End-to-end Secure Multi-hop Communication with Untrusted Relays is Possible

Xiang He Aylin Yener
Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu yener@ee.psu.edu

***Abstract*—We consider a source-destination pair that can communicate only through a chain of unauthenticated intermediate relay nodes over AWGN links. In this scenario, it is desirable to use these relays—as otherwise communicating with the destination is impossible—without the relays being able to decode the information flowing through them. This in turn is tantamount to treating the relays as eavesdroppers from whom the information needs to be kept secret. An important question then becomes that of identifying the limits of reliable and secure communication in this network in the information theoretic sense. In particular, we ask whether it is possible to achieve a non-vanishing perfect secrecy rate regardless of the number of hops. In this work, we find that the answer is yes and show that a constant secrecy rate for an arbitrary number of hops is achievable by employing the combination of a lattice code and a random code.**

I. Introduction

Information theory provides security on the link level [1]. This means a message can be transmitted reliably from a transmitter to a receiver while an eavesdropper is kept unaware of its content. Most known results on information theoretic secrecy focus on "small" networks, which includes the multiple access channel, the broadcast channel, the three node relay channel, and the two user interference channel, e.g., [2], [3], [4]. In this work, in contrast, we consider a scenario where the information has to be transmitted over multiple links and an *end-to-end security* guarantee is desired.

End-to-end security for larger networks with multiple hops has only been addressed in the context of network coding [5]: A potential eavesdropper has access to any one edge of a network and a secure network code design was given therein to keep the eavesdropper oblivious when the network is acyclic. However, a fundamental difference exists between the computer network considered in [5] and the wireless network of interest to us. The latter has *interference*, owing to the broadcast nature of the wireless medium, which can be exploited to enhance security via enlisting the help of friendly nodes, i.e., cooperative jamming [3]. The mechanism of this enhancement is also different from the arithmetic method in [5]. Interference is an addition of real numbers, while the addition in [5] is a modulus addition carried out over a finite group. The latter can perfectly protect the information, as the sum of two independent random variables from a finite group is independent from any one of them. The former cannot.

In this work, we design a coding scheme which provides an end-to-end security guarantee for multi-hop wireless communication. A message is transmitted from the source to the destination over multiple untrusted relays. Since the eavesdropper(s) may reside at any or all of the relays, we require that none of the relay nodes should have any idea of what it is relaying.

A two hop communication system of this nature was considered in [6] in which the relay did compress-and-forward and a positive secrecy rate was achieved via cooperative jamming. However, extending the compress-and-forward coding scheme in [6] to a potentially large number of hops is impractical, since, after each hop, the noise level in the signal increases because the relay can not decode the message and therefore can not completely remove the channel noise. Thus, the main question becomes: Is it possible to achieve a non-vanishing secrecy rate regardless of the number of hops?

Interestingly, in this work, we show that the answer is yes. We provide a coding scheme which is a combination of random wiretap code [1] and a nested lattice code [7]. Nested lattice codes were shown in [7] to achieve the capacity of AWGN channel and then used in [8] to construct a scheme which is asymptotically optimal at high SNR for a bi-directional relay network. Lattice codes for secure communication was considered in [9] for a Modulus-Λ wiretap channel, which is a channel that is more of theoretical interest. On the other hand, the use/benefit of lattice codes in secure communication in Gaussian channels has not been considered. The result of this paper provides the first such use as well as an analytical tool for accomplishing this. The key ingredient is the observation that the modulus operation looses at most 1 bit per channel use under certain conditions.

The analytical tool is presented as Theorem 1 in Section II. It is then used to replace the real sum with a modulus sum with the introduction of genie information with limited rate in Section V. This enables us to lower bound the equivocation using a technique similar to the genie bound from [10] and compute the secrecy rate. The system model is described in Section III. Section IV details the signaling schedule and the coding scheme used to obtain the achievable secrecy rate that is quantified (lower bounded) in Section V. Section VI presents the conclusion of this work.

The following notation is used throughout this paper: H

denotes the entropy, and ε_k is used to denote any variable that goes to 0 when n goes to ∞. We define $C(x) = \frac{1}{2}\log_2(1+x)$. $\lfloor a \rfloor$ denotes the largest integer less than or equal to a. Finally, we note that, due to space limitation, we omit proofs of the lemmas and refer the reader to [11].

