ISIT 2009, Seoul, Korea, June 28 - July 3, 2009

Secure Communication with a Byzantine Relay

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 communication scenario where the source and the destination can communicate only via a relay node who is both an eavesdropper and a Byzantine attacker. Hence for secure communication, two requirements must be met simultaneously: the transmitted message must be kept secret, and a Byzantine attack must be detected reliably. Both a discrete noiseless adder model with the relay receiving the *real* sum of two signals and a Gaussian model are considered. In both models, the loss in rate due to Byzantine detection can be made arbitrarily small. For the discrete adder model, we show that the probability that the adversary wins decreases exponentially with the number of channel uses. For the Gaussian model, we show that this probability decreases exponentially with the square root of the number of channel uses. The rate derived in this paper is the *strong secrecy* rate, and the rate loss incurred due to the untrusted and Byzantine relay is measured with respect to the achievable secrecy rate when the relay is untrusted but honest. The result is obtained via a careful combination of the algebraic manipulation detection (AMD) code, the linear wire-tap code constructed from low density parity check (LDPC) code, randomly generated wire-tap code and for the Gaussian model the lattice code.**

I. Introduction

Information theoretic secrecy was established by Shannon [1]. Wyner had used this notion to show that uncertainty in the channel can facilitate secret communication [2]. This approach was then extended to more involved channel models, e.g. [3], [4], leading to a body of literature which provides fundamental limits under which secret communication can take place in the presence of a computation-power unlimited eavesdropper.

The impact of information theoretic secrecy on cooperative communications was investigated in references [5]–[7]. The cooperative communication schemes in these works rely on a relay node that is not trusted with confidential messages but would *always* employ its designated relaying scheme. An important insight that is gained from this body of work is that even if the relay is not trusted, as long as it is honest, recruiting it to help relay information can be useful in achieving a higher secrecy rate than just treating the relay node as an eavesdropper [5].

Naturally, the next step is to consider the case where the relay node is malicious, or equivalently is a compromised node. If the relay chooses not to perform its designated relay function, one possible consequence is to cause a decoding error at the destination. It is also possible that the decoder produces a message estimate W', such that W' is not the actual message W from the source. In this case, the destination will accept W' as the message from the source. The question is whether it is possible for the adversary at the relay node to manipulate the destination into accepting W' without being detected. The main purpose of this paper is to find a reliable detection method for this *Byzantine attack* in the presence of a *computation-power unbounded* adversary.

Byzantine attack detection can be viewed as an authentication problem, by treating the counterfeit message W' as a message from a non-legitimate source. An information theoretic secrecy scheme with an authentication capability was proposed in [8]. The authors used a wire-tap code providing strong secrecy from [9]. In this approach, the destination needs to know the authentication key beforehand.

It is known, on the other hand, that to detect a Byzantine attack, it is not essential to share keys. In reference [10], the so called algebraic manipulation detection (AMD) code was used for encoding the source data which ensures the probability that the adversary wins can be made arbitrarily small with an arbitrarily small loss in rate. A limitation of this scheme is that it has to be used along with a secrecy sharing scheme that is *linear* [10]. Many secrecy sharing schemes in *noisy* channels use nonlinear coding schemes. This makes the application to noisy channels challenging at best.

In this work, we consider a two-hop communication system with a relay node that is not only untrusted but also potentially malicious. Hence both secrecy and Byzantine detection are needed. Two models are considered: (1) a discrete adder model where the relay receives the *real* sum of the signals transmitted by the other two nodes; (2) a Gaussian model where the transmitted signals are continuous and the received signals are corrupted by Gaussian noise. In both cases, we prove that the probability that a Byzantine adversary wins can be made arbitrarily small at a cost of an arbitrarily small amount of loss in *strong secrecy rate*. To prove this result, we leverage two facts: (i) linear secret sharing schemes exist for the type II wire-tap channel where the eavesdropper channel is a binary erasure channel, and (ii) only a small portion of an AMD codeword needs to be sent over a linear secrecy sharing scheme. In both models, we take advantage of these facts by simulating a low rate binary erasure channel. The end result is obtained by combining the AMD code [10], the LDPC based type II wire-tap code [11], the randomly generated wire-tap code [9], and for the Gaussian case the lattice code [12].

