^N_{Q+2}(j) \tag{60}$$

The block index (j) will be omitted in the following discussion for clarity.

We first prove that $c^j - \hat{c}^j$ is a discrete random variable with a finite support. According to (58), $c^j - \hat{c}^j$ has Q components. Each component can be expressed as

$$\begin{aligned}
&\left(\bar{t}^N_{k-1,i} \oplus d^N_{k-1,i}\right) - \left(t^N_{k-1,i} \oplus d^N_{k-1,i}\right)\\
&+ \left(\bar{t}^N_{k+1,i-1} \oplus d^N_{k+1,i-1}\right) - \left(t^N_{k+1,i-1} \oplus d^N_{k+1,i-1}\right)
\end{aligned} \tag{61}$$

For the two terms of (61) we have

$$\begin{aligned}
&\left(\bar{t}^N_{k-1,i} \oplus d^N_{k-1,i}\right) - \left(t^N_{k-1,i} \oplus d^N_{k-1,i}\right) && (62)\\
=&\bar{t}^N_{k-1,i} + d^N_{k-1,i} + x^N_1 - \left(t^N_{k-1,i} + d^N_{k-1,i} + x^N_2\right) && (63)\\
=&\bar{t}^N_{k-1,i} - t^N_{k-1,i} + x^N_1 - x^N_2 && (64)
\end{aligned}$$

where $x^N_1, x^N_2 \in \Lambda_c$. From Theorem 3, we notice that x^N_1 and x^N_2 each has at most 2^N possible solutions. $\bar{t}^N_{k-1,i}$ and $t^N_{k-1,i}$ each take $\|\mathcal{V}(\Lambda_c) \cap \Lambda_f\|$ possible values. Recall that R_L, as defined in (12), is the rate of the nested lattice codebook. Then (62) takes at most $2^{2N(R_L+1)}$ possible values.

Similarly, we can prove that the last two terms in (61) has at most $2^{2N(R_L+1)}$ possible values as well. Therefore $c^j - \hat{c}^j$ takes at most $2^{4NQ(R_L+1)}$ possible values. Therefore $H\left(c^j - \hat{c}^j\right) \leq 4NQ(R_L+1)$. Similarly, it can be shown that $f^j - \hat{f}^j$ takes at most $2^{2N(R_L+1)}$ values.

Define E^j as a binary random variable such that $E^j = 1$ if $c^j \neq \hat{c}^j$ or $f^j \neq \hat{f}^j$. Otherwise $E^j = 0$. Then $\Pr(E^j = 1)$ is the block error probability $\bar{P}_e$ defined in (30). Also, since $c^j - \hat{c}^j, f^j - \hat{f}^j$ takes at most $(4Q+2)N(R_L+1)$ different values, we have:

$$H(c^j - \hat{c}^j, f^j - \hat{f}^j | E^j = 1) \leq (4Q+2)N(R_L+1) \quad \forall j \tag{65}$$

Let $c = \{c^j\}$, $\hat{c} = \{\hat{c}^j\}$, $f = \{f^j\}$ and $\hat{f} = \{\hat{f}^j\}$, $j = 1, ..., M$. Let b denote the other conditioning terms that appears both in $\mathcal{H}_k$ and $\bar{\mathbf{H}}_k$. Then we have

$$\begin{aligned}
MN\mathcal{H}_k =& H(W|b, \hat{c}, \hat{f}) \geq H(W|b, c, \hat{c}, f, \hat{f}) && (66)\\
=& H(W|b, c, f, c - \hat{c}, f - \hat{f}) && (67)\\
=& H(W|b, c, f) + H(c - \hat{c}, f - \hat{f}|W, b, c, f)\\
& - H(c - \hat{c}, f - \hat{f}|b, c, f) && (68)\\
\geq& H(W|b, c, f) - H(c - \hat{c}, f - \hat{f}) && (69)\\
\geq& H(W|b, c, f) - \sum_{j=1}^{M} H(c^j - \hat{c}^j, f^j - \hat{f}^j) && (70)\\
=& H(W|b, c, f) - \sum_{j=1}^{M} H(c^j - \hat{c}^j, f^j - \hat{f}^j, E^j) && (71)\\
=& H(W|b, c, f) - \sum_{j=1}^{M} H(E^j)\\
& - \sum_{j=1}^{M} \Pr(E^j = 1) H(c^j - \hat{c}^j, f^j - \hat{f}^j | E^j = 1) && (72)\\
\geq& H(W|b, c, f) - M - M\bar{P}_e(4Q+2)N(R_L+1) && (73)
\end{aligned}$$

By dividing NM on both sides and letting $N, M \to \infty$, and $\varepsilon_1 = 1/N + \bar{P}_e(4Q+2)(R_L+1)$, we get $\mathcal{H}_k \geq \bar{\mathcal{H}}_k - \varepsilon_1$. Similarly we can prove $\bar{\mathcal{H}}_k \geq \mathcal{H}_k - \varepsilon_2$.

APPENDIX B
PROOF OF LEMMA 4

The lemma follows because relay nodes receive statistically equivalent signals if there are no decoding errors. As we show in Section VI, the lattice point transmitted by the kth node during the first phase in a block, here denoted by J_k^{NM}, is randomly selected and independent from any previously received signals. Hence, $J_k^{NM} = t_{k,1}^{NM}$. Let $\bar{t}_j^{NM}$ denote lattice points generated by the wiretap encoder at the source node.