II. Preliminaries

In this section we summarize some results about the lattice code which will be useful later.

Let Λ denote a lattice in $\mathcal{R}^N$ and $\mathcal{V}$ denote its fundamental region [7]. Let t_A and t_B be two numbers taken from $\mathcal{V}$. For any set A, define $2A$ as $2A = \{2x : x \in A\}$. Then we have the following lemma:

Lemma 1:

$$\{t_A + t_B : t_A, t_B \in \mathcal{V}\} = 2\mathcal{V} \tag{1}$$

Define A_x as $A_x = \{t_A + t_B + x, t_A, t_B \in \mathcal{V}\}$. Then from the lemma above, we have $A_x = x + 2\mathcal{V}$.

Theorem 1: There is a bijection between $t_A + t_B$ and the tuple $\{T, t_A + t_B \bmod \Lambda\}$, where T is a discrete variable taking value from 1 to 2^N.

Remark 1: Theorem 1 says modulus operation looses at most one bit per dimension of information if $t_A, t_B \in \mathcal{V}$.

Proof: By definition of the modulus Λ operation, we have

$$t_A + t_B \bmod \Lambda = t_A + t_B + x, \quad x \in \Lambda \tag{2}$$

The lemma is equivalent to finding the number of possible x meeting equation (2) for a given $t_A + t_B \bmod \Lambda$.

To do that, we need to know a little more about the structure of lattice Λ. Every point in a lattice, by definition, can be represented by the following form [12]:

$$x = \sum_{i=1}^{N} a_i v_i, v_i \in R^N, a_i \in Z \tag{3}$$

Here $\{a_i\}$ is said to be the coordinates of the lattice point x under the basis $\{v_i\}$.

Based on this representation, we can define the following relationship: Consider two points $x, y \in \Lambda$, with coordinates $\{a_i\}$ and $\{b_i\}$ respectively. Then we say $x \sim y$ if $a_i = b_i \bmod 2$, $i = 1...N$. It is easy to see the relationship $\sim$ is an equivalence relationship. Therefore, it defines a partition over Λ.

1) Depending on the values of $a_i - b_i \bmod 2$, there are 2^N sets in this partition.
2) The sub-lattice 2Λ is one set in the partition, whose members have even coordinates. The remaining $2^N - 1$ sets are its cosets.

Let C_i denote any one of these cosets or 2Λ. Then C_i can expressed as $C_i = 2\Lambda + y_i$, $y_i \in \Lambda$. It is easy to verify that $A_x = x + 2\mathcal{V}$, $x \in C_i$ is a partition of $2\mathcal{R}^N + y_i$, which equals $\mathcal{R}^N$.

We proceed to use the two partitions derived above: Since $C_i, i = 1...2^N$ is a partition of Λ, (2) can be solved by considering the following 2^N equations:

$$t_A + t_B \bmod \Lambda = t_A + t_B + x, \quad x \in C_i \tag{4}$$

From Lemma 1, this means $t_A + t_B \bmod \Lambda \in x + 2\mathcal{V}$ for some $x \in C_i$. Since $x + 2\mathcal{V}, x \in C_i$ is a partition of $\mathcal{R}^N$, there is at most one $x \in C_i$ that meets this requirement. This implies for a given $t_A + t_B \bmod \Lambda$, and a given coset C_i, (4) only has one solution for x. Since there are 2^N such equations, (2) has at most 2^N solutions. Hence each $t_A + t_B \bmod \Lambda$ corresponds to at most 2^N points of $t_A + t_B$. ■

The following crypto lemma [9] is well known and is provided here for completeness.

Lemma 2: Let t_A, t_B be two independent random variables distributed over the a compact abelian group, t_B has a uniform distribution, then $t_A + t_B$ is independent from t_A. Here $+$ is the addition over the group.

