Secrecy and Reliable Byzantine Detection in a Gaussian Untrusted Two-Hop Link

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 Gaussian two-hop link where the source and the destination can communicate only via a relay node who is both an eavesdropper and a Byzantine attacker. Both the source and the destination have transmission capability, and the relay node receives a superposition of their transmitted signals plus noise. The proposed coding scheme ensures that the probability of an undetected Byzantine attack decreases exponentially fast with respect to the number of channel uses N_T while the loss in the secrecy rate can be made arbitrarily small. This improves our previous result where this probability only decreased exponentially with respect to $\sqrt{N_T}$.**

I. Introduction

Information theoretic secrecy, first proposed by Shannon [1], is an approach to study the secrecy aspect of a communication system against a *computation power unbounded* adversary. This approach was later applied to the wiretap channel [2], [3] and recently extended to several other models. including, for example, the multiple access channel [4] and the broadcast channel [5], [6].

The impact of information theoretic secrecy on cooperative communications was investigated in references [7]–[10]. [7]–[9] considered the case where a relay node is "curious but honest". That is to say that the relay is not trusted with confidential messages, yet *honestly* employs its designated relaying scheme. An important insight that is gained from this body of work is that recruiting the help of such a relay can be useful in achieving a higher secrecy rate than merely treating it as an eavesdropper [7].

It is a next natural step to consider the problem where the relay node is curious and is potentially *dishonest* [10]. An example for this type of behavior can be that the relay node stops transmitting, which is relatively easy to detect. A more detrimental scenario would be for the relay to deceive the destination into accepting a counterfeit message by actively manipulating the signals it relays, which we refer to as the "Byzantine attack" in this work. Reference [10] found that for a two-hop link with untrusted relay node, it is possible to detect such behavior reliably with an arbitrarily small amount of loss in secrecy rate. Both a noiseless adder model and a Gaussian model were considered.

This work is a continuation and presents a significant improvement over [10] for the two-hop Gaussian model. For this model, the result from [10] shows the probability that a Byzantine attack goes undetected decreases exponentially with respect to *the square root* of the number of channel uses N_T, rather than N_T itself. This is essentially a consequence of the fact that the scheme used in [10] for Byzantine detection entailed using a wiretap code which can provide strong secrecy *and* employing a linear decoder. The only known code with these properties is for the Type II wiretap channel, which is composed of binary erasure links. Reference [10] in essence "transforms" the Gaussian model into a binary erasure channel using repetition codes, which results in the term $\sqrt{N_T}$.

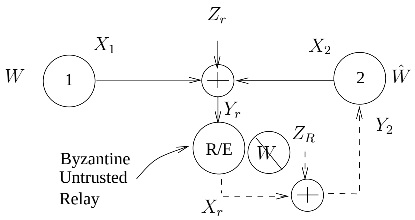

Fig. 1. The Gaussian two-hop link. Phase 1 is indicated by solid line, and phase 2 by dashed line. R/E: Relay/Eavesdropper.

In this work, we present our new finding: the existence of a wiretap code offering both strong secrecy and a linear decoder, proved via a novel combination of Nested Lattice Codes [11] and privacy amplification [12]. As a result, an exponential decrease of the undetected attack probability with respect to N_T is obtained. The key is to view the 1-bit information leaked through observing the real sum of two nested lattice points [13] as the "spoiler information" [14]. This fact is then used to bound Rényi entropy and prove strong secrecy.

II. System Model and Problem Statement

The Gaussian two-hop link with a Byzantine relay node is shown in Figure 1. Node 1 wishes to send a confidential message W to node 2. Since it can not communicate with node 2 directly, it recruits the help of a relay node, who is not trusted with the message W. We assume both node 1 and 2 can transmit [9], and the relay receives a superposition of their transmitted signals plus noise, which is the case in a wireless environment. We let $X_i, i = 1, 2$, and X_r denote the signal transmitted by node 1, 2 and the relay respectively, and similarly $Y_i, i = 1, 2$ and Y_r denote their received signals

978-1-4244-6414-2/10/$26.00 ©2010 IEEE

respectively. After normalizing the channel gains, we have

$$Y_r = X_1 + X_2 + Z_r \tag{1}$$

$$Y_2 = X_r + Z_R, \quad Y_1 = hX_r + Z'_R \tag{2}$$

where Z_r, Z_R and Z'_R are independent Gaussian random variables with zero mean and unit variance, and h is the normalized channel gain. Since Y_1 is not used in the scheme described in this work, it is omitted in Figure 1 for clarity. We assume each node is half duplex. Also, for simplicity, we assume that each node has an average power constraint P.

