Private and Reliable Communication with Untrusted Components

Yvo Desmedt

Univ. of Texas at Dallas
USA

University College London
UK

1st of July 2019

Yvo Desmedt was partially supported by DARPA F30602-97-1-0205, NSF CCR-0209092, EPSRC EP/C538285/1 and BT as BT Chair of Information Security.

Note: this is a summary of a 6 hours talk.

OVERVIEW

1. The enemy is inside
2. What does this mean in the communication context?
3. Denial of service during communication: the issues
4. Complexity of the problem: illustration
5. Classical results
6. Point-to-point networks
7. Partial broadcast
8. Potential applications
9. Some techniques
10. Techniques for general adversary structures
11. Implementations
12. What value should we have for t?
13. Conclusions

1. THE ENEMY IS INSIDE

Since 1946 the British knew about the “atomic spies” at Los Alamos (see e.g., the arrest of Allan Nunn May). Many more got arrested later.

It seems the West has not understood for a long time that:

The enemy is inside

Indeed, we now have many examples, such as Kim Philby (defected to the Soviets in 1963), . . .

Harsh pre-trial punishments, as solitaire confinement (Bradley Manning) has not helped (see Edward Snowden).

Since 1987, my main line of research has been on finding techniques to secure IT systems in which we assume that the enemy is inside. So, I helped, for example, to develop:

- Threshold cryptography, in which one cannot trust all devices that will be used for decryption or for signatures, either because:
  - their keys may have been compromised, or
  - the manufacturer may have become an adversary, or
  - the machine has been hacked.

In this lecture, we will survey some of the research done to design communication systems in which:

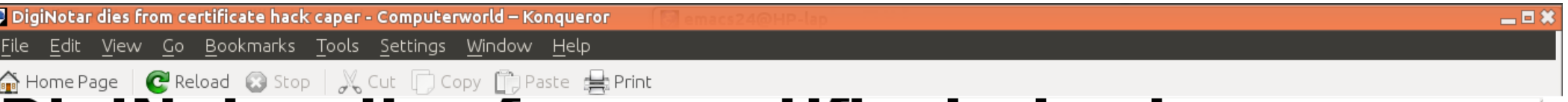
- the manufacturer may have become an adversary,
- the equipment has been hacked.

The design allows for the possibility not to know in advance who the adversary will be, a concept borrowed from the reliability community (see further for details).

2. What does this mean in the communication context?

We give just three examples:

1. DigiNotar
2. BT's use of of Huawei equipment
3. Diverted Huawei documents when using FedEx



DigiNotar dies from certificate hack caper

. . .

By Gregg Keizer
September 21, 2011 04:09 PM ET
2 Comments

Share Like 1

Computerworld - The Dutch company that was hacked earlier this summer by certificate thieves has gone bust and shut down, its U.S.-based owner said Tuesday.

. . .

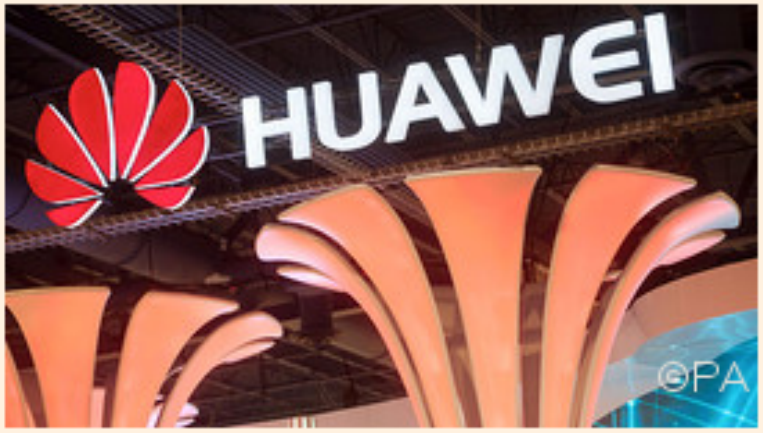
DigiNotar confirmed that it had first discovered the intrusion on July 19, but had not disclosed the breach to browser makers, the Dutch government -- which used DigiNotar certificates to validate the identities of many of its websites -- or other customers until more than a month later.

An investigation sponsored by the Dutch government revealed that the hacker or hackers first compromised DigiNotar's servers in mid-June and made off with more than 500 certificates.