III. System Model

The system model is shown in Figure 1 for the three-hop case. The source, node 0, has to communicate over multiple hops to reach the destination, node 4. We assume nodes can not receive and transmit signals simultaneously, and thus we use half-duplex. As shown in Figure 1, we assume every node can only communicate to its two neighbors, one on each side. Let Y_i and X_i be the received and transmitted signal of the ith node respectively. Then they are related as $Y_i = X_{i-1} + X_{i+1} + Z_i$, where Z_i are zero mean Gaussian random variables with unit variance. We assume link noises are

Fig. 1. A Multi-hop Link with 3 Relays

independent from each other. Each node has the same average power constraint: $\frac{1}{n}\sum_{k=1}^{n} E\left[X_i(k)^2\right] \leq \bar{P}$ and the channel gains are normalized for simplicity.

We consider the case where there is an eavesdropper residing at each relay node and these eavesdroppers are not cooperating. This also addresses the scenario where there is one eavesdropper, but the eavesdropper may appear at any one relay node that is unknown a priori. In either case, we need secrecy from all relays and the secrecy constraints for the K relay nodes are expressed as:

$$\lim_{n\to\infty} \frac{1}{n} H\left(W|Y_i^n\right) = \lim_{n\to\infty} \frac{1}{n} H\left(W\right), i = 1...K \tag{5}$$

IV. Signaling Scheme of the Source, the Relays, and the Destination

Because all nodes are half duplex, a schedule is necessary to control when a node should talk. The node schedule is best represented by the acyclic directional graph as shown in Figure 2. The columns in Figure 2 indicate the nodes and the rows in Figure 2 indicate the phases. The length of a phase is the number of channel uses required to transmit a lattice

point, which equals the dimension of the lattice. A node in a row has an outgoing edge if it transmits during a phase. The node in that row has an incoming edge if it can hear signals during the previous phase. It is understood, though not shown in the figure, 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 is called one block, as shown in Figure 2. The boundary of a block is shown by the dotted line in Figure 2. The data transmission is carried over M blocks.

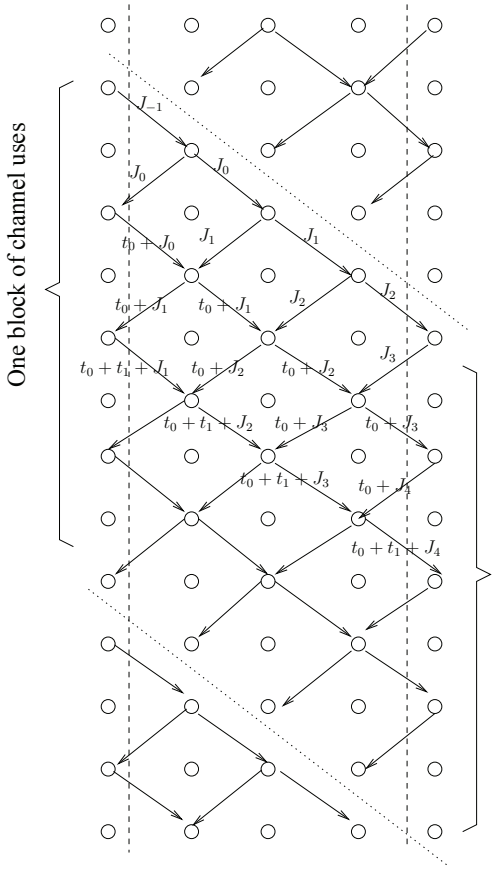

Fig. 2. One Block of Channel Uses

The nested lattice code from [8] is then used within each block. Let (Λ, Λ_1) be a properly designed nested lattice structure in $\mathcal{R}^N$ as described in [7], where Λ_1 is the coarse sub-lattice of the fine lattice Λ. Let $\mathcal{V}_1$ and $\mathcal{V}$ be their respective fundamental regions. Let $a \oplus b$ denotes $(a + b) \bmod \Lambda_1$.

A. The Source Node

The input to the channel by the source has the form $t^N \oplus J^N \oplus d^N$. Here d^N is the dithering noise which is uniformly distributed over $\mathcal{V}_1$. t^N and J^N are determined as follows: If it is the first time the source node transmits during this block, t^N is the origin. J^N is picked from the lattice points in $\Lambda \cap \mathcal{V}_1$ under a uniform distribution. Otherwise, t^N is picked by the encoder. J^N is the lattice point decoded from the jamming signal the source received during the previous phase. This design is not essential but it brings some uniformness in the form of received signals and simplifies explanation.

