

# Secure Coding over Networks

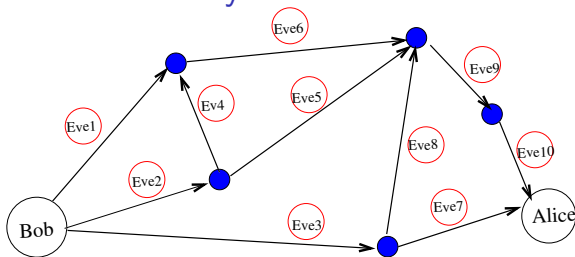
Jin Xu

Advisor: Biao Chen

Syracuse University

2009 School of Information Theory

## System Model



- ▶ Uni-cast: acyclic single-source single-sink planar network.
- ▶ Transmit both confidential message  $S$  and public(key) message  $K$ .
- ▶ Each link is subject to non-cooperating eavesdropping.
- ▶ Each link is modelled as noisy/noiseless wiretap channel.
- ▶ **Task:** determine the rate group  $(R_c, R_k, R_{e,io})$ ,  $(i, o) \in \mathcal{E}$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log |S^n| = R_c; \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log |K^n| = R_k; \quad \lim_{n \rightarrow \infty} \frac{1}{n} H(S^n | Z_{io}^n) \geq R_{e,io}.$$

## Related Work: Over Single Link

- ▶ Noiseless case: **Shannon (1949)**
  - ▶ Measure  $\bar{S}$  from information theoretic viewpoint,  $H(S|Z)$ .
  - ▶ One-time pad: perfect secrecy  $H(S) = H(S|Z)$  only if  $H(K) \geq H(S)$ .
- ▶ Noisy case: **Wyner (1975)**
  - ▶ Wiretap Channel: security from physical layer.
  - ▶ Random coding over noisy channel,  $\frac{1}{n}H(S^n|Z_{io}^n)$ .

$$C_s = \max_{U \rightarrow X \rightarrow YZ} (I(U; Y) - I(U; Z))$$

- ▶ Variations to the Wiretap Channel
  - ▶ **Wyner's Wiretap channel (1975)**: degraded broadcast channel with a confidential message  $S$ .
  - ▶ **Csiszár and Körner (1978)**: general broadcast channel with a confidential message  $S$  and a common message  $C$ .
  - ▶ **Xu and Chen (2008)**: general broadcast channel with a confidential message  $S$  and a public message  $K$ .

## Related Work: Over Multiple Links

- ▶ Cooperating eavesdropping over parallel links
  - ▶ [Li-Yates-Trappe'06, Liang-Poor-Shamai'07, Liu-Prabhakaran-Vishwanath'08]: parallel/compound Gaussian wiretap channels with cooperating eavesdropping.
- ▶ Non-Cooperating eavesdropping over parallel links
  - ▶ [Yamamoto'86, '89, '91]: secret sharing system.
  - ▶ [Xu-Chen'08]: transmit confidential and **public(key)** messages.
- ▶ Non-Cooperating eavesdropping over networks
  - ▶ [Cai-Yeung'02]: eavesdropping an **arbitrary** subset of unit-capacity edges.
    - ▶ Multi-cast noiseless network.
    - ▶ Existence of linear network code (LNC).
  - ▶ [Feldman-Malkin-Stein-Servedio'04, ElRouayheb-Soljanin'07]: restrict eavesdropping edge subset to **r-size** subset of edges.
    - ▶ Efficient algorithms to find the LNC.

## Main Result: Noiseless Case, $X_{io} = Y_{io} = Z_{io}$

### Theorem

The rate tuple for a planar graph network,  $(R_c, R_k, R_{e,io})$ ,  $(i, o) \in \mathcal{E}$ , is achievable, if there exist auxiliary numbers  $r_{io}$  such that

$$0 \leq r_{io} \leq C_{io};$$

$$r_{io} \leq R_c + R_k;$$

$$0 \leq R_{e,io} \leq R_c;$$

$$0 \leq R_c + R_k \leq \min_{Cut} \sum_{(i,o) \in (IO)_{cut}^l} r_{io};$$

$$R_{e,io} \leq R_c + R_k - r_{io}.$$

*Cut is defined as a cut of this network.*

## Interpretation of Result

- ▶  $r_{io}$  is viewed as the bits transmitted via the present edge  $(i, o)$ .
- ▶ The transmitted bits can not exceed the present edge's capacity.
- ▶ The transmitted bits come from the confidential and key message and thus can not exceed the total rate.
- ▶  $R_{e,io}$  can not exceed the confidential message rate  $R_c$  itself.
- ▶ Total throughput can not exceed the network capacity:  
Max-flow Min-cut Theorem.
- ▶  $R_{e,io}$  is bounded by the bits which are not transmitted via the present edge.

