SECURE NETWORK CODING

Ning Cai
ShanghaiTech University

Email: cai@gmx.de

Beyond I.I.D. in Information Theory
IMS, NUS, Singapore

July 25, 2017

CONTENTS

1. Basic Model
2. Extensions and Alternative Models
3. Recent Results

CONTENTS

1. Basic Model
2. Extensions and Alternative Models
3. Recent Results

- Basic Model
- 3 well known special cases
- The Basic Results

Communication network

- A (directed) Graph $\mathbf{G} = (\mathbf{V}, \mathbf{E})$: nodes-users, edges-channels (noiseless);
- A subset of source nodes in $\mathbf{V}$ access to source with message set $\mathbf{M}$;
- A subset of destinations $\mathbf{U} \subset \mathbf{V}$, accessed by receivers;
- The network is acyclic, if $\mathbf{G}$ has no directed cycle.
- The goal is to send as much as possible message from source node to receivers reliably. Coding may improves the transmission.

Wiretap network (C. and Yeung 2002, 2011)

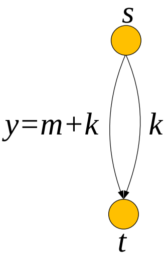
- Communication network;
- A collection of subsets of wiretap channels $\mathbf{B}$: i.e., $\mathbf{B}$ is a collection of subsets of the channels such that all $B \in \mathbf{B}$ may be fully accessed by a wiretapper, but no wiretapper may access more than one wiretap subsets;
- We call a single source acyclic wiretap network $r-$WN, if B is $r-$ subsets of channels i.e., the wiretapper may arbitrarily choose r channels and accesses them.
- The goal is transmitting the message reliably and securely;
- For security generating randomness is necessary, which will reduce throughput.

Secure network code

Fix a network code. Let $k, k^{'}$ be the outputs of the randomness. For $B \in \mathbf{B}$, denote by Y_B, the output of channels in B. Then the code is secure if

- $\forall m \neq m^{'}, u \in U, \psi_u(m^{'}, k^{'})$ for all $k, k^{'}$, where ψ_u is is the message received by sink u, Decodable Condition;
- For all wiretap subsets B, (or in the worst case for the legal communicators) the information leak to the wiretapper $I(M; Y_B) = 0$, (Perfect) Security Condition (or $I(M; Y_B) \leq i$, for $0 \leq i \leq H(M)$, Imperfect Security Condition).

Well known special case I: Shannon Cipher System



- Random message M and key K are generated on the same set $\{0, 1, \cdots, p-1\}$.
- m -output of the message of M
- k -output of key K
- $y = m + k(mod\ p)$

Well known special case II: Secret Sharing

- There are a dealer and n participants in the game.
- The dealer observes a secret message and randomly chooses "sharings" and sends them to participates.
- A subset of participates try to recover the message by pooling their sharings.
- They can recover it if the subset is legal (i.e. in "access structure").
- Otherwise they should have absolutely no information about it from their sharings.
- A secret sharing with n participates is call (r, n)-threshold secret sharing scheme, if exactly all r subsets are legal.

(Blakley 1979, Shamir 1979)

SS is equivalent to a special class of WN. Given an SS with access structure A , we construct a 3 layer WN as follows:

- Top layer: source node S (the dealer);
- Middle layer: n intermediate nodes i(participates): a channel with capacity r_i connects S and the node i if the node i gets r_i bits of sharing;
- Bottom layer: Receivers labeled by members in A (legal subsets); The intermediate node connect to receiver t_A if $i \in A$;
- A wiretap set of channels corresponds an illegal subset B, and has members $(s, b), b \in B$.
- Then existence of secure code for the WN is equivalent to existence of the SS scheme. A (r, n) threshold secret sharing scheme ”is” a $(r - 1)$-secure network code.