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

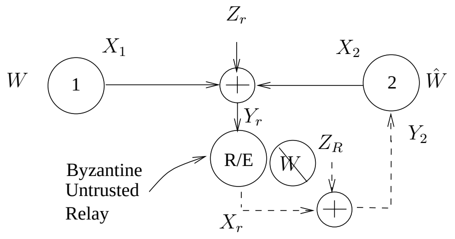

Fig. 1. The Gaussian two-hop link. Phase 1 is indicated by solid line, and phase 2 by dashed line. R/E: Relay/Eavesdropper. For the adder model, simply remove all noise and restrict signals to integers in the range $[0, B-1]$.

II. System Model

We consider a two-hop network with two-phase communications as shown in Figure 1. Node 1 wants to send a confidential message W to node 2 via a relay node that is untrusted. In [7], we showed that by allowing node 2 to transmit, a two-phase protocol can be developed to provide secrecy. In this protocol, during the first phase, both nodes 1 and 2 transmit. We use X_i to denote the signal transmitted by node i. In the Gaussian model, X_i is continuous and the signal received by the relay is denoted by $Y_r = X_1 + X_2 + Z_r$. In phase two, the relay node transmits X_r. Let Y_2 denote the signal received by node 2 during phase two, $Y_2 = X_2 + Z_R$. Z_r and Z_R are independent Gaussian random variables with zero mean and unit variance. For simplicity, we assume that each node has an average power constraint P and the channel gain of each link is unity.

The discrete adder model is very similar to the Gaussian model. The differences are that now $X_i, i = 1, 2$ and X_r are integers in the range $[0, B-1]$, where B is an integer and $B \geq 2$; the noise terms are removed. Hence, we have $Y_r = X_1 + X_2$ and $Y_2 = X_r$.

III. Review of Known Results

A. AMD Code [10]

Let the input to an AMD encoder be denoted by s. It is assumed that s is a $1 \times d$ vector. Each component of it is taken from a finite field $\mathbf{GF}(q^m)$. The output of the encoder is given by the tuple $\{s, x, h\}$, where x is uniformly distributed over $\mathbf{GF}(q^m)$ and is independent from s, and h 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 $\mathbf{GF}(q^m)$. h is usually called the "hash tag". Suppose the node 2 receives s', x', h', where $s' \neq s$. Let $\Delta_x = x' - x$. $\Delta_h = h' - h$. Then [10] has the following result:

Theorem 1: [10, Theorem 2] If the distribution of x conditioned on $\{\Delta_x, \Delta_h, s', s\}$ is uniform over the field $\mathbf{GF}(q^m)$, q being a prime, and $d+2$ is not divisible by q, then the probability that the hash rule holds is bounded by $\frac{d+1}{q^m}$.

B. Limits of AMD Code

To motivate the next section, we briefly describe the difficulty in applying AMD code in our setting. Consider the discrete adder model. It is immediate that a direct application to this model is impossible due to the fact X_r^n is computed from $Y_r^n = X_1^n + X_2^n$, where the component-wise "+" means real addition rather than modulus addition. Hence Y_r^n is not independent from X_1^n and the condition in Theorem 1 is not fulfilled.

To solve this problem, we consider using a serial concatenation of the wire-tap code and the AMD code. Let f be the stochastic encoding function of the wire-tap code. Then Y_r^n contains little information from the input to the wire-tap code encoder, which in this case is an AMD codeword $\{s, x, h\}$, if the wire-tap code is designed according to [9].

Let the input to the decoder of the wire-tap code be $\hat{X}_1^n$. Then in the case of the discrete adder model, it is given by

$$\hat{X}_1^n = X_r^n - X_2^n \mod B \tag{1}$$

If the relay is honest, then $\hat{X}_1^n$ should equal X_1^n, which is mapped to $f^{-1}(X_1^n)$. Otherwise, the decoder will receive $f^{-1}(X_r^n - X_2^n \mod B)$. The difference is hence given by

$$f^{-1}(X_r^n - X_2^n \mod B) - f^{-1}(X_1^n) \tag{2}$$

Note that (2) corresponds to Δ_x, and $f^{-1}(X_1^n)$ corresponds to x in Theorem 1, and even though the adversary has little information about $f^{-1}(X_1^n)$, in general (2) is *not* independent from $f^{-1}(X_1^n)$.