# Proof of Result

- ▶ An algorithmic approach
  - ▶ Explicit encoding/decoding and network routing scheme.
  - ▶ Instead of linear algebra or randomly selected codes arguments.
- ▶ Rely on planar graph assumption
  - ▶ Edges in network intersect only at their nodes.
- ▶ Ford-Fulkerson + Shannon Cipher system (One-time pad).
  1. One-time pad
    - ▶ modulo-2 addition of the confidential and key message bits.
  2. Modified Ford-Fulkerson algorithm
    - ▶ construct the set of virtually parallel paths.
  3. Assign the bit sequence to the corresponding path set.

## Step 1: One-time pad

- ▶ The key and confidential message bits are

$$\{k_1, k_2, \dots, k_{nR_k}\} \quad \{b_1, b_2, \dots, b_{nR_c}\}$$

- ▶ After modulo addition,  $c_1, c_2, \dots, c_{nR_c+nR_k}$  is

$$\begin{aligned} & \{k_1, k_2, \dots, k_{nR_k}, \\ & b_1 \oplus k_1, b_2 \oplus k_2, \dots, b_{nR_k} \oplus k_{nR_k}, \\ & b_{nR_k+1} \oplus k_1, b_{nR_k+2} \oplus k_2, \dots, b_{nR_k+nR_k} \oplus k_{nR_k}, \\ & \dots, b_{nR_c-1} \oplus k_{(nR_c-1)_{nR_k}}, b_{nR_c} \oplus k_{(nR_c)_{nR_k}} \} \end{aligned}$$

- ▶ Any contiguous length- $r$  segment of the bit sequence  $\mathbf{c}$  has the property that

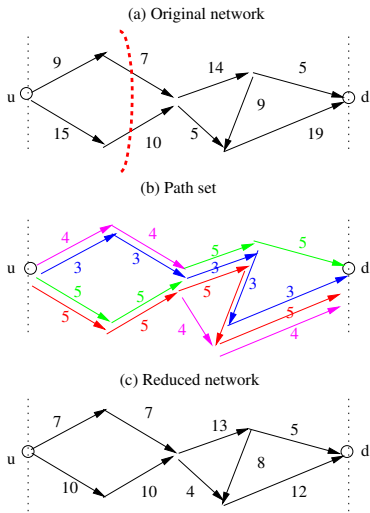
$$H(\mathbf{b} | c_j, c_{j+1}, \dots, c_{j+r-1}) = \min(nR_c, n(R_c + R_k) - r).$$

How to make bits transmitted over each link is a contiguous segment of  $\mathbf{c}$ ?

## Step 2: virtually parallel paths(1)

### Revisit Ford-Fulkerson Algorithm

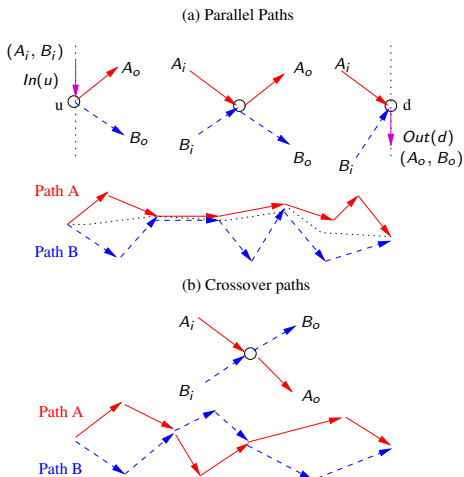
- ▶ A 'greedy' approach to find a set of paths.
- ▶ Routing: assign bits according to the path set.
  - ▶ achieve the maximum flow in a network.
- ▶ The path set constructs a **reduced network**.
  1. The sum flow of the input and output edges of any node are equal.
  2. Any cut in the reduced network is equal to the min-cut value of the original network.



## Step 2: Virtually parallel paths(2)

### How to find virtually parallel path set

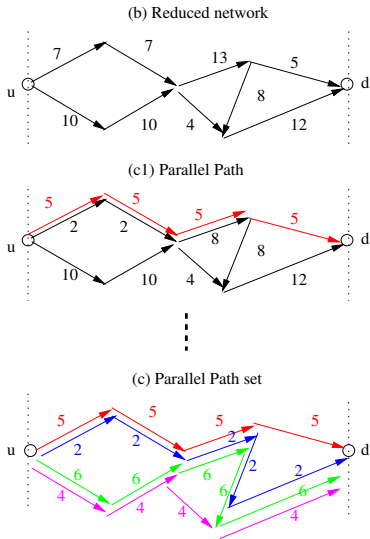
- ▶ Define the order of path.
  - ▶ parallel path
  - ▶ crossover path
- ▶ Planar graph assumption.
- ▶ Modified Ford-Fulkerson Algorithm.