Secret sharing is a special WN

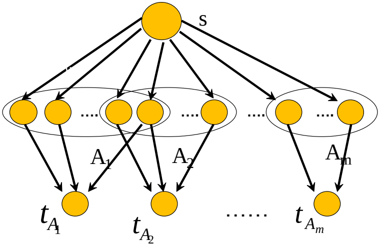


Figure 1.1: Formulating secret sharing schemes to WN

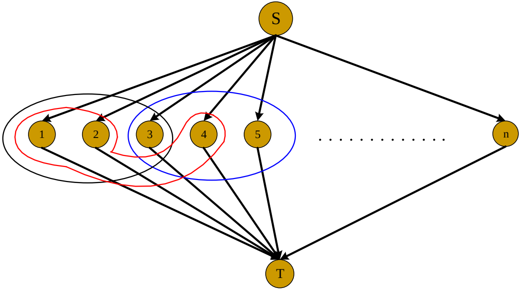
Well known special case III: wiretap channel II

The wiretap channel II (Ozarow-Wyner 1984)

- Message is encoded into a codeword of length n;
- A legal user receives the whole codeword;
- A wtiretapper may access any t components of the codeword;
- The legal user can decode correctly;
- The illegal user has no information about the message (perfect security), more general the “equivocation” (conditional entropy) is lower bounded (imperfect security).
- The optimal code is known (R-S code), (for perfect security, optimal rate: $n - t$).
- Denote the code by (n, t)-WCII.

Wiretap channel is a special WN II

Obviously, (n, t)-WCII. is equivalent to a 3 layer t-WN with a sink and n intermediate nodes.



The Basic Results

- Every decodable linear NC can be linearly transformed to a secure network code by a matrix constructed in P time , provided the coding field is sufficiently large (C.-Yeung 2002).
- The construction of the matrix is equivalent to a coding problem (Feldman et al, 2004).
- For r-WN the code is optimal in the sense to maximize the throughput and minimize the size of random key (Yeung-C. 2008).
- Secure network coding for WN has been extended to imperfect security i.e., replacing the security condition by imperfect security condition $I(M; Y_A) \leq i$ for $0 \leq i \leq H(M)$ and optimal codes for r-WN have been constructed (C.-Yeung 2011, Rouayheb-Soljanin-Sprintson, Ngai-Yeung-Zhang 2009).

CONTENTS

1 Basic Model

2 Extensions and Alternative Models

3 Recent Results

Extensions and Alternative Models

- Necessary and sufficient conditions for security of NC have been found (C.-Yeung, 2007, Zhang-Yeung 2009, C. 2008). By the conditions random network code is secure if the field is sufficiently large (C.,2009).
- To analyze the imperfect secure code for wiretap channel II, Wei introduced generalized Hamming weight of linear codes, this has been extended to secure network coding (Ngai-Yeung-Zhang 2009).
- Algorithms with low complexity over small fields (X. Guang 2016).

Extensions and Alternative Models

- Using the universal hashing lemma to show the existence of universal secrecy code against any type of wiretappers under size constraint (R. Matsumoto and M. Hayashi, 2011; J. Kurihara, R. Matsumoto, and T. Uyematsu 2013).
- Secure network coding was also extended to multiple source network coding (C. 2009).

Extensions and Alternative Models

- Multiple Wiretap (Chan-Grant 2008): Let $M_1, M_2, \cdots, M_j$ be messages of (multiple) sources and W be set of wiretappers. For $w \in W$, fix $A_w \subset 2^E, B_w \subset \{1, 2, \cdots, j\}$ and assume w can access any subset of channels in A_w and wants to have information about the messages $\{M_i : i \in B_w\}$. An inner bound and an outer bound of capacity region of secure codes in terms of Γ^*.

In this case sometimes no random key is needed even for perfect security (C.-Chan,2011).

Extensions and Alternative Models

- Weak security was introduced, for which the wiretapper is no able to decode any part of source message. No additional resource is needed (Bhattad-Narayanan, 2005).
- Strongly secure network codes was introduced and its optimal codes have been constructed. It in fact contained weak secure network code as its special case (Harada and H. Yamamoto, 2008).
- An algebraic security of random linear network codes (Lima te al, 2007).
- A alternative criterion, the cost criterion, was introduced (Tan-Medard, 2006).
- **Many more** . . . . . .

CONTENTS

1. Basic Model
2. Extensions and Alternative Models
3. Recent Results

- Active Attack
- Relay Network

Active Attack (Joint Work with M. Hyayshi at el)

- Traditionally the wiretapper (Eve) is only allowed to read the outputs of the channels accessed by her, but may not change them. Let us call the attack passive attack.
- Now, we assume that Eve is more powerful:
  - her attack is according to the encoding order;
  - she may not only read its output, but also change the output, when she accesses a channel.