This problem can be alleviated if f^{-1} is linear. In this case, (2) is given by

$$f^{-1}((X_r^n - (X_1^n + X_2^n) \mod B) \mod B) \tag{3}$$

Note that X_r^n is computed from Y_r^n. $(X_1^n + X_2^n) \mod B$ can also be computed from Y_r^n. If Y_r^n is almost independent from the confidential message then (3) is almost independent from $f^{-1}(X_1^n)$. One case where f^{-1} *is* linear is the Type II wire-tap channel.

C. Type II Wire-tap Channel

In the Type II wire-tap channel model [13], the main channel is a noiseless binary channel and the eavesdropper channel is a binary erasure channel with erasure probability ϵ. It was shown in [11] that the dual code of a "good" linear code can be used to construct codes for the Type II wire-tap channel as follows.

Let H denote the parity check matrix of a linear block code $\mathcal{C}$. Let the input to the encoder be $\mathbf{s}$, and the output of the encoder be $\mathbf{x}$. Here each component of H, $\mathbf{x}$, $\mathbf{s}$ is taken from $\mathbf{GF}(2)$. The encoder is defined by $\mathbf{x} \leftarrow \{\mathbf{x} : H\mathbf{x} = \mathbf{s}\}$, which means $\mathbf{x}$ is randomly chosen from the set $\{\mathbf{x} : H\mathbf{x} = \mathbf{s}\}$ under a uniform distribution. The decoder is simply:

$$f^{-1}(\mathbf{x}) = H\mathbf{x} \tag{4}$$

To find a good H, [11] looks at the generation matrix G of $\mathcal{C}$. Let $\mathbf{y}$ be the output of the erasure channel. Let G_e be formed by the columns of G that corresponds to the erased positions. Define F_0 as a binary random variable such that $F_0 = 1$ denote the event that G_e has full column rank. Then it was shown in [13] [11, Theorem 2] the following result holds:

Theorem 2: $I(\mathbf{s};\mathbf{y}|F_0 = 1) = 0$

Remark 1: Note that this theorem holds even if the encoder only uses a subset of all possible input sequences. □

We next evaluate the probability $\Pr(F_0 = 0)$. To make $\Pr(F_0 = 0)$ small, [11] proposes to use the parity check matrix H_L of a good LDPC code $\mathcal{C}_L$ for binary erasure channel as G. It can be shown that $\Pr(F_0 = 0)$ can be bounded via the decoding error probability P_e of $\mathcal{C}_L$ as $\Pr(F_0 = 0) \le 2P_e$. In [14, Theorem 6], a lower bound is provided on the error exponent $-\frac{1}{L}\log_2 P_e$. By evaluating [14, (43)], we find that the expurgated regular $(3, 4)$ LDPC code ensemble, whose rate is $1/4$, has a positive error exponent on average when the channel erasure probability is $1/2$. Hence there must exists a $(3, 4)$ LDPC code that the decoding error probability decreases exponentially fast with code length. The corresponding wire-tap code has rate $1/4$. Let L be the length of the wire-tap code. Then $\Pr(F_0 = 0)$ can be bounded as:

$$\Pr(F_0 = 0) < \exp(-L\alpha) \tag{5}$$

for some positive $\alpha > 0$.

D. Simulating a Binary Erasure Channel

In order to leverage the linear wire-tap code from Section III-C, we have to simulate a binary erasure channel in both the adder model and the Gaussian model. In the adder model, this could be done simply by restricting the transmitted signal to be binary. Doing so leads to a significant rate loss. However, since only $\{x, h\}$ needs to be transmitted in this fashion, as we will see later, the overall rate loss is negligible.

In the Gaussian model, we use every N channel use to simulate 1 channel use in a binary erasure channel via a simple repetition code. Note that this leads to the loss of coding gain and to an arbitrarily small rate. However, since we only use this scheme to transmit $\{x, h\}$, which also has an arbitrarily small rate, the overall rate loss will be shown to be small as well in the sequel.