Last updated: June 6, 2013 8:04 pm

UK security committee ‘shocked’ over Huawei contract with BT

By James Blitz and Daniel Thomas



A parliamentary committee has attacked the British government’s failure to investigate the use of equipment from China’s Huawei in the UK national telecommunications network, saying security issues “risked being overlooked”.

However, the committee, which comprises leading politicians and civil servants, said there would always be risks involved in any telecoms system sourced from abroad – and the UK authorities were not doing enough to manage that risk.

The committee said its investigation revealed "a disconnect between the UK's inward investment policy and its national security policy."

In particular, it said a centre set up by the government to monitor the physical equipment and software used by Huawei, "is highly unlikely to provide, or to be seen to provide, the required levels of security assurance".

Beijing to investigate FedEx for 'damaging rights of Chinese clients' amid Huawei dispute - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Osquldas Väg, 114 … | Program | CySeP Summ… | IEEE European Sym… | Beijing to investiga…

https://www.cnbc.com/2019/06/01/beijing-to-investigate-fedex-for-damaging-rights-of-chinese 133% Search

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

MARKETS

Beijing targets FedEx for 'damaging rights of Chinese clients' amid Huawei dispute

PUBLISHED SAT, JUN 1 2019 • 9:33 AM EDT | UPDATED SAT, JUN 1 2019 • 9:08 PM EDT

Spencer Kimball
@SPENCEKIMBALL

SHARE

KEY POINTS

- According to Xinhua, FedEx failed to deliver express packages to designated addresses in China, "seriously damaging the lawful rights and interests of its clients and violating laws and regulations governing the express industry in China."

TRENDING NOW

Japanese oil
disagrees wi
that a mine c
near Iran

docum Highlight All Match Case Whole Words 1 of 1 match

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 (and/or links). The adversary has access to all information received by these nodes (and all secrets of these nodes).

Active adversary. The nodes (and/or links) 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, (fail-and-stop) 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).

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

ε**-privacy.** Unconditional security (See literature: Franklin-Wright.) Edge: considered private communication.

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

The security of sender/receiver We distinguish between the case the sender and/or receiver:

- can use trusted equipment
- can not use trusted equipment

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. COMPLEXITY OF THE PROBLEM: ILLUSTRATION

What about the following solution:

Send a message using standard techniques (TCP), when not receiving an acknowledgment, then the adversary must have control over the communication path. Use a different path then.

This technique does not work

(except when using end-to-end authentication, which is non-trivial without the use of a PKI, which is itself a "directed graph" (of which computer signs someone's else public key)).