## Step 2: Virtually parallel paths(3)

### Modified Ford-Fulkerson Algorithm

- ▶ A 'greedy' algorithm to find such virtually parallel path set
  - ▶ based on reduced network.
  - ▶ iterative step to find highest paths.
- ▶ Assign the bit sequence  $\mathbf{c}$  to the paths successively.
  - ▶ Bits over each link is a contiguous segment of  $\mathbf{c}$ .
  - ▶ Desired equivocation rate is achieved.
  - ▶ Total throughput achieves the min-cut value at the same time.



# Implication of Result

- ▶ Without secrecy constraint
  - ▶ an alternative expression of Max-flow Min-cut theorem

$$\begin{aligned}0 &\leq r_{io} \leq R_c + R_k; \\r_{io} &\leq C_{io}; \\0 &\leq R_c + R_k \leq \min_{Cut} \sum_{(i,o) \in (IO)_{cut}^l} r_{io}.\end{aligned}$$

- ▶ Coupling to the work of [Cai-Yeung'02].
  - ▶ Define the eavesdropping set to be the set of every individual link.
  - ▶ Perfect secrecy, set  $R_{e,io} = R_c$ .

# Main Result: Noisy Case, $P(Y_{io}Z_{io}|X_{io})$

## Theorem

The rate tuple for a planar graph network,  $(R_c, R_k, R_{e,io})$ ,  $(i, o) \in \mathcal{E}$ , is achievable, if there exist auxiliary numbers  $r_{io}$  and random variables  $U_{io} \rightarrow V_{io} \rightarrow X_{io} \rightarrow Y_{io}Z_{io}$  such that

$$0 \leq r_{io} \leq R_c + R_k;$$

$$0 \leq R_{e,io} \leq R_c;$$

$$0 \leq R_c + R_k \leq \min_{Cut} \sum_{(i,o) \in (IO)_{cut}^l} r_{io};$$

$$r_{io} \leq I(V_{io}; Y_{io}|U_{io}) + \min(I(U_{io}; Y_{io}), I(U_{io}; Z_{io}));$$

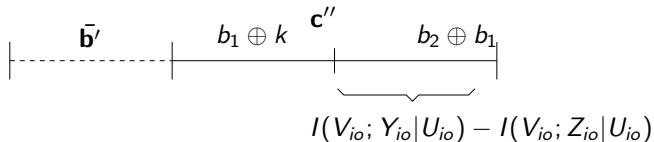
$$R_{e,io} \leq [I(V_{io}; Y_{io}|U_{io}) - I(V_{io}; Z_{io}|U_{io})]^+ + R_c + R_k - r_{io};$$

- ▶ Random coding and one-time pad contribute to the equivocation rate in an additive manner.

## Sketch proof of Noisy Case

- ▶ Decode-Forward coding scheme
  - ▶ The result in noiseless case can be directly adopted.
- ▶ Apply random coding over wiretap channel to each edge.
- ▶ It is optimal for parallel links, [Xu-Chen'08].

## Sketch proof of Noisy Case



- ▶ Assume some edge  $(i, o)$  is required to transmit  $\mathbf{c}' = (b_1 \oplus k, b_2 \oplus k)$ .
  - ▶  $\mathbf{b}' = (b_1, b_2)$ ,  $\mathbf{b} = (\mathbf{b}', \bar{\mathbf{b}}')$ .
- ▶ Convert  $\mathbf{c}'$  to  $\mathbf{c}'' = (b_1 \oplus k, b_2 \oplus b_1)$ .  $\mathbf{c}' \Leftrightarrow \mathbf{c}''$
- ▶ Apply random coding to protect  $b_2 \oplus b_1$  part of  $\mathbf{c}''$ .

$$H(\mathbf{b} | Z_{io}^n) = H(\mathbf{c}'' | Z_{io}^n) + H(\mathbf{b} | \mathbf{c}'') - H(\mathbf{c}'' | \mathbf{b}', Z_{io}^n)$$

# Conclusion

- ▶ Secure communication over a single-source single-sink acyclic planar network with noisy/noiseless links.
- ▶ Non-cooperating eavesdropping: an achievable region found.
  - ▶ An algorithmic approach: an explicit intuitive coding scheme.
- ▶ It builds up the connection to known result for various special cases.