B. The Relay Node

As this signal propagates toward the destination, each relay node sends a jamming signal in the form of $t_k^N + d_k^N \bmod \Lambda, k = 2...K-1$, where K is the number of nodes. Subscript k denotes the node index which transmit this signal. If this is the first time the relay transmits during this block, then t_k^N is drawn from a uniform distribution over $\Lambda \cap \mathcal{V}_1$, and all previous received signals are ignored. Otherwise, t_k^N is computed from the signal it received during the previous phase. This will be clarified in the sequel. d_k^N again is the dithering noise uniformly distributed over $\mathcal{V}_1$.

The signal received by the relay within a block can be categorized into the following three cases. Let z^N denote the Gaussian channel noise.

1) If this is the first time the relay receives signals during this block, then it has the form $(t_A^N \oplus d_A^N) + z^N$. It only contains interference from its left neighbor.
2) If this is the last time the relay receives signals during this block, then it has the form $(t_B^N \oplus d_B^N) + z^N$. It only contains interference from its right neighbor.
3) Otherwise it has the form

$$y_k^N = (t_A^N \oplus d_A^N) + (t_B^N \oplus d_B^N) + z^N$$

Here t_A^N, t_B^N are lattice points, and d_A^N, d_B^N represent the dithering noise. Following reference [8], if the lattice is properly designed and the cardinality of the set $\Lambda \cap \mathcal{V}_1$ is properly chosen, then for case (3), the relay, with the knowledge of d_A^N, d_B^N, will be able to decode $t_A^N \oplus t_B^N$. For case (1) and (2), the relay will be able to decode t_A^N and t_B^N respectively. Otherwise, we say that a decoding error has occurred at the relay node.

The transmitted signal at the relay node is then computed as follows:

$$x^N = t_A^N \oplus t_B^N \oplus (-x'^N) \oplus d_C^N \tag{6}$$

Here x'^N is the lattice point contained in the jamming signal transmitted by this relay node during the previous phase. $-$ is the inverse operation defined over the group $\mathcal{V}_1 \cap \Lambda$. $t_A^N \oplus t_B^N$ are decoded from the signal it received during the previous phase.

In Figure 2, we labeled the lattice points transmitted over some edges. For clarity we omitted the superscript ^{N}. The $+$ signs in the figure are all modulus operations. The reason why we have $(-x'^N)$ in (6) is now apparent: it leads to a simple expression for the signal as it propagates from the relay to the destination.

C. The Destination

As shown in Figure 2, the destination simulates the behavior of a relay node when it computes its jamming signal. Doing

so ensures the signal received by any relay node has a uniform form.

It is also clear from Figure 2 that the destination will be able to decode the data from the source. This is because the lattice point contained in the signal received by the destination has the form $t^N \oplus J^N$, where t^N is the lattice point determined by the transmitted data, and J^N is the lattice point in the jamming signal known by the destination.

V. A Lower Bound to the Secrecy Rate

Suppose the source transmits $Q+1$ times within a block. Then each relay node receives $Q+2$ batches of signals within the block. An example with $Q = 2$ is shown in Figure 2. Given the inputs from the source of current block, the signals received by the relay node are independent from the signals it received during any other blocks. Therefore, if a block of channel uses is viewed as one mega-channel use, with the source inputs as the channel input, the signals received by the relay as the channel output, then the effective channel is memoryless. Any relay node has the following side

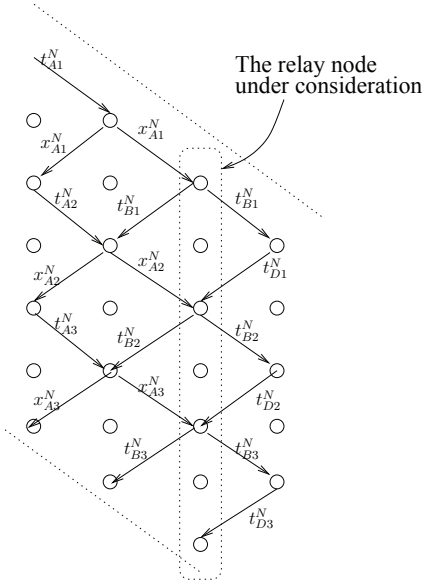

Fig. 3. Notations for Lattice Points contained in Signals, $Q = 2$

information regarding the source inputs within one block:

1) $Q+2$ batches of received signals.
2) All the dithering noises d.
3) Signals transmitted from the relay node during this block. Only the first batch of signals it transmitted may provide more information because all subsequent transmitted signals are computed from received signals and dithering noises.

