

# Robust Operations Research I: Introduction & Communication Networks

Yvo Desmedt  
BT Chair of  
Information Security  
University College London  
UK

March 6, 2006

Yvo Desmedt was also partially supported by NSF CCR-0209092, EPSRC EP/C538285/1 and DARPA F30602-97-1-0205. He is also a courtesy professor at Florida State University (USA).

# OVERVIEW

1. Introduction
2. What do routers do?
3. Denial of service during communication: the issues
4. Point-to-point: a  $t$ -bounded adversary: introduction
5. A  $t$ -bounded adversary: small error
6. A  $t$ -bounded adversary: no error
7. Adversary structure
8. Finding the network graph while under attack
9. Partial broadcast: a survey
10. Conclusions

# 1. INTRODUCTION

The October 1997 US report of the President's Commission on Critical Infrastructure Protection identified the following areas as critical:

1. Information and Communications,
2. Electrical Power Systems,
3. Gas and Oil Transportation and Storage,
4. Banking and Finance,
5. Transportation,
6. Water Supply Systems,
7. Emergency Services, and
8. Government Services.

**Obviously**, it lacks, for example, the agricultural and food distribution



sector, the pharmaceutical industry, mechanical manufacturing sector (as pointed out by the author, e.g. on March 5, 1998).

To understand the approach used to identify the Critical Infrastructures, consider the list of commissioners:

- Robert T. Marsh, *Chairman*
- John R. Powers, *Executive Director Federal Emergency Management Agency*
- Merritt E. Adams *AT&T*
- Richard P. Case *IBM*
- Mary J. Culnan *Georgetown University*
- Peter H. Daly *Department of the Treasury*
- John C. Davis *National Security Agency*
- Thomas J. Falvey *Department of Transportation*
- Brenton C. Greene *Department of Defense*
- William J. Harris *Association of American Railroads*
- David A. Jones *Department of Energy*
- William B. Joyce *Central Intelligence Agency*
- David V. Keyes *Federal Bureau of Investigation*

- Stevan D. Mitchell *Department of Justice*
- Joseph J. Moorcones *National Security Agency*
- Irwin M. Pikus *Department of Commerce*
- William Paul Rodgers, Jr. *National Association of Regulatory Utility Commissioners*
- Susan V. Simens *Federal Bureau of Investigation*
- Frederick M. Struble *Federal Reserve Board*
- Nancy J. Wong *Pacific Gas and Electric Company*

Source: PCCIPreport.pdf (<http://www.pccip.gov> WWW page exists no longer)

We find:

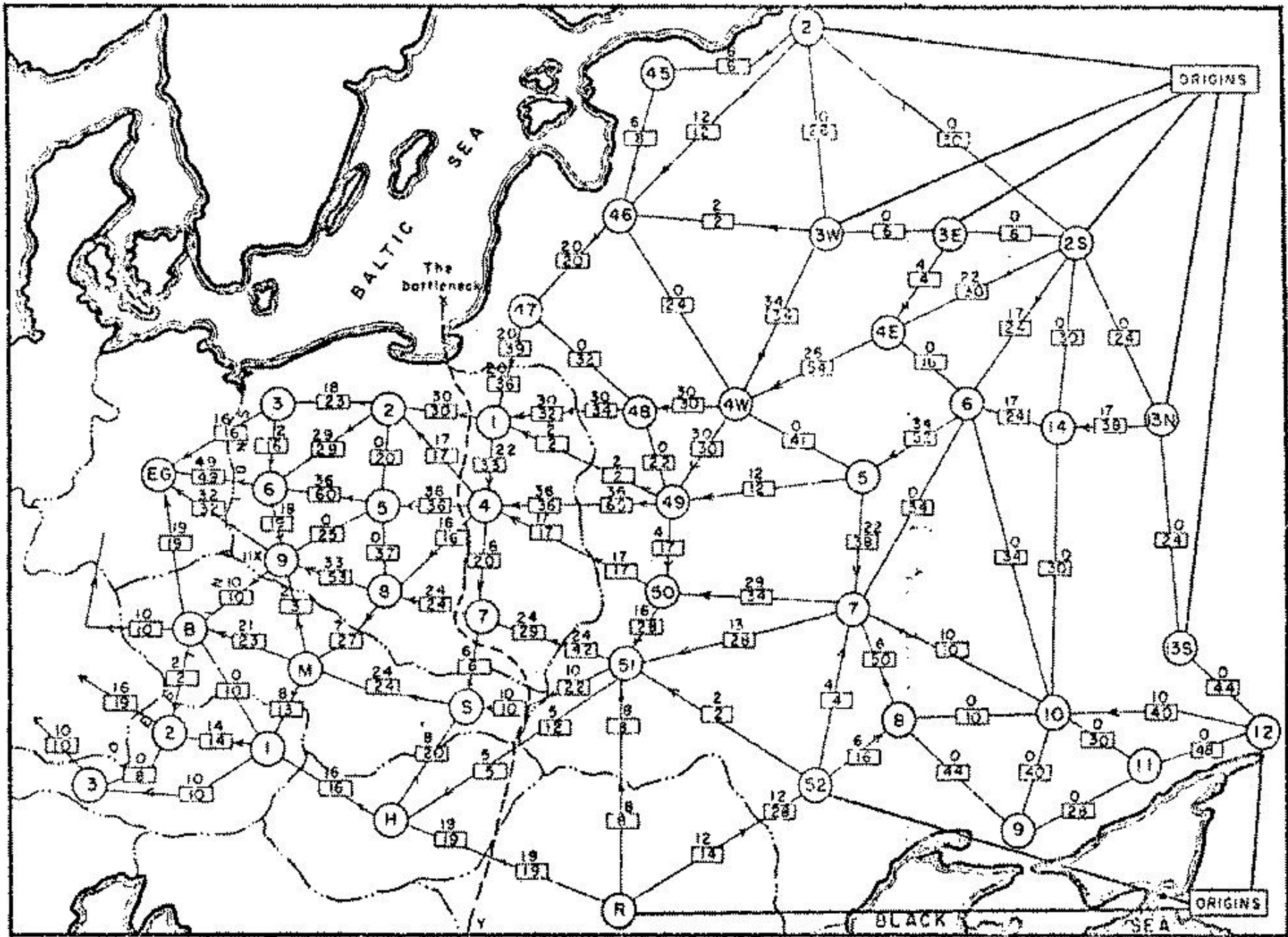
there was almost a one-to-one mapping between the background of the commissioners and the areas identified

Such an approach to identify the critical infrastructures is clearly unacceptable!