The relaying and the signaling scheme under the repetition code is described as following: Let $\mathbf{1}$ denote an n-bit vector of ones. Let $\mathbf{0}$ denote an n-bit vector of zeros. Node 1 sends $\sqrt{P}\mathbf{1}$ as 1 and $-\sqrt{P}\mathbf{1}$ as 0. Node 2 sends $\sqrt{P}\mathbf{1}$ or $-\sqrt{P}\mathbf{1}$ with equal probability. Let u_i^N be the signal transmitted by node i. Define $\oplus$ over $\{-\sqrt{P}\mathbf{1}, \sqrt{P}\mathbf{1}\}$ so that this set forms a modulus 2 group $G(2)$. Define $\mathbf{I}_1$ as the isomorphism from $\{\sqrt{P}\mathbf{1}, -\sqrt{P}\mathbf{1}\}$ to $G(2)$.

The relay node receives receives $u_1^N + u_2^N + Z_r^N$, which is a vector from the set $\{-2\sqrt{P}\mathbf{1}, \mathbf{0}, 2\sqrt{P}\mathbf{1}\}$ corrupted by Gaussian noise. Note that this is a degraded version of $u_1^N + u_2^N$. Hence if a wire-tap code supports the notion of secrecy as in Theorem 2, the same result holds here as well due to data processing inequality. This means that, we can design the wire-tap code assuming the adversary receives $u_1^N + u_2^N$ instead. Note that if $u_1^N + u_2^N = \mathbf{0}$, then the conditional probability distribution of the signal transmitted by node 1 is the same as this distribution without the conditioning. Hence an *erasure* has occurred.

The relay scheme is composed of the following two steps:

1) It uses a maximum likelihood detector to determine $\{-2\sqrt{P}\mathbf{1}, \mathbf{0}, 2\sqrt{P}\mathbf{1}\}$.
2) It transmits $-\sqrt{P}\mathbf{1}$ if it detects $-2\sqrt{P}\mathbf{1}$ or $2\sqrt{P}\mathbf{1}$. It transmits $\sqrt{P}\mathbf{1}$ if it detects $\mathbf{0}$.

Node 2 uses a maximum likelihood detector to determine whether the relay transmits $-\sqrt{P}\mathbf{1}$ or $\sqrt{P}\mathbf{1}$. Let the detection result be u_r^N. It then recovers the binary bit sent by node 1 from $\mathbf{I}_1(u_r^N) \oplus \mathbf{I}_1(u_2^N)$. If the relay is honest and all decoding operation is successful, it should equal $\mathbf{I}_1(u_1^N)$. Their difference is given by

$$\mathbf{I}_1\left(u_r^N\right) \oplus \mathbf{I}_1\left(u_1^N \oplus u_2^N\right) \tag{6}$$

Note that u_r^N is computed from the received signal by the relay node Y_r^N and the noise Z_R^N. $\mathbf{I}_1\left(u_1^N \oplus u_2^N\right)$ can be computed from Y_r^N as well if the detection operation at the relay is successful. With the repetition code, the detection error probability decreases exponentially fast with N. As we have shown in Section III-C, with high probability Y_r^N is independent from the confidential message $\{x, h\}$ conveyed by the linear wire-tap code. Hence, with high probability (6) is independent from $\{x, h\}$.

IV. Main Results

The overall achievability scheme can then be summarized as follows: A string of confidential messages s is first encoded into an AMD code tuple $\{s, x, h\}$, which is transmitted in two stages:

1) During the first stage, $\{x, h\}$ is transmitted using the linear wire-tap code in Section III-C via the simulated Type II wire-tap channel described in Section III-D. The transmission is done via the two phase protocol described in Section II.
2) During the second stage, s is transmitted using a randomly generated wire-tap code and the two phase protocol described in Section II. This wire-tap code from [9] is nonlinear but offers a higher rate.

Let the overall number of channel uses be N_T. Let R_e denote the achievable *strong* secrecy rate for these two models when the relay is honest. For the discrete adder model, it can shown that $R_e = H(X_1) - I(X_1; X_1 + X_2)$ which equals 0.5 when $B = 2$ and is lower bounded by $\log_2 B - 0.8$ in general. For the Gaussian model, it can be shown that combining lattice code [12] and the wiretap code from [9], $R_e = \left[\frac{1}{2}\log_2(\frac{1}{2} + P) - 1\right]^+$. [1]

Remark 2: The reason for using lattice codes in the Gaussian model is in effect to avoid the continuous channel outputs in the Gaussian case. This is needed in order to apply the result of [9]. Also note that we can not use the approach in [15] to achieve strong secrecy as [15] requires transmitting a negligible amount of random bits via an *authenticated* public channel for privacy amplification. In our case, all bits must be transmitted via the relay, which is *not* authenticated. □

[1] Due to the half duplex constraints, rates should be multiplied by the time sharing factor $1/2$.