Observe that since the relay can be a Byzantine adversary, node 2 may or may not accept what it decodes as a genuine message from node 1 based on certain criteria.

The Byzantine detection problem for secure communication can then be stated as follows: Let $\hat{W}$ be the estimate of W computed by the destination, i.e., node 2. We wish to find the rate R_e of W, defined as $R_e = \lim_{n\to\infty} \frac{1}{n} H(W)$, such that the following three conditions are satisfied:

1) *Reliability*: When the relay is honest, both $\Pr(W \neq \hat{W})$ and $\Pr(\hat{W} \text{ is not accepted by Node 2} | W = \hat{W})$ is negligible, i.e., they decrease exponentially in n.
2) *Byzantine Detection*: The probability that the Byzantine adversary wins, defined as $\Pr(A \ wins) \triangleq \Pr(\hat{W} \text{ is accepted by Node 2} | W \neq \hat{W})$ is negligible.
3) *Strong Secrecy*: $I(W; Y_r^n)$ is negligible. Since Y_r^n is the observation of the eavesdropper, this means the adversary has virtually no idea on the value of W.

III. Secrecy

In this section, we briefly review the communication scheme when the relay is "curious but honest", which will be an underlying building block in the sequel. Each node is half-duplex, and consequently we have a two-phase scheme. During phase one, nodes 1 and 2 transmit, and the relay node receives. During phase two, only the relay transmits. It was shown in [9] that these two phases can be used to facilitate the transmission of the confidential message W from node 1 to 2: The channel alternates between phase one and phase two. During phase one, node 1 transmits the confidential message via X_1 and at the same time node 2 sends a signal X_2 to jam the relay node. During phase two, the relay node transmits to node 2 based on the signal it received during phase one. Since node 2 knows X_2, it can subtract it to obtain a cleaner signal. The relay node, however, does not know X_2 and hence can only observe a noisy version of X_1. Intuitively, this means node 1 can transmit to node 2 at a rate higher than the relay node can decode. The exceeding part of the rate can be used to convey confidential messages. Reference [13] used this idea with the compute-and-forward relaying [15].

In this work, we utilize this scheme from [13] as it offers *the algebraic structure* that facilitates reliable detection of a Byzantine attack. The scheme uses Nested Lattice codes [11] as follows:

Consider a pair of N dimensional nested lattice pair $\{\Lambda, \Lambda_c\}$ which is properly designed as in [11]. $\Lambda_c \subset \Lambda$. The modulus operation is defined as $x \bmod \Lambda_c = x - \arg\min_{t\in\Lambda_c} d(x,t)$, where $d(x,t)$ is the Euclidean distance between x and t. The fundamental region of a lattice $\mathcal{V}(\Lambda_c)$ is defined as the set $\{x : x \bmod \Lambda_c = x\}$.

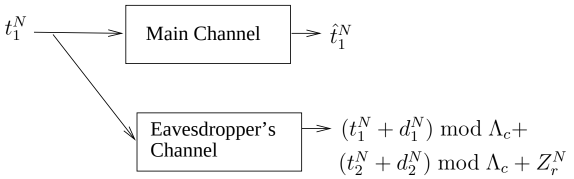
t_1^N
Main Channel
$\hat{t}_1^N$
Eavesdropper's Channel
$(t_1^N + d_1^N) \bmod \Lambda_c +$
$(t_2^N + d_2^N) \bmod \Lambda_c + Z_r^N$