## The main questions we address:

- to find **scientific** methods to identify which infrastructures are critical,
- to find **scientific** approaches to study the robustness of critical infrastructures
- to find **scientific** methods to design robust critical infrastructures.

We first consider some historical examples.



In the **1950s**, Harris-Ross, of the US Air Force, analyzed the rail network that linked the Soviet Union to its satellite countries in Eastern Europe using graph theory. They used it to evaluate the maximum flow of goods via rail from the Soviet Union to Eastern Europe and which rail links to blow up to disrupt the network.

Sources: e.g., Alexander Schrijver, “On the history of the transportation and maximum flow problems” October 26, 2001. It states:

the interest of Harris and Ross was not to find a maximum flow, but rather a minimum cut

For actual and earlier denial of services, see:





Accordingly to:

<http://www.catalogue.nationalarchives.gov.uk/Leaflets/ri2026.htm>

On 5 August 1914, the cable ship **Telconia** lifted from the bed of the North Sea the German overseas telegraph cables. Thereafter German diplomatic communications had to go by wireless, as did signals to the High Seas Fleet and the U boats. These could be intercepted and so were sent by cypher. Cryptography had been subject to a lot of study in Britain before the War, particularly at Naval Intelligence Department, and as a result, specialists at NID were able to read many of Germany's diplomatic and operational signals.

During the 3 lectures we will focus on the robustness of:

- Communication Networks (and the like)
- Production Networks
- Operations (in general)

## 2. WHAT DO ROUTERS DO?

We only discuss this at a high level.

They primarily:

- construct an edge-labeled graph (label: e.g. label: delay) of the network, and
- route communication packages.

Traditional algorithms to construct the graph do not assume the existence of untrusted routers. They can deal with routers that are down.

### 3. DENIAL OF SERVICE DURING COMMUNICATION: THE ISSUES

There are several issues, depending on:

**The type of network.** We distinguish:

**Point-to-point networks**

**(Partial) broadcast**

**The type of adversary.** We have:

**Passive adversary** has control to a subset of nodes. The adversary has access to all information received by these nodes (and all secrets of these nodes).

**Active adversary.** The nodes over which the adversary has control



can behave in a Byzantine way. This means they can decide, not to forward information, modify, not follow the protocol, follow the protocol, etc.

**Destroyed nodes**, i.e. just stops communicating.

**Jamming adversary** in the case of (partial) broadcast, a third party can prevent communication between two parties.

**The nodes controlled by the adversary.** These can be specified by a **threshold**. A  $t$ -bounded adversary can control up to  $t$  nodes.

**an adversary structure.** Let  $V$  be the nodes in the network. An adversary structure  $\mathcal{A}_V$  over  $V$  is a subset of the power set  $2^V$  such that if  $B \in \mathcal{A}_V$  then subsets of  $B$  are also in  $\mathcal{A}_V$ .

**The level of security.** We distinguish between:

**Perfect** (see further).

**$\delta$ -reliability**, i.e. with probability at least  $1 - \delta$ ,  $B$  terminates with the same message as  $A$  sent.

**$\varepsilon$ -privacy**. Unconditional security (See literature: Franklin-Wright.)

Edge: considered private communication.

The perfect case corresponds to  $\delta = 0$  and  $\varepsilon = 0$ .

**Decisional versus search.** We distinguish between:

**Decisional questions:** given a network, does it allow the desired security against a type of adversary? So, issues are:

- necessary and sufficient conditions
- if possible, what protocol do the participants run
- an algorithm for deciding, or
- proving the problem is hard (e.g. **NP**-hard).

**Computational questions** , in particular:

**Construct a network** for the desired security against a type of adversary with parameters, e.g. number of nodes is given.

Issues:

**Bounds:** Necessary conditions



## **Constructions:** Sufficient conditions

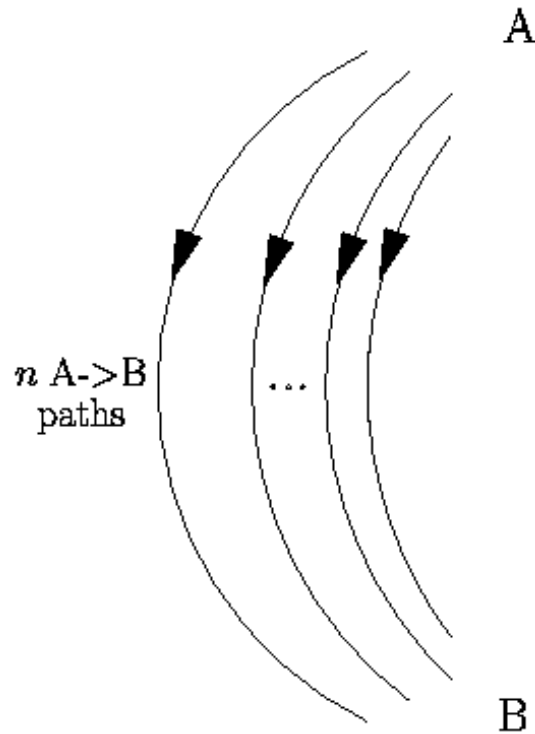
**Update a network.** Start from existing network (satisfying a security property). How to update it (with minimum “cost”) so it satisfies a (new) security property?

## 4. POINT-TO-POINT: A $t$ -BOUNDED ADVERSARY: INTRODUCTION

If an adversary can **destroy  $t$  nodes**, then  **$t + 1$  vertex disjoint (directed) paths** are needed and sufficient to communicate from node  $A$  to node  $B$ . If any two non-destroyed nodes want to communicate, it is necessary and sufficient that the directed graph must be strongly  $t + 1$  connected.

If the **adversary can be Byzantine**, then one needs  **$2t + 1$  vertex disjoint (directed) paths**, respectively  $2t + 1$  strong connectivity.