Let W be the secret message transmitted over M blocks. Following the notation in Figure 3, the equivocation with respect to the relay node is given by:

$$H_2 = \frac{1}{NM} H(W|(x_{A1}^{NM} \oplus d_{\alpha 1}^{NM}) + z_1^{NM}, d_{\alpha 1}^{NM} (x_{Ai}^{NM} \oplus d_{\alpha i}^{NM}) + (t_{D(i-1)}^{NM} \oplus d_{\beta(i-1)}^{NM}) + z_i^{NM}, d_{\alpha i}^{NM}, d_{\beta(i-1)}^{NM}, i = 2...Q+1 (t_{D(Q+1)}^{NM} \oplus d_{\beta(Q+1)}^{NM}) + z_{Q+1}^{NM}, d_{\beta(Q+1)}^{NM}, t_{B1}^{NM}, d_{b1}^{NM}) \quad (7)$$

Let the equivocation under error free decoding be

$$\bar{H}_2 = \frac{1}{NM} H(W|(x_{A1}^{NM} \oplus d_{\alpha 1}^{NM}) + z_1^{NM}, d_{\alpha 1}^{NM} (\bar{x}_{Ai}^{NM} \oplus d_{\alpha i}^{NM}) + (\bar{t}_{D(i-1)}^{NM} \oplus d_{\beta(i-1)}^{NM}) + z_i^{NM}, d_{\alpha i}^{NM}, d_{\beta(i-1)}^{NM}, i = 2...Q+1 (\bar{t}_{D(Q+1)}^{NM} \oplus d_{\beta(Q+1)}^{NM}) + z_{Q+1}^{NM}, d_{\beta(Q+1)}^{NM}, t_{B1}^{NM}, d_{b1}^{NM}) \quad (8)$$

where $\bar{x}_{Ai}^{NM}$ equals the value x_{Ai}^{NM} takes when all decodings are correct. $\bar{t}_{D(i-1)}^{NM}$ and $\bar{t}_{D(Q+1)}^{NM}$ are defined in a similar fashion. Then we have the following lemma:

Lemma 3: For a given Q, $\bar{H}_2 + \varepsilon_2 \geq H_2 \geq \bar{H}_2 - \varepsilon_1$ where $\varepsilon_{1,2} \to 0$ as $N, M \to \infty$.

Lemma 3 says if a equivocation value is achievable with regard to one relay node, when all the other relay nodes do ideal error free decode and forward, then the same equivocation value is achievable when other relay nodes do decode and forward which is only error free in asymptotic sense.

Lemma 4: $\bar{H}_2$ is the same for any relay node.

Lemma 4 can be verified on Figure 2. Given the source node input, the joint distribution of the side information for any relay node is the same. As mentioned earlier, due to the space limit, we omit the proof of Lemma 3 and 4 which can be found in [11].

Theorem 2: For any $\varepsilon > 0$, a secrecy rate of at least $0.5(C(2\bar{P} - 0.5) - 1) - \varepsilon$ bits per channel use is achievable regardless of the number of hops.

Proof: According to Lemma 4, we only need to design the coding scheme based on one relay node. We focus on one block of channel uses as shown in Figure 2. Let $V(j)$ to denote all the side information available to the relay node within the jth block. We start by lower bounding $H(t_0^{NQ}|V(j))$ under ideal error free decoding, where t_0^{NQ} are the lattice points picked by the encoder at the source node as described in Section IV-A within this block. $H(t_0^{NQ}|V(j))$ equals

$$H(t_0^{NQ}|(\bar{x}_{Ai}^{N} \oplus d_{\alpha i}^{N}) + (\bar{t}_{D(i-1)}^{N} \oplus d_{\beta(i-1)}^{N}) + z_i^{N}, d_{\alpha i}^{N}, d_{\beta(i-1)}^{N}, i = 2...Q+1, t_{B1}^{N}, d_{b1}^{N}) \quad (9)$$

Comparing (9) with the condition terms in (8), we see that we have removed the first batch and the last batch of received signals during a block from the condition terms because they are independent from everything else. The last batch of received signals contains the lattice point of the most recent jamming signal observable by the relay node. Its independence follows from Lemma 2.