  We call it active attack.

Question: Can Eve do better by applying an active attack?

Answer 1: No, if a linear network is employed.

Reason: Errors are linearly additive, if a linear network code is applied in a network. Thus, Eve may figure out the changing at a downstream channel, caused by the changing of the output of a upstream channel. So she can “simulate” the changing at downstream channels, without changing the outputs of an upstream channels. That is, changing makes no difference.

Answer 2:Yes, an active attack may possibly improve the performance, if the code is non-linear.

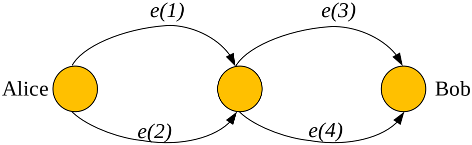


Figure 3.1: An example for the active attack

Alice: sends a binary secrete message M to Bob;
generates a binary randomness L to protect M.
Eve: chooses one of $\{e(1), e(3)\}, \{e(1), e(4)\}, \{e(2), e(3)\}$ and $\{e(2), e(4)\}$ to access.
Denote by Y_i, the output of $e(i)$.

A Coding Scheme: on $GF(2)$

$Y_1 = L, Y_2 = L + M, Y_3 = Y_1(Y_1 + Y_2), Y_4 = (Y_1 + 1)(Y_1 + Y_2)$

That is,

- Sending L via $e(1)$, $L + M$ via $e(2)$ (Shannon Cipher System)
- sending 0 via $e(3)$ and sending M via $e(4)$ if $e(1)$ outputs 0
  sending M via $e(3)$ and sending 0 via via $e(4)$ if $e(1)$ outputs 1.

Bob: Uniquely decodable

$(Y_3, Y_4) = (0, 0) \Rightarrow M = 0$;

$(Y_3, Y_4) = (1, 0) \Rightarrow M = 1$;

$(Y_3, Y_4) = (0, 1) \Rightarrow M = 1$;

$(Y_3, Y_4) = (1, 1)$ never occurs.

Passive attack vs Active attack

- *Passive attack:* $I(M;Y_1,Y_3) = I(M;Y_1,Y_4) = I(M;Y_2,Y_3) = I(M;Y_2,Y_4) = \frac{1}{2}$. No mater with subset of channels Eve takes, she is no able to recover M with probability one.
- *Active attack:* Eve first accesses $e(1)$ and changes $Y_1 = 0 \Rightarrow 1;\ 1 \Rightarrow 1$ such that $e(1)$ always outputs 1. As a consequence, $e(3)$ always outputs M. Then she accesses $e(3)$ and decodes M successfully, with probability one.
- With active attack, Eve may get more!

More results:

- In the same network, there is no binary secure code may successfully protect the message from active attack;
- In the same network, when sizes of alphabets are $3, 4, \ldots$, constructing codes by “anti-Latin square”, to protect message from active attack;
- *secrecy and the robustness Code:* Let the transmission rate from Alice to Bob is m_0, the rate of “errors” injected by Eve is m_1, and the rate of information leakage to Eve is m_2. Then $m_0 - m_1 - m_2$ is achievable by codes with vanishing probability of error and information leak to Eve.

Open problem:

- We have known that in the above network, by active attack Eve may do better than passive attack for binary alphabet but she may not do better when the alphabet size larger than 2;
- We also have known that the properties of network codes is strongly related to alphabet sizes and the most ‘good” network codes need a sufficiently large alphabet/field;
- What is the relation between the types of attacks and the alphabet sizes, in particular whether there is a WN such that for any d_0, there is a $d \geq d_0$ such that Eve can improve her performance by applying active attack when the alphabet size is d.

Relay Network (joint a work with M. Hyayshi)

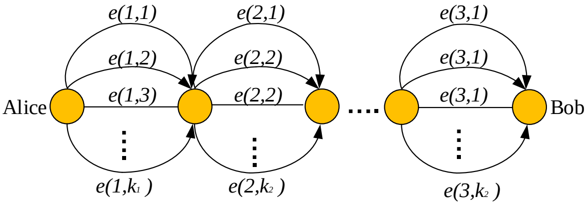


Figure 3.2: The relay network

- Alice and Bob are connected by l groups of relay channels, and all channels in the i group have capacity γ_i. Denote the output of jth channel in the ith group, by $Y_{i,j}$.