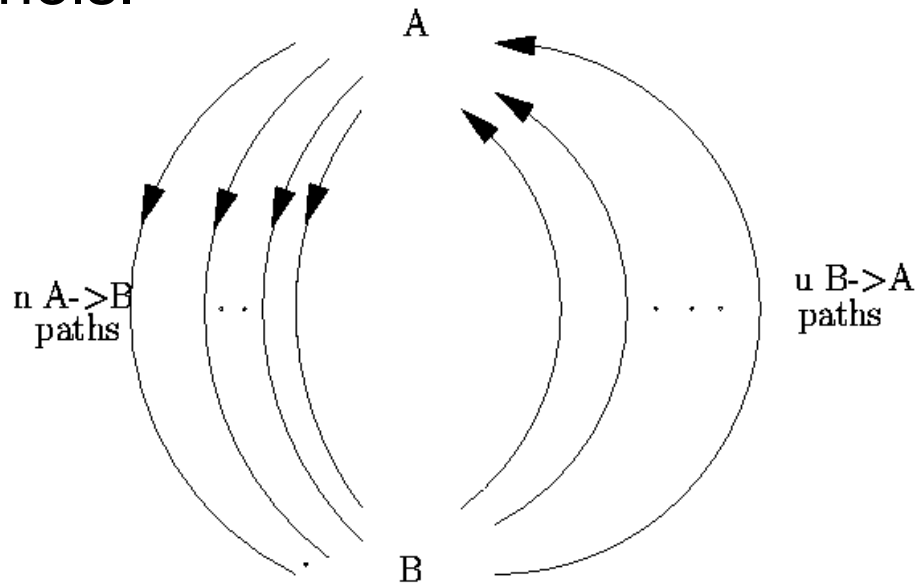
Dolev-Dwork-Waarts-Yung (1993) **added privacy** and studied the cases **all communication links** (edges in the graph) are:



**one-way without feedback.** It is necessary and sufficient to have  $3t + 1$  **vertex disjoint directed paths** from  $A$  to  $B$  (for any two nodes: the graph must be  $3t + 1$  connected).

**two-way.**  $2t + 1$  vertex disjoint paths are necessary and sufficient.

Desmedt and Wang (2002) observed this is not the most general case, since there **could be feedback channels**. They focussed primarily on the case the feedback channels are vertex disjoint from the forward channels.



## 5. POINT-TO-POINT: A $t$ -BOUNDED ADVERSARY: SMALL ERROR

The receiver may accept an incorrect message with  $\delta$  probability (any  $0 < \delta < 1/2$ ).

No feedback:

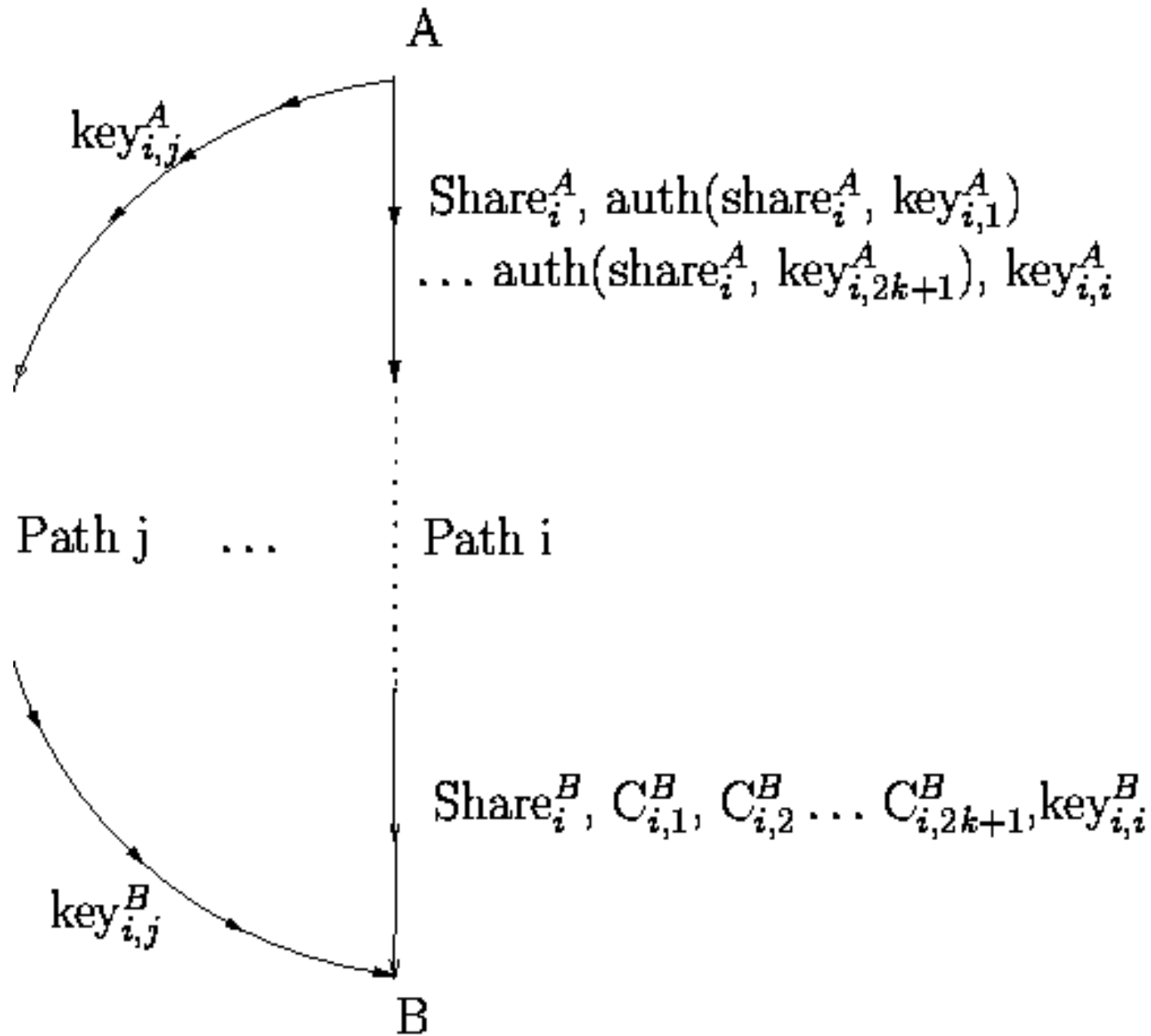
Call sender  $A$  and receiver  $B$ .

required:  $2k + 1$  vertex disjoint paths (Franklin-Wright).

Claim:  $2k + 1$  is sufficient.

**Protocol**  $A$  makes shares from the secret using a  $k + 1$ -out-of- $2k + 1$  perfect secret sharing scheme. Then:

For each  $i$  ( $1 \leq i \leq 2k + 1$ ), for each  $j$ :



If  $|\{C_{i,j}^B : C_{i,j}^B = \text{auth}(\text{Share}_i^B, \text{key}_{i,j}^B)\}| \geq k + 1$ , then  $B$  accepts  $\text{Share}_i^B$ . Then from accepted shares  $B$  reconstructs the secret.