Fig. 2. The Lattice-input Wiretap Channel

Define R_0 as the rate of the lattice codebook, i.e.,

$$R_0 = \frac{1}{N} \log_2 |\Lambda \cap \mathcal{V}(\Lambda_c)| \tag{3}$$

where $|A|$ is the cardinality of the set A. The signal transmitted by each node is given by $X_i^N = \left(t_i^N + d_i^N\right) \bmod \Lambda_c$, $i = 1, 2$, where $t_i^N \in \Lambda \cap \mathcal{V}(\Lambda_c)$, and $d_i^N, i = 1, 2$ are two fixed vectors in $\mathcal{V}(\Lambda_c)$ and are known by the relay node. t_1^N is computed from the confidential message. t_2^N is independent from t_1^N, and is chosen from $\Lambda \cap \mathcal{V}(\Lambda_c)$ according to a uniform distribution. Hence, $X_2^N = t_2^N + d_2^N \bmod \Lambda_c$ serves as the jamming signal to confuse the untrusted relay node.

The relay node will then decode $t_1^N + t_2^N \bmod \Lambda_c$ and transmit $t_1^N + t_2^N + d_3^N \bmod \Lambda_c$ during phase two, where d_3^N is a fixed vector in $\mathcal{V}(\Lambda_c)$ and is known by node 2. Node 2 then decodes $\hat{t}^N = t_1^N + t_2^N \bmod \Lambda_c$ from the signal it received during phase two. An estimate of t_1^N, denoted by $\hat{t}_1^N$, is then computed from $\hat{t}^N - t_2^N \bmod \Lambda_c$.

With this coding scheme, the Gaussian two-hop link is equivalent to the lattice input wiretap channel shown in Figure 2. Reference [15] proves that, when $R_0 < \frac{1}{2}\log_2(\frac{1}{2} + P)$, the probability $\Pr(\hat{t}_1^N \neq t_1^N)$ decreases exponentially with respect to N. Reference [13] proves the eavesdropper can get *at most* 1 *bit of information* from its observation; see also [16]. Hence the achievable secrecy rate is [13]:

$$R_e = [R_0 - 1]^+ \tag{4}$$

where $[x]^+$ equals x if $x \geq 0$ or 0 otherwise.

Remark 1: We emphasize the coding scheme [13] is *non-linear*. To achieve (4), the codewords are generated in an i.i.d. fashion from the set $\Lambda \cap \mathcal{V}(\Lambda_c)$. Hence each codeword is composed of a sequence of lattice points. These codewords are then randomly binned into several bins, such that each bin by itself is a codebook with a rate of 1 bit per channel use. The encoder at node 1 first chooses a bin according to W, then randomly chooses a codeword to transmit from that bin according to a uniform distribution. This is needed in order to confuse the eavesdropper. However, it also introduces a *nonlinear* mapping between the codewords and the message set. □

IV. Byzantine Detection

For Byzantine detection, we use the algebraic manipulation detection (AMD) code [17]. An AMD codeword is composed of three parts: $\{s, x, h\}$, where s is the $d \times 1$ vector composed of elements from $\mathcal{GF}(q^r)$ and represents the message. The component x is called the random seed and is also from $\mathcal{GF}(q^r)$. h is the hash tag and is computed according to the hash rule: $h = x^{d+2} + \sum_{i=1}^{d} s_i x^i$, where s_i is the ith component of s and the addition and multiplication is defined over $\mathcal{GF}(q^r)$. Suppose node 2 receives s', x', h', where $s' \neq s$. Let $\Delta_x = x' - x$. $\Delta_h = h' - h$. Then [17] has the following result:

Theorem 1: [17, Theorem 2] Assume at least one of $s' - s, \Delta_x, \Delta_h$ is not zero. If the distribution of x conditioned on $\{\Delta_x, \Delta_h, s', s\}$ is uniform over the field $\mathcal{GF}(q^r)$, q being a prime, and $d+2$ is not divisible by q, then the probability that the hash rule holds for $\{s', x', h'\}$ is bounded by $\frac{d+1}{q^r}$.