- Alice encodes for and sends message via the first group of channels, she is allow to generate unlimited randomness;
- The $i-1$st relay node encodes for and sends message via the ith group of channels, and he may at most generate κ_i unites of randomness;
- Eve may access any r_i channels in the ith group, for every i. (for passive attack)
- Denote $\bar{Y}_i = (Y_{i,1}, Y_{i,2} \ldots, Y_{i,k_i})$, $Y_{i,s_i} := (Y_{i,j}, j \in s_i)$ for r_i subset s_i of the ith group of channels.
- The goal is to send as much as possible message from Alice to Bob, under the (perfect security)condition:

$$I_W = max_{s_1 \times s_2 \ldots \times s_l} I(M; Y_{l,s_l}, Y_{l-1,s_{l-1}}, \ldots, Y_{2,s_2}, Y_{1,s_1}) = 0,$$

where the "max" is taken over all r_i subsets s_i of the ith group of channels, for all i.

For $i = 0, 1, 2, \ldots, l$, we define $h_i^i := k_i\gamma_i$; and for $a = i + 1, i + 2, \ldots, l$, $h_i^a := \min\{k_a\gamma_a, \frac{k_{a-1}-r_{a-1}}{k_{a-1}}h_i^{a-1} + \kappa_a\}$, recursively.

Theorem:

(i) For all relay code sending h unites of message from Alice to Bob, $I_W \geq h - \min_{1\leq a\leq l} \frac{k_a - r_a}{k_a} h_1^a$. Consequently for a perfect secure code,

$$h \leq \min_{1\leq a\leq l} \frac{k_a - r_a}{k_a} h_1^a.$$

(ii) There exists a perfect secure code sending

$$h := \min_{1\leq a\leq l} \frac{k_a - r_a}{k_a} h_1^a$$

unites of secrete message from Alice to Bob, on all sufficiently large field, in the case that $\underline{\gamma}_i := \frac{h_1^a}{k_a}, a = 1, 2, \ldots, l$ are integers.

(i) The Outline of the converse proof:

We let Eve randomly independently and uniformly chooses S_i from $\binom{[k_i]}{r_i}$ for $i = 1, 2, \ldots, l$, and use $\mathbb{E}H(M|Y_{l,S_l}, \ldots, Y_{2,S_2}, Y_{1,S_1})$ to upper bound $\min_{s_1 \times s_2 \ldots \times s_l} H(M|Y_{l,s_l}, Y_{i-1,s_{l-1}} \ldots, Y_{2,s_2}, Y_{1,s_1})$, where $\mathbb{E}$ is expectation with respect to the random sets $S_i, i = 1, 2, \ldots, l$. To upper bound $\mathbb{E}H(M|Y_{l,S_l}, \ldots, Y_{2,S_2}, Y_{1,S_1})$, we need to prove that for $1 \leq i \leq b \leq l$,

$$\mathbb{E}H(M|Y_{l,S_l}, Y_{l-1,S_{l-1}} \ldots, Y_{2,S_2}, Y_{1,S_1})$$
$$\leq \frac{k_b - r_b}{k_b}\mathbb{E}H(\bar{Y}_b|Y_{b-1,S_{b-1}}, \ldots, Y_{2,S_2}, Y_{1,S_1}),$$

and

$$\mathbb{E}H(\bar{Y}_b|Y_{b-1,S_{b-1}}, Y_{b-2,S_{b-2}}, \ldots, Y_{2,S_2}, Y_{1,S_1})$$
$$\leq \frac{k_{b-1} - r_{b-1}}{k_{b-1}}\mathbb{E}H(\bar{Y}_{b-1}|Y_{b-2,S_{b-2}}, \ldots, Y_{2,S_2}, Y_{1,S_1}) + \kappa_b.$$