We then assume that the eavesdropper residing at the relay node knows the channel noise. This means (9) can be lower

bounded by:

$$H(t_0^{NQ}|(\bar{x}_{Ai}^N \oplus d_{\alpha i}^N) + (\bar{t}_{D(i-1)}^N \oplus d_{\beta(i-1)}^N), d_{\alpha i}^N, d_{\beta(i-1)}^N, i = 2...Q+1, t_{B1}^N, d_{b1}^N) \quad (10)$$

Next, we invoke Theorem 1 as described in Section II. Equation (10) can be lower bounded by:

$$H(t_0^{NQ}|\bar{x}_{Ai}^N \oplus d_{\alpha i}^N \oplus \bar{t}_{D(i-1)}^N \oplus d_{\beta(i-1)}^N, T_i, d_{\alpha i}^N, d_{\beta(i-1)}^N, i = 2...Q+1, t_{B1}^N, d_{b1}^N) \quad (11)$$

where, according to Theorem 1, T_i can be represented with N bits. We then apply the following genie lower bound to equation (11):

$$H(A|B,T) = H(A|B) + H(T|B,A) - H(T|B) \quad (12)$$
$$\geq H(A|B) - H(T) \quad (13)$$

and find that (11) is lower bounded by:

$$H(t_0^{NQ}|\bar{x}_{Ai}^N \oplus d_{\alpha i}^N \oplus \bar{t}_{D(i-1)}^N \oplus d_{\beta(i-1)}^N, d_{\alpha i}^N, d_{\beta(i-1),i=2...Q+1}^N, t_{B1}^N, d_{b1}^N) - H(T_{i,i=2...Q+1}) \quad (14)$$
$$= H(t_0^{NQ}|\bar{x}_{Ai}^N \oplus \bar{t}_{D(i-1),i=2...Q+1}^N, t_{B1}^N) - H(T_{i,i=2...Q+1}) \quad (15)$$

It turns out that in the first term in (15), the conditional variables are all independent from t_0^{NQ}. This is because $\bar{t}_{D(i-1)}^N$ contains J_{i-2+k}^N, which is a new lattice point not contained in previous $\bar{t}_{D(j-1)}^N$ or $\bar{x}_{Aj}^N$ $j < i$. The new lattice point is uniformly distributed over $\mathcal{V}_1 \cap \Lambda$. Therefore, from Lemma 2, $\bar{x}_{Ai}^N \oplus \bar{t}_{D(i-1)}^N$ is independent from t_0^{NQ}. Therefore (15) equals

$$H(t_0^{NQ}) - H(T_{i,i=2...Q+1}) \quad (16)$$

Define $c = \frac{1}{NQ} I(t_0^{NQ}; V(j))$. Then from (16), we have $c \in (0,1)$.

To achieve perfect secrecy, we next construct a codebook of rate R and size $2^{\lfloor MNQR \rfloor}$ that spans over M blocks as follows: 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 $\mathcal{V}_1 \cap \Lambda$. The codebook is then randomly binned into several bins. Each bin contains $2^{\lfloor MNQc \rfloor}$ codewords. Denote the codebook with $\mathcal{C}$.