Remark 2: As shown in [10, Section III.B], transmitting an AMD tuple $\{s, x, h\}$ using a randomly generated wiretap code, whose decoder is nonlinear, will render Δ_x correlated with x. Hence conditioned on $\{\Delta_x, \Delta_h, s', s\}$, x is not uniformly distributed and Theorem 1 can not be used. □

V. Main Results

As eluded in Remark 1 and 2, a new coding scheme is needed to properly combine Byzantine detection and secrecy sharing scheme for the Gaussian model. In [10], we circumvented this problem by transforming the channel into a Type II wiretap channel via the repetition code. In this work, we describe a different coding scheme to transmit x and h, which leads to faster decrease in the probability of undetected Byzantine attack with a cost of arbitrarily small loss in the strong secrecy rate.

A. Extracting Strong Secrecy from a Lattice Point

1) When $\Lambda_c = q\Lambda$ for a prime q: In this case, the set $(\Lambda + d^N) \cap \mathcal{V}(\Lambda_c)$ is isomorphic to a finite field, as shown by Lemma 1. The proof is omitted due to space limitation, please see [18].

Lemma 1: When $\Lambda_c = q\Lambda$ for a prime q and Λ has full rank, $(\Lambda + d^N) \cap \mathcal{V}(\Lambda_c)$, for the modulus-Λ_c plus operation, is isomorphic to the group of a finite field $\mathcal{GF}(q^N)$.
The reason that we consider this case is that the resulting coding scheme has a linear decoder and hence can be used to transmit x and h. This is shown by the following theorem:

Theorem 2: For an integer r, such that

$$0 \leq r \leq N \left[1 - \frac{1+\varepsilon}{\log_2 q}\right]^+ \tag{5}$$

where $\varepsilon > 0$ is a constant that can be arbitrarily small, there exists a linear mapping $\mathbf{g}$ from $\mathcal{GF}(q)^N$ to $\mathcal{GF}(q)^r$ such that

1) $\mathbf{g}$ has full row rank r.
2) Define $\bar{Y}_r^N = \sum_{i=1}^{2} ((t_i^N + d_i^N) \bmod \Lambda_c)$, which is the signal component in the observation of the eavesdropper in Figure 2. When $t_i^N, i = 1, 2$ are uniformly distributed over $(\Lambda + d_i^N) \cap \mathcal{V}(\Lambda_c)$ and are independent of each other, we have

$$I\left(\mathbf{g}\left(t_1^N\right); \bar{Y}_r^N\right) \leq 2e^{-\beta N} \tag{6}$$

for a certain constant $\beta > 0$.

Before proving the theorem, we need several supporting results: First, the *representation theorem* from [13] is useful:

Theorem 3: [13, Theorem 1] [16, Corollary 1] For any u_1, u_2, such that $u_i \in \mathcal{V}(\Lambda_c), i = 1, 2$, $\sum_{k=1}^{2} u_k$ is uniquely determined by $\{T, \sum_{k=1}^{2} u_k \bmod \Lambda_c\}$, where T is an integer such that $1 \leq T \leq 2^N$.
Based on Theorem 3, $\bar{Y}_r^N$ can be represented by $\{(\sum_{i=1}^{2}(t_i^N + d_i^N)) \bmod \Lambda_c, T\}$. Since $d_i^N, i = 1, 2$ are known by all nodes, this means $\bar{Y}_r^N$ can be represented by $\{(t_1^N + t_2^N) \bmod \Lambda_c, T\}$.

We also need the following result: Let $\mathbf{G}$ be taken from a set of linear mappings from $\mathcal{GF}(q)^N$ to $\mathcal{GF}(q)^r$ according to a uniform distribution. Hence $\mathbf{G}$ can be represented as a matrix over $\mathcal{GF}(q)$ with r rows and N columns. For $\mathbf{G}$, we have the following lemma. The proof is omitted due to space limitation, see [18].

Lemma 2: The probability that $\mathbf{G}$ has full row rank is greater than $1 - q^{r-N}$.

Finally, we need the results from [12]: For a discrete random variable X, let $H_2(X)$ denote the Rényi entropy. $H(X)$ denotes the Shannon entropy. The notion of "universal hash function" is as defined in [12].

Lemma 3: [12] The set of linear mappings is a class of universal hash function.