Theorem 3: For the discrete adder channel in Section II, for a rate smaller but arbitrarily close to R_e, there exists $\alpha_i > 0, i = 1, 2$ such that

1) When the relay is honest, data can be reliably transmitted at this rate with the mutual information between the adversary's knowledge and the confidential message decreases at the rate of $O(\exp(-\alpha_1 N_T))$.
2) The probability that a counterfeit message is accepted by node 2 decreases at the rate of $O(\exp(-\alpha_2 N_T))$

Theorem 4: For the Gaussian model in Section II, for a rate smaller but arbitrarily close to R_e: Then there exists $\alpha_i > 0, i = 3, 4, 5$ such that

1) When the relay is honest, data can be transmitted at the rate such that the mutual information between the adversary's knowledge and the confidential message decreases at the rate of $O(\exp(-\alpha_3 N_T^{1/2}))$. The error probability decreases at the speed of $O(\exp(-\alpha_4 N_T^{1/2})$.
2) When the relay is not honest, the probability that a counterfeit message is accepted by node 2 decreases at the rate of $O(\exp(-\alpha_5 N_T^{1/2}))$.

V. Proofs of the Main Results

The following notation is used: $X_i(j), i = 1, 2, X_r(j)$ denote the signals transmitted by node $1, 2$ and the relay during the jth stage, $j = 1, 2$. Similarly, $Y_i(j), i = 1, 2,\ Y_r(j)$ denote the signals received during the jth stage.

Note that in order to use AMD code, as shown in Theorem 1, we need to prove x is almost independent from $\{\Delta_h, \Delta_x, s, s'\}$. Define F as a binary random variable such that $F = 1$ indicates that (1) the relay node can decode the binary modulus sum of the signals transmitted by node 1 and 2 during stage one and (2) the binary linear wire-tap code does not leak information. Then for the discrete adder model, $\Pr(F = 0)$ is bounded by (5), since the channel is noiseless. For the Gaussian model, let γ denote the error exponent of the detection operation. Then $\Pr(F = 0)$ can be bounded as:

$$\Pr(F = 0) \leq L \exp(-N\gamma) + \exp(-L\alpha) \tag{7}$$

where L is the length of the binary wiretap code described in Section III-C. The first term in (7) is the union bound on the probability that any detection operation at the relay or node 2 is not successful. The second term comes from the imperfectness of the linear wire-tap code. For both models, we have the following lemma:

Lemma 1: $I(x; \Delta_h, \Delta_x, s, s') \leq m \Pr(F = 0)$

Proof Outline:

$$\begin{aligned}
&I(x; \Delta_h, \Delta_x, s, s') \leq I(x; \Delta_h, \Delta_x, s, s', F) && (8)\\
=&I(x; \Delta_h, \Delta_x, s, s'|F) && (9)\\
=&\Pr(F = 1) I(x; \Delta_h, \Delta_x, s, s'|F = 1)\\
&+ \Pr(F = 0) I(x; \Delta_h, \Delta_x, s, s'|F = 0) && (10)
\end{aligned}$$

(9) is due to the fact that F is solely determined by $X_2(1)$ and the structure of the code. Hence $I(x, F) = 0$. The second term in (10) is upper bounded by $m \Pr(F = 0)$. For the first term, we have:

$$\begin{aligned}
&I(x; \Delta_h, \Delta_x, s, s'|F = 1) && (11)\\
=&I(x; \Delta_h, \Delta_x, s'|F = 1, s) + I(x; s|F = 1) && (12)\\
=&I(x; \Delta_h, \Delta_x, s'|F = 1, s) && (13)\\
\leq&I(x; Y_r(1), \Delta_h, \Delta_x, s'|F = 1, s) && (14)\\
=&I(x; Y_r(1), s'|F = 1, s) && (15)\\
\leq&I(x; Y_r(1), Y_2(2), X_2(2), s'|F = 1, s) && (16)\\
=&I(x; Y_r(1), Y_2(2), X_2(2)|F = 1, s) && (17)
\end{aligned}$$