The transmitted codeword is determined as follows: Consider a message set $\{W\}$, whose size equals the number of the bins. The message is mapped to the bins in a one-to-one fashion. The actual transmitted codeword is then selected from the bin according to a uniform distribution. Let this codeword be u^{MNQ}. Let $V = \{V(j), j = 1...M\}$. Then we have:

$$H(W|V,\mathcal{C}) \quad (17)$$
$$= H\left(W|u^{MNQ},V,\mathcal{C}\right) + H\left(u^{MNQ}|V,\mathcal{C}\right) - H\left(u^{MNQ}|W,V,\mathcal{C}\right) \quad (18)$$
$$\geq H\left(u^{MNQ}|V,\mathcal{C}\right) - MNQ\varepsilon \quad (19)$$
$$= H\left(u^{MNQ}|\mathcal{C}\right) - I\left(u^{MNQ};V|\mathcal{C}\right) - MNQ\varepsilon \quad (20)$$
$$\geq H\left(u^{MNQ}|\mathcal{C}\right) - \sum_{j=1}^{M} I\left(u^{MNQ}(j);V(j)\right) - MNQ\varepsilon \quad (21)$$
$$= H\left(u^{MNQ}|\mathcal{C}\right) - MNQc - MNQ\varepsilon \quad (22)$$

(19) follows from Fano's inequality and the size of the bin is picked according to the rate of information leaked to the eavesdropper under the same input distribution used to sample the codebook. (21) follows from $\mathcal{C} \rightarrow u^{MNQ} \rightarrow V$ being a Markov chain. Divide (17) and (22) by MNQ and let $M \rightarrow \infty$, we have $\varepsilon \rightarrow 0$ and $\lim_{M\rightarrow\infty} \frac{1}{MNQ} H(W|V,\mathcal{C}) = \lim_{M\rightarrow\infty} \frac{1}{MNQ} H(W)$. Therefore a secrecy rate of $R - c$ bits per channel use is achieved. According to [8], R can be arbitrarily close to $C(P - 0.5)$ by making $N \rightarrow \infty$, where P is the average power per channel use spent to transmit a lattice point. For a given node, during $2Q+3$ phases, it is active in $Q+1$ phases. Since $c \in [0,1]$, a secrecy rate of $\frac{Q+1}{2Q+3}(C(\frac{2Q+3}{Q+1}\bar{P} - 0.5) - 1)$ is then achievable by letting $M \rightarrow \infty$. Taking the limit $Q \rightarrow \infty$, we have the theorem. ■

VI. Conclusion

In this work, we have considered a source destination pair which can only communicate over a chain of untrusted relay nodes, and showed that, surprisingly, perfectly secure end-to-end communication in the sense of information theoretic security is possible via an intelligent combination of wire-tap and structured codes. Specifically, we have designed a coding scheme which supports a non-vanishing secrecy rate regardless of the number of hops.

References

[1] A. D. Wyner. The Wire-tap Channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[2] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions. *IEEE Transactions on Information Theory*, 54(6):2493–2507, June 2008.

[3] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[4] X. He and A. Yener. Cooperation with an Untrusted Relay: A Secrecy Perspective. Submitted to IEEE Transaction on Information Theory, October, 2008.

[5] N. Cai and R. W. Yeung. Secure Network Coding. *IEEE International Symposium on Information Theory*, June 2002.

[6] X. He and A. Yener. Two-hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming. *IEEE Global Telecommunication Conference*, November 2008.

[7] U. Erez and R. Zamir. Achieving 1/2 log (1+ SNR) on the AWGN Channel with Lattice Encoding and Decoding. *IEEE Transactions on Information Theory*, 50(10):2293–2314, October 2004.

[8] K. Narayanan, M.P. Wilson, and A. Sprintson. Joint Physical Layer Coding and Network Coding for Bi-Directional Relaying. *Allerton Conference on Communication, Control, and Computing*, September 2007.

[9] L. Lai, H. El Gamal, and H.V. Poor. The Wiretap Channel with Feedback: Encryption over the Channel. *IEEE Transaction on Information Theory*, 54(11):5059–5067, November 2008.

[10] S.A. Jafar. Capacity with Causal and Non-Causal Side Information - A Unified View. *IEEE Transactions on Information Theory*, 52(12):5468–5475, December 2006.

[11] X. He and A. Yener. End-to-end Secure Multi-hop Communication with Untrusted Relays. submitted for publication. Available at http://labs.ee.psu.edu/labs/wcan, 2008.

[12] J.H. Conway and N.J.A. Sloane. *Sphere Packings, Lattices and Groups*. Springer, 1999.