Theorem 4: [12, Corollary 4] Let A, B be two random variables. Let $\mathcal{A}$ be the alphabet set A is defined on. Let $\mathbf{G}$ be chosen according to a uniform distribution from a class of universal hash function from $\mathcal{A}$ to $\mathcal{GF}(q)^r$. For two random variables A, B, if for a constant c, $H_2(A|B = b) > c$, then

$$H(\mathbf{G}(A)|\mathbf{G}, B = b) > r \log_2 q - 2^{r \log_2 q - c}/\ln 2 \tag{7}$$

Now, with the supporting results at hand, we provide the proof for Theorem 2:

Proof: Define $a \oplus b$ as $a + b \bmod \Lambda_c$. Then for the distribution for $t_i^N, i = 1, 2$ stated in Theorem 2, $t_1^N \oplus t_2^N$ is independent from t_1^N. Therefore we have:

$$H_2\left(t_1^N | t_1^N \oplus t_2^N = t^N\right) = H_2\left(t_1^N\right) = N \log_2 q \tag{8}$$

Let T be the integer defined in Theorem 3 and $|\mathcal{T}|$ be the cardinality of the set of possible values for T. Then according to [14, Theorem 5.2] [19, Lemma 3], for a given integer a, $1 \leq a \leq 2^N$ and $t^N \in \Lambda \cap \mathcal{V}(\Lambda_c)$, with probability $1 - 2^{-(s/2-1)}$:

$$H_2\left(t_1^N | t_1^N \oplus t_2^N = t^N, T = a\right) \tag{9}$$
$$\geq H_2\left(t_1^N | t_1^N \oplus t_2^N = t^N\right) - \log_2 |\mathcal{T}| - s \tag{10}$$
$$= N\left(\log_2 q - 1\right) - s \tag{11}$$

Note that the adding group of $\mathcal{GF}(q^N)$ is isomorphic to $\mathcal{GF}(q)^N$. Hence we can write $t_1^N \in \mathcal{GF}(q)^N$. Let $\mathbf{G}$ be taken from a set of linear mappings from $\mathcal{GF}(q)^N$ to $\mathcal{GF}(q)^r$ according to a uniform distribution. Then according to Lemma 3, $\mathbf{G}$ is a universal hash function. According to Theorem 4, from (11) we have:

$$H\left(\mathbf{G}\left(t_1^N\right) | \mathbf{G}, t_1^N \oplus t_2^N = t^N, T = a\right) \tag{12}$$

$$\geq r\log_2 q - \frac{2^{r\log_2 q - c}}{\ln 2} \tag{13}$$

where $c = N(\log_2 q - 1) - s$.

Since (11) holds with probability $1 - 2^{-(s/2-1)}$, (13) means

$$H\left(\mathbf{G}\left(t_1^N\right)|\mathbf{G}, t_1^N \oplus t_2^N, T\right) \tag{14}$$

$$\geq \left(1 - 2^{-(s/2-1)}\right)\left(r\log_2 q - \frac{2^{r\log_2 q - c}}{\ln 2}\right) \tag{15}$$

Choose $s = \varepsilon N$, where $0 < \varepsilon < \log_2 q - 1$. Choose r such that for $\delta > 0$:

$$r\log_2 q < N\left(\log_2 q - 1\right) - s - N\delta = N\left(\log_2 q - 1 - \varepsilon - \delta\right) \tag{16}$$

which yields (5). For this r and s, from (15), we observe that there exists $\beta > 0$, such that

$$I\left(\mathbf{G}\left(t_1^N\right); t_1^N \oplus t_2^N, T|\mathbf{G}\right) \leq e^{-\beta N} \tag{17}$$

We next use the fact that for sufficiently large N, most $\mathbf{G}$ will have full row rank as shown in Lemma 2. Therefore, with a uniform distribution for $t_i^N, i = 1, 2$, t_1^N and t_2^N being independent, there must exists a $\mathbf{G} = \mathbf{g}$, such that

1) $\mathbf{g}$ has full rank.
2) $I\left(\mathbf{G}\left(t_1^N\right); t_1^N \oplus t_2^N, T|\mathbf{G} = \mathbf{g}\right) \leq 2e^{-\beta N}$