Based on the second inequality on the last slide and the trivial inequality

$$\mathbb{E}H(\bar{Y}_a|Y_{a-1,S_{a-1}},\dots,Y_{2,S_2},Y_{1,S_1})\leq H(\bar{Y}_a)\leq k_a\gamma_a$$

we show

$$\mathbb{E}H(\bar{Y}_a|Y_{a-1,S_{a-1}},\dots,Y_{2,S_2},Y_{1,S_1})\leq h_1^a$$

by induction on a. Then by combining the above inequality with the first inequality (by setting $b=a$) on the last slide, we obtain

$$\mathbb{E}H(M|Y_{l,S_l},Y_{l-1,S_{l-1}}\dots,Y_{2,S_2},Y_{1,S_1})\leq\frac{k_a-r_a}{k_a}h_1^a.$$

Thus, the converse part of the theorem follows.

The outline of direct proof;

Let $h := \min_{1\leq a\leq l} \frac{k_a - r_a}{k_a} h_1^a$ and $\underline{\gamma}_i := \frac{h_1^a}{k_a}, a = 1, 2, \ldots, l$ be integers.

- Alice generates $h_1^1 - h$ unites of randomness and sends it with M of h unites (totally h_1^1 unites) via the first group of channels by (k_1, r_1)-WCII (a code for wiretap channel II), to keep M and $\frac{k_1 - r_1}{k_1} h_1^1 - h$ unites of randomness (totally $\frac{k_1 - r_1}{k_1} h_1$ unites) in secrete from Eve, and other part of randomness is "insecure". Here each channel carries one components of the codeword (with rate $\underline{\gamma}_1 \leq \gamma_1$);

- For $i = 1, 2, \ldots, l-1$, the ith relay node receives M (of h unites), $\frac{k_i - r_i}{h_1^i} h_1^i - h$ unites of "secure randomness" and $h_1^i - \frac{k_i - r_i}{h_1^i} h_1^i$ unites of "insecure randomness" from the ith group of the channels. Then he discards "the insecure" part of randomness, uniformly generates $h_1^{i+1} - \frac{k_i - r_i}{k_i} h_1^i \leq \kappa_{i+1}$ unites of randomness and send it with M and the "secure randomness" received by him, by applying (k_{i+1}, r_{i+1})-WCII to keep M and $\frac{k_{i+1} - r_{i+1}}{h_1^{i+1}} h_1^{i+1} - h$ unites of randomness in secrete.
- To continue the procedure, until Bob receives M and $h_1^l - h$ (secure and insecure) randomness, who discards all randomness and decodes M.
- By information inequalities, one may show the code is perfect secure.

The theorem has 2 consequences in the extremal cases:

Corollary 1

Assume that no relay node is allow to generate randomness.

(1) If there is a perfect secure code sending h unites of secrete message from Alice and Bob, then $h \leq min_{1\leq i\leq l}\prod_{j=i+1}^{l}\frac{k_j-r_j}{k_j}(k_i-r_i)\gamma_i$.

(2) On the other hand, if $\frac{h_1^i}{k_i}$ is an integer for every i, there is a perfect secure code sending h unites of secrete message from Alice and Bob, with

$$h = min_{1\leq i\leq l}\prod_{j=i+1}^{l}\frac{k_j-r_j}{k_j}(k_i-r_i)\gamma_i,$$

provided that the coding field is sufficiently large.

Corollary 2

Assume that all relay nodes are allow to generate unlimited randomness.

(1) If there is a perfect secure code sending h unites of secrete message from Alice and Bob, then

$$h \leq min_{1 \leq i \leq l}(k_i - r_i)\gamma_i.$$

(2) On the other hand, if γ_i is an integer for very i, there is a perfect secure code sending h unites of secrete message from Alice and Bob, with

$$h = min_{1 \leq i \leq l}(k_i - r_i)\gamma_i,$$

provided the coding field is sufficiently large.

We also have the capacity region for the following homogeneous multicast relay network:

- The network has one source node, b (legal) user nodes and $c-1$ groups of relay nodes. We regard the source and user nodes as in the 0th and cth groups resp.;
- The capacities of all channels are one unite;
- Each node of the $i-1$st group is connected to every node of the ith group by k_i channels (totally $b_{i-1}b_ik_i$ channels);
- Eve may access any r_i of $b_{i-1}k_i$ incoming channels of each node in the ith group;
- Only the source node (Alice) may generate randomness.

Thank You!