**Theorem 1.** Gives perfect privacy,  $\delta$  reliability, by choosing proper authentication code.

**Feedback:** Assume  $u$  disjoint feedback channels (i.e. from  $B$  to  $A$ ).

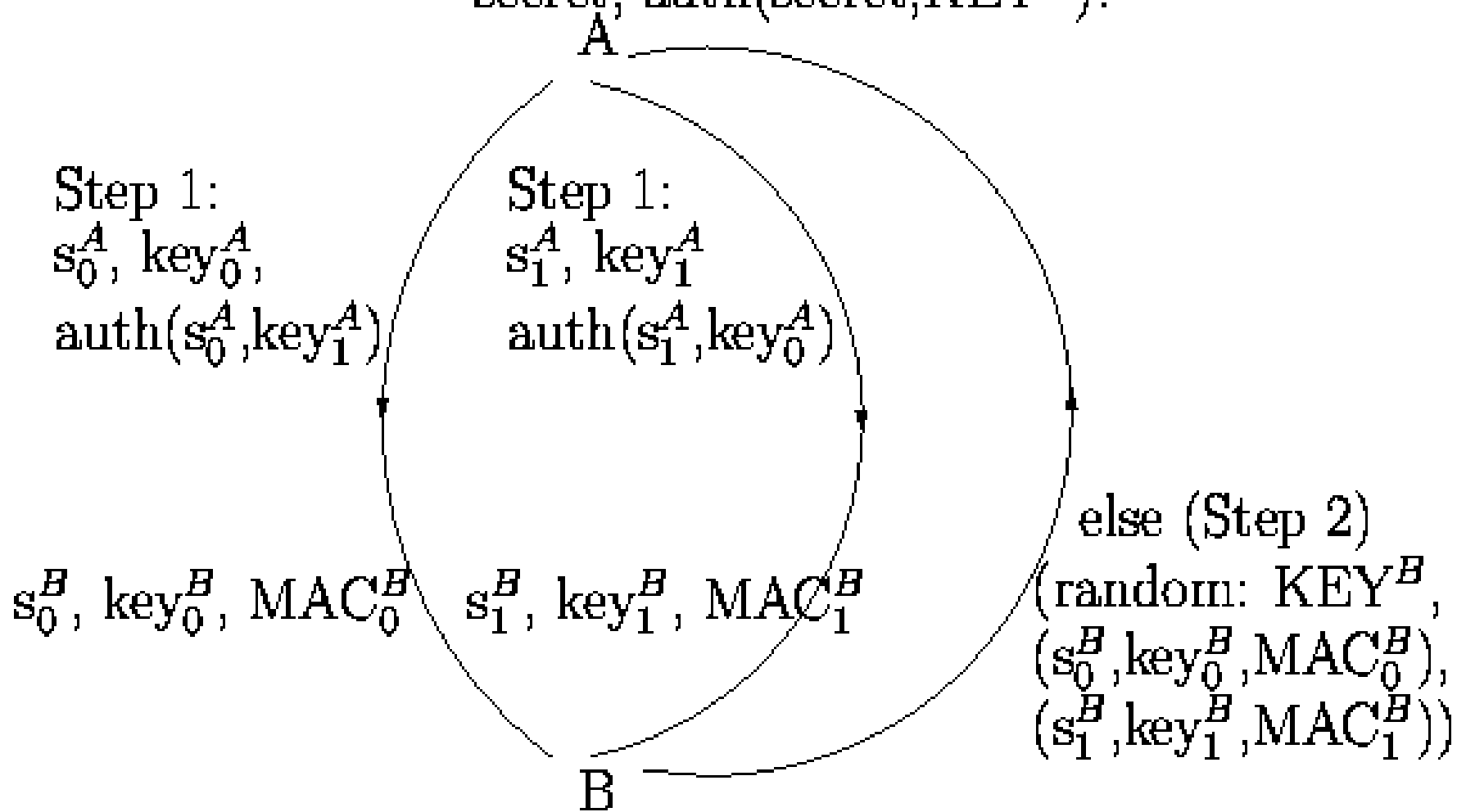
**Corollary 1.** *(Follows from Franklin-Wright) Necessary conditions:*

- *# vertex-disjoint  $A \rightarrow B$  paths  $\geq k + 1$ .*
- *#disjoint  $A \rightarrow B$  paths + #disjoint  $B \rightarrow A$  paths  $\geq 2k + 1$ .*

**Theorem 2.** *There exists an efficient protocol when there are  $2k + 1 - u$  disjoint  $A \rightarrow B$  paths that are also disjoint from the  $B \rightarrow A$  paths (for any  $u, 1 \leq u \leq k$ ).*

Explain here: case  $u = 1$  and  $k = 1$ .

Step 3: A decides which A  $\rightarrow$  B path is honest and sends:  
secret,  $\text{auth}(\text{secret}, \text{KEY}^A)$ .



Step 2:  
If both auth correct then "end"

## 6. A $t$ -BOUNDED ADVERSARY: NO ERROR

i.e.  $\delta = 0$

**Theorem 3.** *It is necessary to have: # vertex-disjoint  $A \rightarrow B$  paths*

- $\geq 2k + 1$ , and
- $\geq 3(k - u) + 1$ ,

**Theorem 4.** *There exists an efficient protocol when there are  $3k + 1 - u$  disjoint  $A \rightarrow B$  paths that are also disjoint from the  $B \rightarrow A$  paths (for any  $u$ ,  $0 \leq u \leq k$ ).*

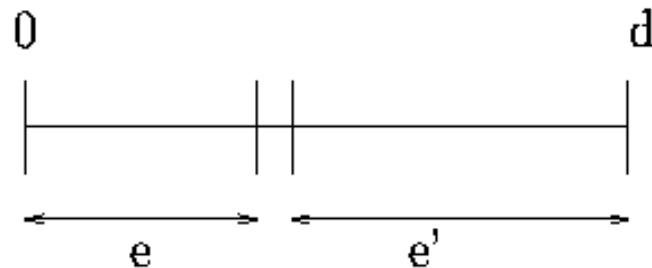
**Lemma 1.** *Let:*

- $e$  be the # errors that can be corrected,
- $e' \geq e$  be the # errors that can be detected **simultaneously**, and
- $d$  be the minimum distance of the code.