Hence we have proved Theorem 2. ■

2) The General Case: When (Λ, Λ_c) does not have the self-similar relationship as described in Section V-A1, we can still extract strong secrecy from a lattice point using the same method, except that the resulting coding scheme is not linear. Let $\lfloor x \rfloor$ be the operation that rounds x to the nearest integer less than or equal to x. Define $N_0 \triangleq \lfloor \log_2 |\Lambda \cap \mathcal{V}(\Lambda_c)| \rfloor$. Recall that N is the dimension of lattice Λ, and R_0 is defined in (3). Hence we have $N_0 \geq NR_0 - 1$. Choose the subset K of the codebook $(\Lambda + d_1^N) \cap \mathcal{V}(\Lambda_c)$ that yields the minimal average decoding error probability with the lattice decoder and has size $|K| = 2^{N_0}$. Define v as the one-to-one mapping from K to $\mathcal{GF}(2^{N_0})$. Then we have the following theorem:

Theorem 5: For an integer r_0, such that

$$0 \leq r_0 \leq N[R_0 - 1 - \varepsilon]^+ \tag{18}$$

for a constant $\varepsilon > 0$, there exists a linear mapping $\mathbf{g}$ from $\mathcal{GF}(2)^{N_0}$ to $\mathcal{GF}(2)^{r_0}$ such that

1) $\mathbf{g}$ has full row rank r_0.
2) When t_1^N is uniformly distributed over K, t_2^N is uniformly distributed over $(\Lambda + d_2^N) \cap \mathcal{V}(\Lambda_c)$, t_1^N, t_2^N are independent of each other, we have $I\left(\mathbf{g}\left(v(t_1^N)\right); \bar{Y}_r^N\right) \leq 2e^{-\beta N}$ for a certain $\beta > 0$.

The proof is similar to Theorem 2 and therefore omitted.

Theorem 5 can be used to construct an encoder with rate arbitrarily close to $[R_0 - 1]^+$, as shown below:

Let $\mathbf{g}'$ be an $(N_0 - r_0) \times N_0$ matrix such that $\begin{bmatrix} \mathbf{g}' \\ \mathbf{g} \end{bmatrix}$ is invertible. Define $\mathbf{S}$ and $\mathbf{S}'$ such that

$$\begin{bmatrix} \mathbf{g}'_{(N_0 - r_0) \times N_0} \\ \mathbf{g}_{r_0 \times N_0} \end{bmatrix} v(t_1^N) = \begin{bmatrix} \mathbf{S}'_{(N_0 - r_0) \times 1} \\ \mathbf{S}_{r_0 \times 1} \end{bmatrix} \tag{19}$$

Then $\mathbf{S} = \mathbf{g}(v(t_1^N))$. Define $\mathbf{A}$ as the inverse of $\begin{bmatrix} \mathbf{g}' \\ \mathbf{g} \end{bmatrix}$, then the encoder is given by:

$$t_1^N = v^{-1}\mathbf{A}\begin{bmatrix} \mathbf{S}'_{(N_0 - r_0) \times 1} \\ \mathbf{S}_{r_0 \times 1} \end{bmatrix} \tag{20}$$

where $\mathbf{S} \in \mathcal{GF}(2^{r_0})$ be the input to the encoder. We assume $\mathbf{S}$ is uniformly distributed over $\mathcal{GF}(2^{r_0})$. $t_1^N \in \Lambda \cap \mathcal{V}(\Lambda_c)$ be its output. $\mathbf{S}'$ represents the randomness in the encoding scheme. We observe that, if $\{\mathbf{S}'_{(N_0 - r_0) \times 1}, \mathbf{S}_{r_0 \times 1}\}$ is uniformly distributed over $\mathcal{GF}(2)^{N_0}$ and (20) is used as the encoder, t_1^N is also uniformly distributed over the set K. Since $\mathbf{G} = \mathbf{g}$ is chosen when t_1^N has a uniform distribution over K, this means that when (20) is used as an encoder, the secrecy constraint in Theorem 5 still holds.

B. Transmitting the AMD tuple

We now describe how to use the coding scheme in Section V-A to transmit an AMD tuple. Note that the distribution of hash tag h is in general not uniform. Hence, we can not directly use the linear coding scheme in Section V-A to transmit h, which needs an uniform input distribution. However, this problem can be solved by introducing another random seed k from $\mathcal{GF}(q^r)$, which can be generated via the linear coding scheme in Section V-A. From Section V-A, k is uniformly distributed over $\mathcal{GF}(q^r)$. Hence h can be transmitted by using k as *a one-time pad* [1].