(15) is because based on (3) and (6), we observe that, conditioning on $F = 1$, $\{\Delta_x, \Delta_h\}$ can be computed from $Y_r(1)$ by the relay. (17) is due to the fact s' can be computed from $Y_2(2), X_2(2)$ by node 2. It can then be shown that (17) equals 0. For details, the reader is referred to [16]. ■

In the following, 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:

$$\begin{aligned}
&\Pr(A\ wins)\\
=&\sum_{\substack{x,\Delta_x\\ \Delta_h,s,s'}} \begin{array}{l}\Pr(\text{HRH}|x, \Delta_h, \Delta_x, s, s')\\ \Pr(x|\Delta_h, \Delta_x, s, s') \Pr(\Delta_h, \Delta_x, s, s')\end{array} && (18)
\end{aligned}$$

Define Q as the term (18) with $\Pr(x|\Delta_h, \Delta_x, s, s')$ replaced by $\Pr(x)$. Then we have

Lemma 2:

$$|\Pr(A\ wins) - Q(A\ wins)| \leq \sqrt{(2\ln 2)m \Pr(F = 0)} \tag{19}$$

Proof: The right hand side of (19) is bounded by:

$$\sum_{\substack{x,\Delta_x\\ \Delta_h,s,s'}} \left(\begin{array}{l} |\Pr(x|\Delta_h, \Delta_x, s, s') \Pr(x)\\ - \Pr(x) \Pr(\Delta_h, \Delta_x, s, s')| \end{array} \right) \tag{20}$$

Then we use Pinsker's inequality:

$$I(A; B) \geq \frac{1}{2\ln 2} D^2(p(A, B), p(A)p(B)) \tag{21}$$

where $D(p(x), q(x)) = \sum_x |p(x) - q(x)|$. Let A be x. Let B be $\Delta_h, \Delta_x, s, s'$. Then, applying Lemma 1 leads to Lemma 2. ■

From Theorem 1, $Q(A\ wins)$ is bounded by $\frac{d+1}{2^m}$. Hence, using Lemma 2, we have

$$\Pr(A\ wins) \leq \frac{d+1}{2^m} + \sqrt{(2\ln 2)m \Pr(F = 0)} \tag{22}$$

To prove Theorem 3 and Theorem 4, it remains to apply (22) to the two models we considered, as will be done next.

A. The Discrete Adder Model (Theorem 3)

For the adder model, (22) is given by

$$\Pr\left(A\ wins\right) \leq \frac{d+1}{2^m} + \sqrt{m}\exp(-L\alpha') \tag{23}$$

where α' is chosen to be within the range $0 < \alpha' < \alpha/2$. Now choose the length of information bits in the linear wire-tap code as the length of x and h. This means $L/4 = 2m$. The number of channel uses needed to transmit s is slightly larger than $\frac{dm}{R_e}$, where R_e is defined in Section IV. Hence the total number of channel uses needed to transmit $\{s, x, h\}$ bits is given by $8m + \frac{dm}{R_e}$. This means the overall transmission rate converges to $d/(8 + d/R_e)$, which can be made arbitrarily close to R_e by making d sufficiently large.

For a given rate and hence fixed d, the total number of channel uses is proportional to m. From (23), we see that the probability that the adversary wins decreases exponentially fast with the total number of channel uses.

Finally, we check the secrecy constraint. The wire-tap code from [9] offers the following strong notion of secrecy:

$$I\left(s; Y_r\left(2\right)\right) < \exp\left(-\beta L'\right) \tag{24}$$

where $L' = md/R_e$ is the length of the wire-tap code. Hence:

$$\begin{aligned} I\left(s; Y_r\left(1\right), Y_r\left(2\right)\right) &\leq I\left(s, x, h; Y_r\left(1\right), Y_r\left(2\right)\right) && (25)\\ \leq& I\left(x, h; Y_r\left(1\right)\right) + I\left(s; Y_r\left(2\right)\right) && (26)\\ =& m\exp\left(-8m\alpha\right) + \exp\left(-\beta md/R_e\right) && (27)\end{aligned}$$

(26) is due to the fact that the channel and the signal transmitted by node 2 are both memoryless. (27) follows from Theorem 2 and (24). Hence for a given rate, the mutual information between the confidential message and the observation of the eavesdropper also decreases exponentially fast with the total number of channel uses.