*Then the necessary and sufficient conditions are that:*

$$e \leq \lfloor \frac{d-1}{2} \rfloor, \quad \text{and} \quad e + e' \leq d - 1.$$

**Proof:**



□



We use MDS-code as a perfect secret sharing,

$k + 1$ -out-of- $3k + 1 - u$  (input: secret +  $k$  random values). We call this an MDS secret sharing. Note:

$$d - 1 = 3k + 1 - u - (k + 1) = 2k - u = (k - u) + k.$$

For simplicity we focus on the case  $u = 1$ , i.e.  $3k$  disjoint  $A \rightarrow B$  paths and 1  $B \rightarrow A$  path, disjoint from the  $A \rightarrow B$  path.

## Protocol (sketch)

**Step 1**  $A$  sends share $_i$  of  $key$  via  $A \rightarrow B$  path  $i$ .

**Step 2** From the “shares”  $B$  detects whether  $\#errors \leq k - u$ . **If, then**  $B$  corrects and send  $A$  STOP, **else** ask help to  $A$  (by sending back all “shares”).

**Step 3** **If**  $A$  receives STOP,  $A$  stops, **else**  $A$  finds “dishonests”  $A \rightarrow B$  path and reliably sends this to  $B$ .

**Step 4** **If**  $B$  found key **then** ignore step, **else**  $B$  finds  $key$  from honest shares.

**Step 5**  $key$  used to send message from  $A$  to  $B$ .

## General protocol (rough sketch)

**Step 1** Split key into  $R_0, R_1$ .  $A$  sends share $_i$  of  $R_0$ .

**Step 2** If # errors  $\leq k - u$ , then  $B$  recovers  $R_0$ , else  $B$  asks  $A$ 's help (note:  $A$  may receive  $u$  different versions of "help", but one is correct).

**Step 3**  $A$  sends share $_i$  of  $R_1$ .

**Step 4** If # errors  $\leq k - u$ , then  $B$  recovers  $R_1$ , else  $B$  asks  $A$ 's help if not asked before, else (assuming  $k'$  dishonest  $A \rightarrow B$  have been identified) restart from Step 1 using  $(k + 1)$ -out-of- $3k + 1 - u - k'$  MDS secret sharing however it will be used to detect errors only.

**Corollary 2.** *Can be extended to allow that of the  $3k + 1 - u$   $A \rightarrow B$*



*paths only  $3k + 1 - 2u$  are node disjoint from the  $u$   $B \rightarrow A$  paths.*

**Corollary 3.** *(New) If there are  $2k + 1$  disjoint  $A \rightarrow B$  paths and  $k + 1$  disjoint  $B \rightarrow A$ , then these do not have to be mutually disjoint.*

Results improved recently (Wang-Desmedt, unpublished):

**Theorem 5.** *Assume that there are  $u$  directed node disjoint paths from  $B$  to  $A$ , vertex disjoint from the forward channels. Then a **necessary and sufficient** condition for private message transmission from  $A$  to  $B$  against a  $t$ -active adversary is that there are  $\max\{3t + 1 - 2u, 2t + 1\}$  directed node disjoint paths from  $A$  to  $B$ .*

## 7. ADVERSARY STRUCTURE

Let  $V$  be the nodes in the network. An **adversary structure**  $\mathcal{A}_V$  over  $V$  is a subset of the power set  $2^V$  such that if  $B \in \mathcal{A}_V$  then subsets of  $B$  are also in  $\mathcal{A}_V$ .

If  $\mathcal{Z}_1$  and  $\mathcal{Z}_2$  are adversary structures for  $P$ , then

$$\mathcal{Z}_1 + \mathcal{Z}_2 = \{Z_1 \cup Z_2 : Z_1 \in \mathcal{Z}_1, Z_2 \in \mathcal{Z}_2\},$$

which is also an adversary structure for  $P$ .

$2\mathcal{Z}$  and  $3\mathcal{Z}$  indicate  $\mathcal{Z} + \mathcal{Z}$  and  $\mathcal{Z} + \mathcal{Z} + \mathcal{Z}$  respectively.

**Definition 1.** Let  $G(V, E)$  be a directed graph,  $A, B$  be nodes in  $G(V, E)$ , and  $\mathcal{Z}$  be a an adversary structure on  $V \setminus \{A, B\}$ .

- $A, B$  are called  $\mathcal{Z}$ -separable in  $G$ , if there is a set  $Z \in \mathcal{Z}$  such that all paths from  $A$  to  $B$  go through at least one node in  $Z$ . We say that  $Z$  separates  $A$  and  $B$ .
- $A, B$  are called  $(\mathcal{Z} + 1)$ -connected if they are not  $\mathcal{Z}$ -separable in  $G$ .

A necessary and sufficient condition for  $A$  and  $B$  to privately communicate in the presence of a Byzantine adversary, in the case **all communication links** (edges in the graph) are:

**two-way** is that  $A, B$  are  $(2\mathcal{Z} + 1)$ -**connected** in  $G$   
(Kumar-Goundan-Srinathan-Rangan, 2002).

**one-way without feedback**, is that  $A, B$  are  $(3\mathcal{Z} + 1)$ -**connected** in  $G$   
(Desmedt-Wang-Burmester, 2005: see further).

The **general case, i.e. with feedback channels** has **not** been studied.

## passive adversary

Desmedt-Wang-Burmester, 2005 observed the results of Franklin-Yung (related to partial broadcast) can easily be adapted to general adversary structure, i.e.

- a connectivity of  $\mathcal{Z} + 1$  and 1 strongly connected is necessary and sufficient, and
- a protocol has been proposed which is polynomial in  $|V|$ , the number of nodes in the graph, i.e. logarithmic in  $|\mathcal{Z}|$ .

## Algorithm

$A$  is the sender and  $B$  is the receiver.

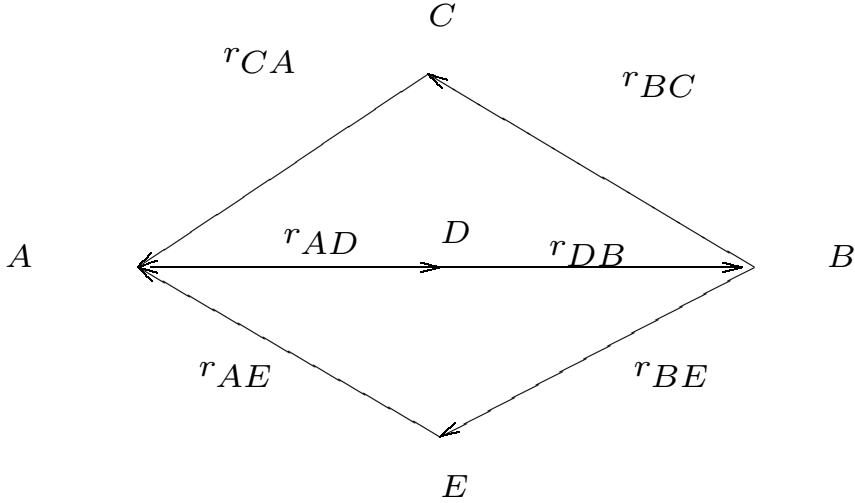
**Step 1** For each edge  $e$  where  $u$  is the originator,  $u$  chooses a random message  $r_e$  and sends it to the recipient of that edge.