The transmission is hence divided into 4 stages:

1) $x \in \mathcal{GF}(q^r)$ is extracted from an N dimensional lattice code as shown in Section V-A1.
2) $k \in \mathcal{GF}(q^r)$ is extracted from an N dimensional lattice code as shown in Section V-A1. Let $\hat{k}$ be the estimate of it computed by node 2. Let P_1 be the average power per channel use of the N dimensional lattice code.
3) $u = h \oplus k$ is transmitted via the relay to node 2 using an r-dimensional lattice code at $\log_2 q$ bits per channel use. Node 2 does not transmit during this stage since h is already protected by the one-time pad k. Let $\hat{u}$ be the estimate of it computed by node 2. Let P_2 be the power per channel use of the r dimensional lattice code.
4) s is transmitted via the encoder described in Section V-A2. Let $\hat{s}$ be the estimate of s computed by node 2, which corresponds to s' in Theorem 1.

Note that both P_1 and P_2 are only a function of the rate of their respective lattice code. Hence P_1 and P_2 are only a function of q. Then we have the following lemma:

Lemma 4:

$$I\left(x; \Delta_x, \Delta_h, \hat{s}, s\right) < 4\exp(-\beta N) \tag{21}$$

where β is a positive number defined in Theorem 2.
The proof of Lemma 4 is based on the strong secrecy offered by Theorem 2 and Theorem 5 and is omitted here due to space limitation. We next link Lemma 4 and Theorem 1 with Pinsker's inequality which leads to our **main result**:

Theorem 6: For the Gaussian two-hop link, for a rate smaller but arbitrarily close to R_e given by (4), and a total number of channel uses $N_T = O(N)$:

1) When the relay is honest, the confidential message W can be transmitted at this rate such that all the three terms $\Pr(W \neq \hat{W})$, $I(W; Y_r^n)$ and $\Pr\left(\hat{W} \text{ is not accepted by Node } 2 | W = \hat{W}\right)$ decrease exponentially fast with N.
2) When the relay is dishonest, $\Pr(A\ wins)$ decreases exponentially fast with N.

Proof Outline: Here, we only outline the proof for part 2), due to space limitations. For the complete proof, see [18]. The proof technique used is similar to the one used in [10], where Lemma 4 corresponds to [10, Lemma 1]. As in [10], we use “HRH” for “hash rule holds” when for $s \neq s'$, $x^{d+2} + \sum_{i=1}^{d} s_i x^i = x'^{d+2} + \sum_{i=1}^{d} s_i' x'^i + \Delta_h$. This means the message s', x', h' will be accepted by node 2. Hence the probability that the adversary wins is given by:

$$\begin{aligned} &\Pr(A\ wins) \\ &= \sum_{\substack{x,\Delta_x \\ \Delta_h, s, s'}} \begin{aligned} &\Pr(\text{HRH} | x, \Delta_h, \Delta_x, s, s') \\ &\Pr(x | \Delta_h, \Delta_x, s, s') \Pr(\Delta_h, \Delta_x, s, s') \end{aligned} \end{aligned} \tag{22}$$

Define $Q(A\ wins)$ as the term (22) with $\Pr(x | \Delta_h, \Delta_x, s, s')$ replaced by $\Pr(x)$. Then as shown in [10, Lemma 2], Lemma 4 leads to the following result due to Pinsker’s inequality:

$$|\Pr(A\ wins) - Q(A\ wins)| \leq \sqrt{(8 \ln 2) \exp(-\beta N)} \tag{23}$$

From Theorem 1, $Q(A\ wins)$ is bounded by $\frac{d+1}{q^r}$. Hence

$$\Pr(A\ wins) \leq \sqrt{(8 \ln 2) \exp(-\beta N)} + \frac{d+1}{q^r} \tag{24}$$

Each $\{s\}$ conveys $dr \log_2 q$ bits of information, where r is defined in Theorem 2. Hence the total number of channel uses N_T is given by

$$N_T = 2N + r + \left\lceil \frac{dr \log_2 q}{N R_e} \right\rceil N \tag{25}$$

since N channel uses are needed to transmit x or k, and r channel uses are needed to transmit $k \oplus h$. The third term in (25) is the number of channel uses needed to transmit s, where $\lceil x \rceil$ is the operation that rounds x to the nearest integer greater than or equal to x.