B. The Gaussian Model (Theorem 4)

For the Gaussian model, (22) is given by

$$\frac{d+1}{2^m} + \sqrt{\left(2\ln 2\right) m \left(L\exp\left(-N\gamma\right) + \exp\left(-L\alpha\right)\right)} \tag{28}$$

Let N_2 denotes the number of channel uses during the second stage. Then the total number of channel uses is $N_T = N_2 + LN$. Let R'_e is the rate of the randomly generated wire-tap code per channel use. To match the rate with an AMD tuple of $(d+2)m$ bits, We require $R'_e(N_2) = dm$ and $\frac{L}{4} = 2m$, where 4 in the denominator comes from the fact we are using a rate $1/4$ linear wiretap code. Let N_L be the dimension of the lattice code used in stage two. Let γ_L is the error exponent of the lattice code decoder. Then, with the wire-tap code from [9], it can be shown that R'_e can be chosen to be any value smaller than $(1 - e^{-\gamma_L N_L})R_e - e^{-\gamma_L N_L} - 1/N_L$ [16]. Transmission below this rate will allow the decoding error probability at node 2 to decrease exponentially fast with respect to $N_2/N_L = dm/(N_L R'_e)$. The overall rate per channel use is given by

$$R_{overall} = \frac{dm}{N_2 + LN} = \frac{d/N}{\frac{d/N}{R'_e} + 8} \tag{29}$$

When d/N and N_L is sufficiently large, $R_{overall}$ can be made arbitrarily close to R_e. If we fix d/N and let $k = d/N$, then the total number of channel uses is given by $mN\left(8 + \frac{k}{R'_e}\right)$. Let $m = N$. Then $N_T \sim O(m^2)$. It can be verified by checking (28) that $\Pr\left(\mathrm{A\ wins}\right)$ decreases exponentially fast with respect to m. It remains to check the secrecy constraints: The L' in (24) is given by $N_2/N_L = km^2/(N_L R'_e)$. Hence $I\left(s; Y_r\left(1\right), Y_r\left(2\right)\right) = me^{-8m\alpha} + e^{-\frac{\beta km^2}{N_L R'_e}}$. Hence if we choose $N_L = m$, then it decreases exponentially fast with respect to m. The decoding error probability of the wire-tap code used to transmit s decreases exponentially fast with respect to $O(dm/(N_L R'_e)) = O(m)$.

VI. Conclusion

In this work, we have considered a source-destination pair that communicates via a relay node. The relay node is an eavesdropper and a Byzantine attacker. For the adder model, we showed that the probability that the adversary wins decreases exponentially fast with respect to the total number of channel uses N_T. For the Gaussian two-hop model, we showed that that the probability that the adversary wins decreases exponentially fast with respect to $\sqrt{N_T}$. For both models, the loss in rate due to Byzantine detection is arbitrarily small.

References

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

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

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

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

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

[6] E. Ekrem and S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. submitted to IEEE Trans. on Info. Theory, October, 2008.

[7] X. He and A. Yener. Two-hop Secure Communication Using an Untrusted Relay. Submitted to EURASIP Journal on Wireless Communication and Networking, December, 2008.

[8] L. Lai, H. El-Gamal, and H. V. Poor. Authentication over Noisy Channels. to appear in IEEE Trans. on Info. Theory, 2008.

[9] I. Csiszar. Almost independence and secrecy capacity. *Problems of Info. Transmission*, 32(1):48–57, 1996.

[10] 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.

[11] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.M. Merolla. On the application of LDPC codes to a novel wiretap channel inspired by quantum key distribution. *IEEE Trans. on Info. Theory*, 53(8):2933–2945, August 2005.

[12] X. He and A. Yener. Providing Secrecy with Lattice Codes. *Allerton Conf. on Communication, Control, and Computing*, September 2008.

[13] L. H. Ozarow and A. D. Wyner. Wire-tap channel. II. *AT & T Bell Laboratories technical journal*, 63(10):2135–2157, 1984.

[14] D. Burshtein and G. Miller. Asymptotic enumeration methods for analyzing LDPC codes. *IEEE Trans. on Info. Theory*, 50(6):1115–1131, June 2004.

[15] J. Barros and M. Bloch. Strong Secrecy for Wireless Channels. *International Conf. on Info.-Theoretic Security*, August 2008.

[16] X. He and A. Yener. Secure Communication in the Presence of a Byzantine Relay. to be submitted to IEEE Trans. on Info. Theory.