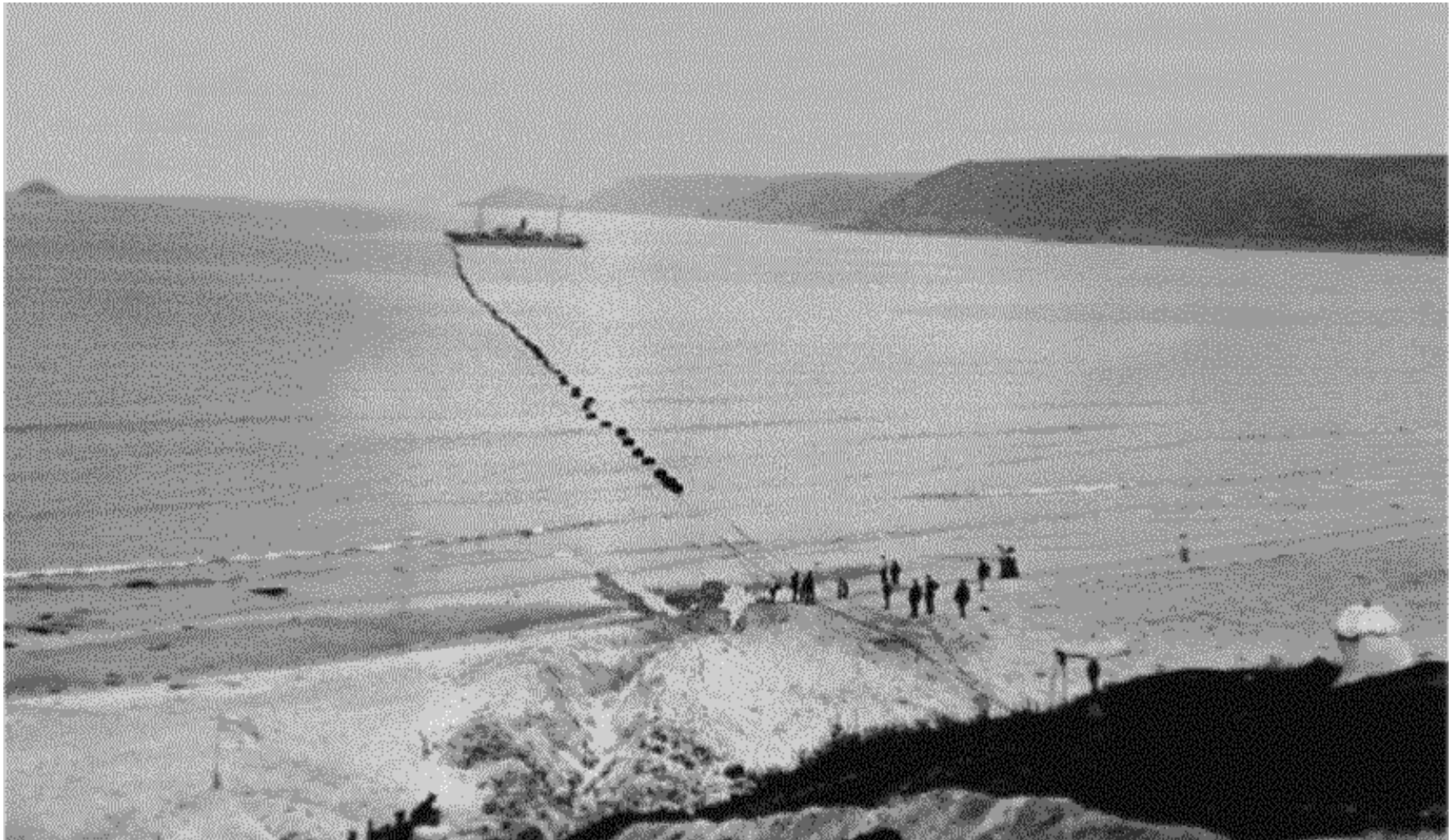
Indeed, the adversary will just send a fraudulent ACK to the sender.

The solutions borrow from the reliability community. As an example:

When you fly an airbus, 3 computers compute fuel consumption, route, etc. all the time!

5. CLASSICAL RESULTS

This goes back to World War I, after the cable ship Telconia lifted from the bed of the North Sea the German overseas telegraph cables:



If an adversary can destroy t nodes, then $t+1$ vertex disjoint paths are needed and sufficient to communicate from sender (node A) to receiver (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.

Illustration: node disjoint paths: a closed station

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

Dolev-Dwork-Waarts-Yung (1993) added privacy. They required perfect reliability, and perfect privacy.

6. POINT-TO-POINT NETWORKS

- Sender/receiver equipment is trusted:
  - Point-to-point: threshold adversary:

    Dolev-Dwork-Waarts-Yung (1993) considered:

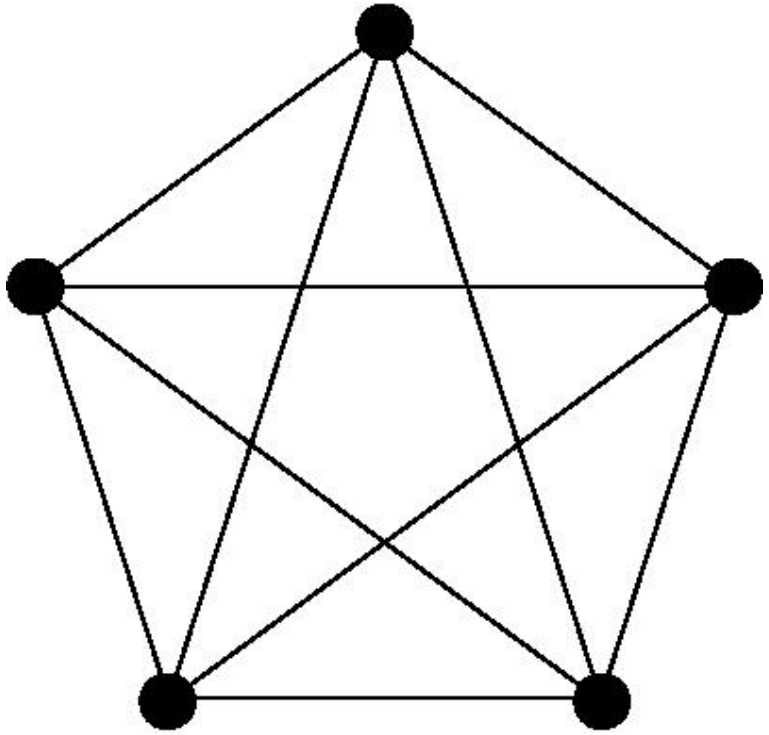
    all communication links (edges in the graph) are:

    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).