**Step 2** Every node computes the sum of messages it has received and subtracts the sum of messages it has sent out. If the node is the actual sender  $A$ , then it adds to this total the message  $M^A$ . Call this sum the “final result” for this node. Each final result, except the one of the actual receiver  $B$ , is propagated by the nodes openly to the receiver  $B$ .

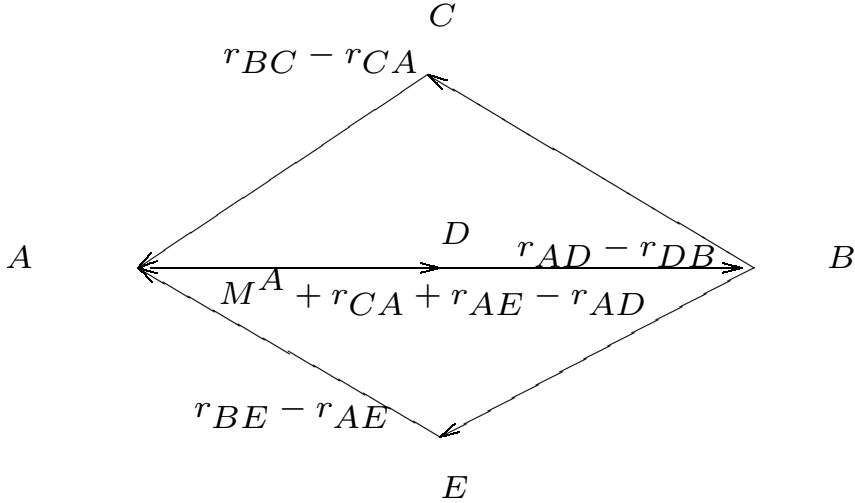
**Step 3**  $B$  adds all final results, including his. The result is the message  $M^B$ .

Example:

Step 1



Step 2



Step 3 Easy to verify.



## Active adversary, no privacy

**Lemma 2.** *Let  $G = G(V, E)$  be a directed graph,  $A, B$  be nodes in  $G$ , and  $\mathcal{Z}_1, \mathcal{Z}_2$  be adversary structures on  $V \setminus \{A, B\}$ . Then  $A, B$  are  $(\mathcal{Z}_1 + \mathcal{Z}_2 + 1)$ -connected if, and only if: for all sets  $Z_1 \in \mathcal{Z}_1$  there is a set  $S_{Z_1}$  of paths between  $A$  and  $B$  such that,*

- *the paths in  $S_{Z_1}$  are free from nodes of  $Z_1$ ,*
- *for every  $Z_2 \in \mathcal{Z}_2$  there is at least one path in  $S_{Z_1}$  that is free from nodes of  $Z_2$ .*

**Theorem 6.** *Let  $G = G(V, E)$  be a directed graph,  $A, B$  be nodes in  $G$ , and  $\mathcal{Z}$  be an adversary structure on  $V \setminus \{A, B\}$ . We have  $\mathcal{Z}$ -reliable message transmission from  $A$  to  $B$  if, and only if,  $A, B$  are strongly  $(2\mathcal{Z} + 1)$ -connected in  $G$ .*

## Algorithm

Assume that  $A, B$  are strongly  $(2\mathcal{Z} + 1)$ -connected in  $G$

Let  $S$  be the set of all directed paths from  $A$  to  $B$ .

**Step 1** For each path  $p \in S$ ,  $A$  sends  $M^A$  to  $B$  over  $p$ .

**Step 2**  $B$  receives  $M_p^B$  through path  $p \in S$ .  $B$  finds a node set  $Z_1 \in \mathcal{Z}$  whose path set  $S_{Z_1}$  is such that the same message  $M^B = M^A$  is received on all its paths.

**Claim:**  $M^B = M^A$ .

Indeed, Suppose that the adversary selects  $Z_2 \in \mathcal{Z}$ . We have: by Lemma 2 that since  $A, B$  are  $(2\mathcal{Z} + 1)$ -connected, there will be a path  $p_0 \in S_{Z_1}$  free from nodes of  $Z_2$ . On this path  $M_{p_0}^B = M^A$ . Since



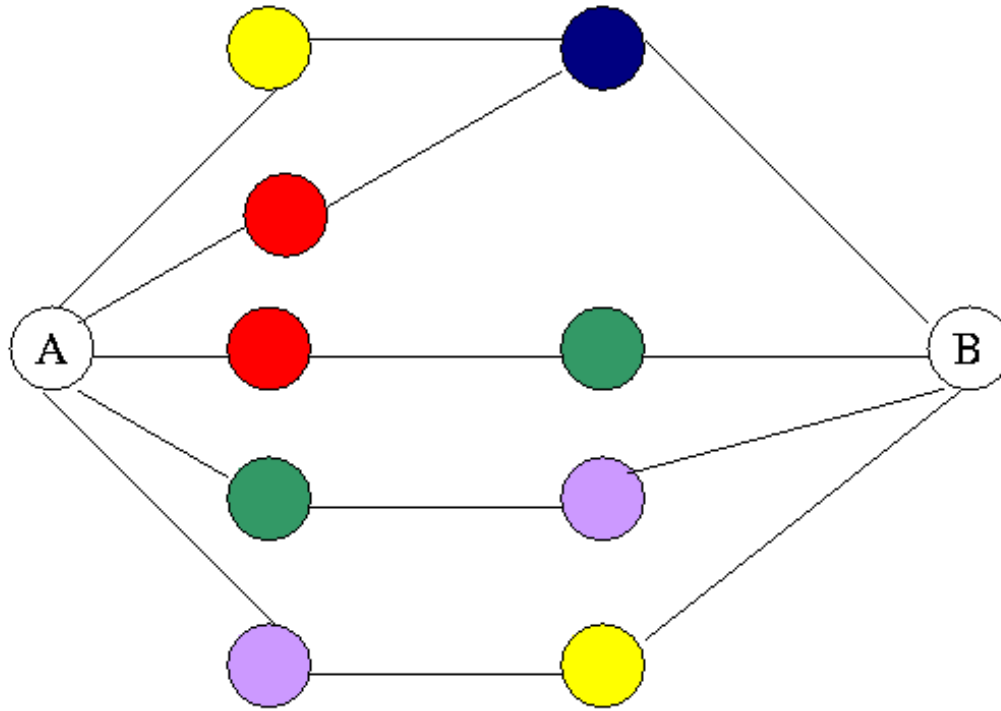
$B$  receives the same message from all paths in  $S_{Z_1}$ , we must have

$$M^A = M_{p_0}^B = M^B.$$

It follows that  $B$  can reliably recover the message  $M^A$ .