Then, for the kth relay node, the lattice points on the condition term of $\bar{\mathcal{H}}_k$ in (32) are related to $\bar{t}_j^{NM}$ as follows:

$$t_{k-1,1}^{NM} = J_{k-1}^{NM}, \qquad \bar{t}_{k-1,t}^{NM} = (\sum_{j=0}^{t-2} \bar{t}_j^{NM}) \oplus J_{k+t-2}^{NM},$$
$$t = 2, ..., Q+1 \tag{74}$$

$$\bar{t}_{k+1,1}^{NM} = J_{k+1}^{NM}, \qquad \bar{t}_{k+1,t}^{NM} = (\sum_{j=0}^{t-2} \bar{t}_j^{NM}) \oplus J_{k+t}^{NM},$$
$$t = 2, ..., Q+1 \tag{75}$$

An example is provided in Figure 2 where we label each edge with the lattice point transmitted on this edge. The case for arbitrary k can be easily proved by induction.

From (74)-(75), given the lattice points from the wiretap encoder at the source, i.e., $\bar{t}_j^{NM}$, the joint distribution of the condition terms on $\mathcal{H}_k$ is the same for any k. Hence we have the lemma.

REFERENCES

[1] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2009.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical J.*, vol. 28, no. 4, pp. 656–715, Sep. 1949.

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[7] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.

[8] L. Lai and H. El Gamal, "Cooperation for secrecy: the relay-eavesdropper channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[9] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[10] N. Cai and R. W. Yeung, "Secure network coding," in *2002 IEEE International Symposium on Information Theory*.

[11] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1124–1135, 2011.

[12] L. Lima, M. Medard, and J. Barros, "Random linear network coding: a free cipher?" in *2007 IEEE International Symposium on Information Theory*.

[13] A. Mills, B. Smith, T. Clancy, E. Soljanin, and S. Vishwanath, "On secure communication over wireless erasure networks," in *2008 IEEE International Symposium on Information Theory*.

[14] M. Sikora, J. N. Laneman, M. Haenggi, D. J. Costello, and T. E. Fuja, "Bandwidth-and power-efficient routing in linear wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2624–2633, 2006.

[15] Y. Oohama, "Coding for relay channels with confidential messages," in *2001 Information Theory Workshop*.

[16] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3801–3827, Aug. 2010.

[17] ——, "Two-hop secure communication using an untrusted relay," *Eurasip J. Wireless Commun. and Networking*, vol. vol. 2009, Article ID 305146, 13 pages, 2009, doi:10.1155/2009/305146.

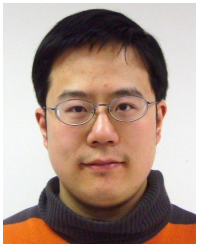
[18] ——, "The role of feedback in two-way secure communication," submitted to *IEEE Trans. Inf. Theory*, Nov., 2009. Available: http://arxiv.org/abs/0911.4432, revised May, 2012.

[19] ——, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," to appear in *IEEE Trans. Inf. Theory*, submitted in March, 2010. Available: http://arxiv.org/abs/1004.1423.

[20] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," *European Trans. Telecommun.*, vol. 19, no. 4, pp. 455–474, June 2008.

[21] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 6463–6486, Oct. 2011.

[22] U. Erez and R. Zamir, "Achieving 1/2 log (1+ SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.
[23] X. He and A. Yener, "Providing secrecy with structured codes: tools and applications to Gaussian two-user channels," submitted to *IEEE Trans. Information Theory*, July, 2009, in revision. Available: http://arxiv.org/abs/0907.5388.
[24] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.
[25] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.
[26] L. Lai, H. El Gamal, and H. V. Poor, "The wiretap channel with feedback: encryption over the channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5059–5067, Nov. 2008.
[27] S. A. Jafar, "Capacity with causal and non-causal side information: a unified view," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5468–5475, Dec. 2006.



Xiang He (S'08, M'10) received B.S. and M.S. degrees in Electrical Engineering from Shanghai Jiao Tong University, Shanghai, China in 2003 and 2006 respectively. His master study is about high speed FPGA implementation of channel encoder, decoder and MIMO detectors. He received his Ph.D. degree in 2010 from the Department of Electrical Engineering at the Pennsylvania State University and joined Microsoft in the that year. In 2010, he received Melvin P. Bloom Memorial Outstanding Doctoral Research Award from the Department of Electrical Engineering at the Pennsylvania State University and the best paper award from the Communication Theory Symposium in IEEE International Conference on Communications (ICC). In 2011, he was named as one of the exemplary reviewers by IEEE Communication Letters. His research interests include information theoretic secrecy, coding theory, queuing theory, optimization techniques, distributed detection and estimation.

Aylin Yener (S'91, M'00) received two B.Sc. degrees, with honors, in Electrical and Electronics Engineering, and in Physics, from Boğaziçi University, Istanbul, Turkey, in 1991, and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from Rutgers University, NJ, in 1994 and 2000, respectively. During her Ph.D. studies, she was with Wireless Information Network Laboratory (WINLAB). From September 2000 to December 2001, she was with the Electrical Engineering and Computer Science Department, Lehigh University, PA, where she was a P.C. Rossin Assistant Professor. In January 2002, she joined the faculty of The Pennsylvania State University, University Park, where she was an Assistant Professor, then Associate Professor, and is currently Professor of Electrical Engineering since 2010. During the academic year 2008-2009, she was a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford CA. Her research interests are in communication theory, information theory and network science, with emphasis on information theoretic security and green communications.

Dr. Yener received the NSF CAREER award in 2003. She has served as Technical Program chair/co-chair on a number of IEEE Symposia including in ICC, PIMRC and VTC, and as an editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and for the IEEE TRANSACTIONS ON COMMUNICATIONS. Her service to the IEEE Information Theory Society includes chairing the Student Committee between 2007-2011, where she co-founded the Annual School of Information Theory in North America in 2008. She currently serves on the Board of Governors of the IEEE Information Theory Society as its treasurer.