    Definition 1. A graph is (vertex) 1-connected if there is a path from every vertex to every vertex. When $k > 1$, a graph is k-connected if after the removal of any single vertex (and its adjacent edges) remains $(k - 1)$-connected.

Theorem 1. *A graph is k-connected if and only if between any two vertices A and B there are k vertex disjoint paths.*

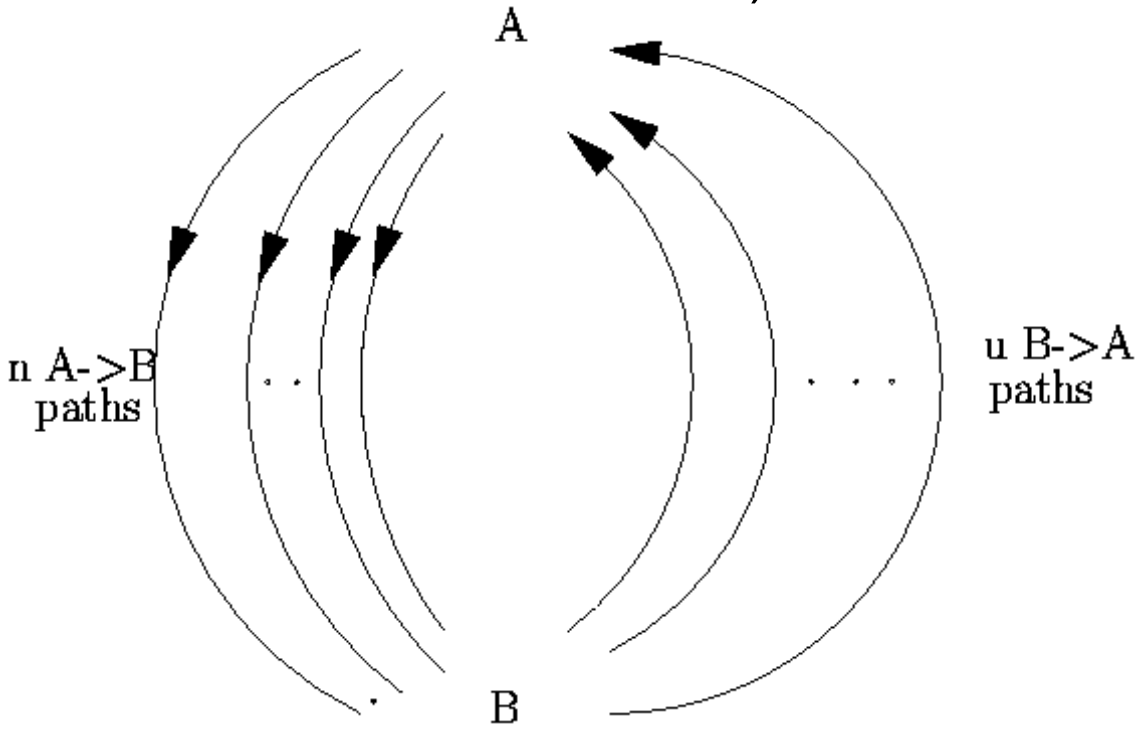
Example:



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

Their algorithm was inefficient. It took until 2008 until it was made practical (Kurosawa-Suzuki).

Desmedt and Wang (2002) observed above are not the most general cases, since there could be feedback channels. They focused primarily on the case the feedback channels are vertex disjoint from the forward channels. (Several follow papers improved on some of these results.)



– Point-to-point: general adversary What is a general adversary structure?

Given a set P (e.g., of nodes and links), one specifies what subsets might behave maliciously. So, as stated earlier:

The design allows for the possibility not to know in advance who the adversary will be.