An interesting adversary structure is the  $t$ -color adversary structure. A weakness of one router/computer can easily be exploited on another one if it runs the same platform. Vertices are given colors.  $t$  colors can be corrupted. It allows to model routers that run the same platform, i.e. have the same weakness, to be assigned the same color.

Color adversary structure is interesting to understand counter-intuitive arguments: i.e.: **color separable is not linked to vertex disjoint paths.**



**New result:**

Deciding whether a vertex colored graph with  $C$  the set of colors, is  $\mathcal{Z}_{C,k} + 1$ -connected is co-**NP**-complete.

**Definition 2.** Let  $G(V, E)$  be a directed graph,  $A, B$  be nodes in  $G$ ,  $S$  be a set of simple paths in  $G$  between  $A$  and  $B$ , and  $G_S$  be the graph obtained by removing all nodes and edges of  $G$  not in  $S$ . Let  $\mathcal{Z}$  be an adversary structure. We say that  $S$  is a **minimal  $(\mathcal{Z} + 1)$ -connected path-set from  $A$  to  $B$**  in  $G$ , if

1.  $A$  and  $B$  are  $(\mathcal{Z} + 1)$ -connected in  $G_S$ , and
2. for each path  $p \in S$ ,  $A$  and  $B$  are  $\mathcal{Z}$ -separable in  $G_{S \setminus \{p\}}$ .

**Theorem 7.** *Let  $G = G(V, E, C, f)$  be a colored graph which is  $(\mathcal{Z}_{C,k} + 1)$ -connected. If the number of colors is minimal then the paths in a minimal path-set are node-disjoint and each path is monochrome (all nodes on one path have the same color).*

# 8. FINDING THE NETWORK GRAPH WHILE UNDER ATTACK

## Model

**Similar** to classical one:

**Input:** each node knows its neighbors only.

**Question:** find the network

**Different:**

- $t$ -bounded Byzantine adversary. **Special attack:** can claim non-existent nodes exist.
- use a communication network (which is not immediately reconstructed)
- use a PGP like certificate graph (virtual graph).



**Solutions:** polynomial time solution by Burmester-Desmedt (1999) if the PGP like network is  $2t + 1$  strongly connected.

Lots of hueristics afterwards.

## More details (sketch):

Impossible to obtain the graph  $G$ , but at best a good approximation  $G'$ .

**Client:** wants to find network graph. **Servers:** are the other nodes.

**Initially:** nodes only know their neighbors.

Use Round-Robin to avoid flooding. All communication is signed and all signatures are verified on consistency.

**Phase 1** Not all honest nodes have been found.

Servers provide client with the list of their neighbors (one at a time).



Client checks whether all nodes that are real and responding have been found. If so, move to the next phase.

**Phase 2** Same as above. However, nodes that claim new nodes are being found are declared dishonest.

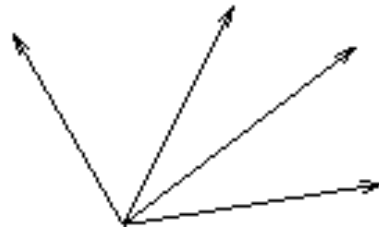
## 9. PARTIAL BROADCAST: A SURVEY

$t$ -bounded adversary only (some results on general adversary structure easily extend). We distinguish:

### 9.1. PASSIVE ADVERSARY

Franklin-Yung (1995,2004) replaced the point-to-point network by a **partial broadcast**. They use a directed hypergraph. A directed hypergraph  $H = (V, E)$  consists of set of vertices  $V$ , however a directed hyperedge  $e \in E$  has the form  $(v, V')$ , where  $v \in V$  and  $V' \subset V$ . **When the node  $v$  uses this directed hyperedge all nodes in  $V'$  receive the same information (others learn nothing about that information).**

## Directed hyperedge



Franklin-Yung (1995,2004) focussed on a passive adversary who eavesdrops. They demonstrated:

- that a necessary and sufficient condition for private communication secure against a  $t$ -bounded passive adversary is that the directed hypergraph is strongly 1-connected and weakly  $(t + 1)$ -connected.
- proposed a protocol (not necessarily polynomial time).

Franklin-Yung also introduced special cases, one of these is called a **neighbor network**, which can be represented by an ordinary graph. **Ethernets are a special case** of these.

In this graph if a vertex broadcast a message, all its neighbors will receive identically the same information.

## 9.2. ACTIVE AND EAVESDROPPING ADVERSARY

This is a very challenging problem. We distinguish between:

### 9.2.1. THE CASE OF NEIGHBOR NETWORKS.

Franklin and Wright (1998,2000) introduced the concept of **interiorly neighborhood-disjoint lines**.

Formally,  $A$  and  $B$  are connected by  $n$  **interiorly neighborhood-disjoint lines** if there are  $n$  lines  $p_1, \dots, p_n \subseteq V$  with the following properties:

- For each  $1 \leq j \leq n$ , the  $j$ -th line  $p_j$  is a sequence of  $m_j + 2$  nodes  $A = X_{0,j}, X_{1,j}, \dots, X_{m_j+1,j} = B$  where  $X_{i,j}$  is a neighbor of  $X_{i+1,j}$ .
- For each  $i_1, i_2, j_1$ , and  $j_2$  with  $j_1 \neq j_2$ , the only possible common neighbors of  $X_{i_1,j_1}$  and  $X_{i_2,j_2}$  are  $A$  and  $B$ .