The overall rate R_T is given by $R_T = \frac{dr \log_2 q}{N_T}$. The average power per channel use P_T is given by

$$P_T = \frac{P_1 2N + P_2 r + P\left(\frac{dr \log_2 q}{R_e}\right)}{N_T} \tag{26}$$

R_T and P_T can be made arbitrarily close to R_e and P respectively by choosing a sufficient large d. Once R_T and P_T is fixed, d is fixed. On the other hand, as shown by (25) and (5), for a fixed d, N_T increases linearly with respect to N. Now, choose r as in (5) such that r increases linearly with respect to N. Then, from (24), we observe that the probability that the adversary wins decreases exponentially fast with N. Hence, we have the bound on $\Pr(A\ wins)$ stated in the theorem.

■

VI. Conclusion

In this work, we proved that for the Gaussian two-hop model where the relay is both an eavesdropper and a Byzantine attacker, the probability that a Byzantine attack goes undetected can decrease exponentially fast with respect to the total number of channel uses. In this process, we showed how to provide strong secrecy via a novel combination of Nested Lattice Codes and privacy amplification. Furthermore, we showed that the secrecy rate loss caused by the redundancy introduced for Byzantine detection can be made arbitrarily small.

References

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, September 1949.

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

[3] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[4] 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.

[5] R. Liu, T. Liu, H. V. Poor, and S. Shamai. Multiple-Input Multiple-Output Gaussian Broadcast Channels with Confidential Messages. Submitted to IEEE Transactions on Information Theory, March 2009.

[6] E. Ekrem and S. Ulukus. The Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel. Submitted to IEEE Transactions on Information Theory, March 2009.

[7] X. He and A. Yener. Cooperation with an Untrusted Relay: A Secrecy Perspective. Submitted to IEEE Transactions on Information Theory, October, 2008, revised, October, 2009.

[8] E. Ekrem and S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. Submitted to IEEE Transactions on Information Theory, October, 2008.

[9] X. He and A. Yener. Two-hop Secure Communication Using an Untrusted Relay. to appear in EURASIP Journal on Wireless Communication and Networking, Special issue in Wireless Physical Layer Security, Available online at http://arxiv.org/abs/0910.2718, October, 2009.

[10] X. He and A. Yener. Secure Communication with a Byzantine Relay. In *IEEE International Symposium on Information Theory*, June 2009.

[11] 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.

[12] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized Privacy Amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, November 1995.

[13] X. He and A. Yener. Providing Secrecy with Lattice Codes. In *46th Allerton Conference on Communication, Control, and Computing*, September 2008.

[14] C. Cachin. Entropy Measures and Unconditional Security in Cryptography. *PhD Thesis*, 1997.

[15] K. Narayanan, M. P. Wilson, and A. Sprintson. Joint Physical Layer Coding and Network Coding for Bi-Directional Relaying. In *45th Allerton Conference on Communication, Control, and Computing*, September 2007.

[16] X. He and A. Yener. Providing Secrecy With Structured Codes: Tools and Applications to Gaussian Two-user Channels. Submitted to IEEE Transactions on Information Theory, July, 2009, Available online at http://arxiv.org/abs/0907.5388.

[17] R. Cramer, Y. Dodis, S. Fehr, C. Padro, and D. Wichs. Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors. *Lecture Notes in Computer Science*, 4965:471, 2008.

[18] X. He and A. Yener. Strong Secrecy and Reliable Byzantine Detection in the Presence of an Untrusted Relay. to be submitted to IEEE Transactions on Information Theory, 2009.

[19] U. Maurer and S. Wolf. Information-theoretic Key Agreement: From Weak to Strong Secrecy for Free. *Lecture Notes in Computer Science*, pages 351–368, 2000.