Franklin-Wright (1998,2000) proved that:

- If  $n > t$ ,  $\delta > 0$  and  $\varepsilon > 0$ , then there is an efficient  $(\varepsilon, \delta)$ -secure message transmission protocol between  $A$  and  $B$ .
- If  $n > \lceil 3t/2 \rceil$  and  $\delta > 0$ , then there is a  $\delta$ -reliable and perfectly private message transmission protocol.
- If  $t < n \leq \lceil 3t/2 \rceil$  and  $\delta > 0$ , then there is an **exponential bit complexity**  $(0, \delta)$ -secure message transmission protocol between  $A$  and  $B$ .

They opened the question:

is it possible to efficiently achieve perfect privacy when  $t < n \leq \lceil 3t/2 \rceil$ , i.e. a **polynomial time**  $(0, \delta)$ -secure message transmission protocol?

Wang-Desmedt (1999,2001) gave an affirmative answer using a



constructive proof.

They extended the results by introducing:

$A$  and  $B$  are weakly  $(n, t)$ -connected (Wang-Desmedt)

- if there are  $n$  vertex disjoint paths  $p_1, \dots, p_n$  between  $A$  and  $B$  and,
- for any vertex set  $T \subseteq (V \setminus \{A, B\})$  with  $|T| \leq t$ , there exists an  $i$  ( $1 \leq i \leq n$ ) such that all vertices of  $p_i$  have no neighbor in  $T$ .

If  $A$  and  $B$  are weakly  $(n, t)$ -connected for some  $t < n$ , then there is a perfectly private transmission protocol which is an efficient  $(0, \delta)$ -secure message transmission protocol between  $A$  and  $B$ .

Wang-Desmedt posed as open problem whether:

the weakly  $(n, t)$ -connectivity condition is necessary.

Desmedt-Wang (2002) gave a counter example.



## 9.2.2. DIRECTED HYPERGRAPHS

Desmedt-Wang (2002):

A necessary and sufficient condition for reliable message transmission from  $A$  to  $B$  against a  $t$ -active adversary is that  $A$  and  $B$  are not  $2t$ -separable, in which  $2t$ -separable is similar to  $2\mathcal{Z}$ -separable where  $\mathcal{Z}$  corresponds to a threshold adversary structure.

## 9.3. ADDING JAMMING

We distinguish between:

### 9.3.1. Jamming adversary only in traditional broadcast

Well known approach:

Sender and receiver agree on random “seed,” and use a pseudo-random generator for frequency hopping.

More interesting case:

$t$  receivers collaborate with adversary. Above fails. The problem and solutions go back to the the 1960's, e.g. Kautz-Singleton, 1964.

Solution:

Superimposed codes (also viewed as a covering problem:

Erdős-Frankl-Furedi), i.e.:

Use **set of indices of seeds**. Each receiver is given a “block” (subset). The blocks are such that: none is covered by the union of  $t$  others.

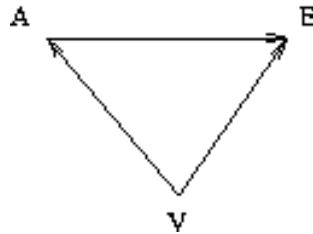
Lots of research, in particular by Russian scientists, such as: Dyachkov-Rykov, Levenshtein (jointly with Ericson).

(See also Desmedt-Safavi Naini-Wang-Batten-Charnes-Pieprzyk, 2000 for bounds.)

## 9.3.2. JAMMING IN NETWORKS

Third party can prevent communication between two parties.

Studied by Desmedt-Wang-Safavi Naini-Wang (2005):



$V$  can jamm nodes  $A$  and/or  $B$

### Model

Use **radio network**, i.e. a **directed colored-edge multigraph**

$R(V, E, F, c)$ , where  $V$  is the node set,  $E$  is the directed edge set,  $F$  is the frequency (color) set, and  $c$  is a map from  $E$  to  $F$  (the map  $c$  assigns a frequency to each edge).

Cases (jamming only):

**Receiver-jamming:** A node  $v$  can receiver-jam on a frequency  $f$  if there is a directed edge  $e$  from  $v$  to some node  $u$  with  $c(e) = f$ . The result of receiver-jamming by  $v$  on frequency  $f$  is that for any node  $u$  such that there is a directed edge  $e$  from  $v$  to  $u$ ,  $u$  cannot receive any message transmitted on the frequency  $f$  by any node.

**Sender-jamming:** A node  $v$  can sender-jam on a frequency  $f$  if there is a directed edge  $e$  from  $v$  to some node  $u$  with  $c(e) = f$ . The result of sender-jamming by  $v$  on frequency  $f$  is that for any node  $u$  such that there is a directed edge  $e$  from  $v$  to  $u$ ,  $u$  cannot send any message on the frequency  $f$  to any node.

**Destroy-jamming:** A node  $v$  can destroy-jam on a frequency  $f$  if



there is a directed edge  $e$  from  $v$  to some node  $u$  with  $c(e) = f$ . The result of destroy-jamming by  $v$  on frequency  $f$  is that for any node  $u$  such that there is a directed edge  $e$  from  $v$  to  $u$ ,  $u$  cannot receive or send any message on **any** frequency.

## Receiver jammers only (no privacy)

Let  $R(V, E, F, c)$  be a radio network, and  $S \subset V$  be a node set.

The reduced radio network  $R(V \setminus S, E_{V \setminus_{rj}S}, F, c)$  is defined by letting

$E_{V \setminus_{rj}S} = E \setminus E_S^{rj}$ , where  $E_S^{rj}$  is the set of the following directed edges:

- all edges originated from nodes in  $S$ .
- all edges  $e$  from  $u$  to  $v$  such that there is an edge  $e'$  from some node in  $S$  to  $v$  and  $c(e) = c(e')$ .

**Theorem 8.** *Reliable message transmission from  $u$  to  $v$  in a radio network  $R(V, E, F, c)$  against a  $t$ -receiver-jamming adversary is possible if and only if for any  $t$ -node set  $S$ , there is a directed path from  $u$  to  $v$  in the reduced radio network  $R(V \setminus S, E_{V \setminus r_j S}, F, c)$ .*

## Other cases studied

- receiver-and-sender jammers
- destroy-jamming
- adding active (Byzantine) adversaries
- adding privacy

Theorems are similar.

# 10. CONCLUSIONS

We do **not** pretend to have surveyed all related papers on the topic. For example: the work on private/reliable communication in which two graphs are used one being the communication graph and the other an “authentication graph” where an edge indicates that parties share a secret key (See Beimel-Franklin 1997 and Beimel-Malka 2005.)