This prevents preparing everything for a full blown war with the Soviets, and then being attacked by Al Qaeda on September 11, 2001.

Example set $P = \{1, 2, 3\}$ and $\mathcal{A}_P = \{\{1\}, \{2, 3\}, \{2\}, \{3\}, \emptyset\}$.

Maximal adversary set: $\mathcal{A}_P^* = \{\{1\}, \{2, 3\}\}$.

Applied to communication:

Let A and B be the sender and receiver. Let

$Z_1, Z_2, Z_3 \in \Lambda_{V \setminus \{A,B\}}$.

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 that removing any nodes specified by any $Z_1 \cup Z_2$ (see above) A, B remain connected (Kumar-Goundan-Srinathan-Rangan, 2002).

one-way without feedback, that removing any nodes specified by any $Z_1 \cup Z_2 \cup Z_3$ is that A, B remain connected (Desmedt-Wang-Burmester, 2005).

Necessary and sufficient conditions for privacy-only and perfect reliability-only were given in Desmedt-Wang-Burmester, 2005. (See also Yang-Desmedt, for efficiency improvements.)

Note: this work predates Perrig (ETH Zurich) work. Moreover, it avoids to have a "declared adversary," as happened during the cold war. In that case September 11 attack was not by the Soviets!

- Sender/receiver equipment is untrusted: (e.g., when the country is technological challenged, or has outsourced all its production of electronics).

  Two cases were studied:

  – Non-interactive $\mathrm{mod}10$ with a human receiver

  – Two-phase $\mathrm{mod}10$ with a human receiver

  Moreover, a method to add $\mathrm{mod}10$ in a human friendly way was proposed and human experiments confirmed its ease.

  For details: Erotokritou-Desmedt 2012.

7. PARTIAL BROADCAST

- The general case

  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).

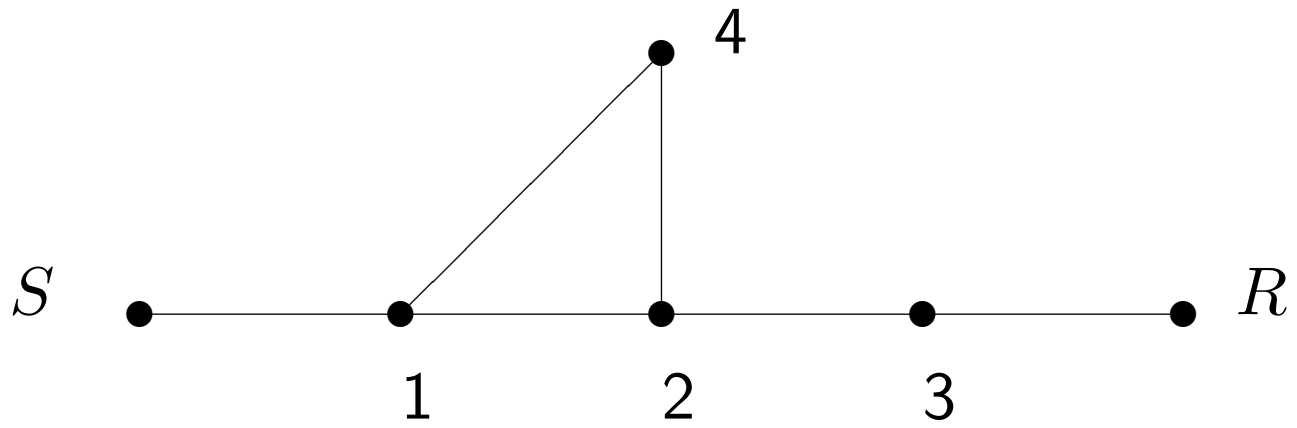
  For the threshold case, Franklin-Yung gave necessary and sufficient conditions for privacy-only.

- Partial broadcast: the multicast case

  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.

  Example:



  If node 2 sends u, 1, 3, and 4 receive the same u. Using Franklin-Yung 1995 terminology, $(2, \{1, 3, 4\})$ is a directed hyperedge in which 2 is broadcasting.

Necessary and sufficient conditions for privacy and reliability were an open problem since 1995 and were finally solved in 2011 (Yang-Desmedt).

8. POTENTIAL APPLICATIONS

We give two examples:

- PKI:

  PKI is the foundation of electronic commerce. It is supposed to guarantee the correctness of the public keys used in secure modern communication.

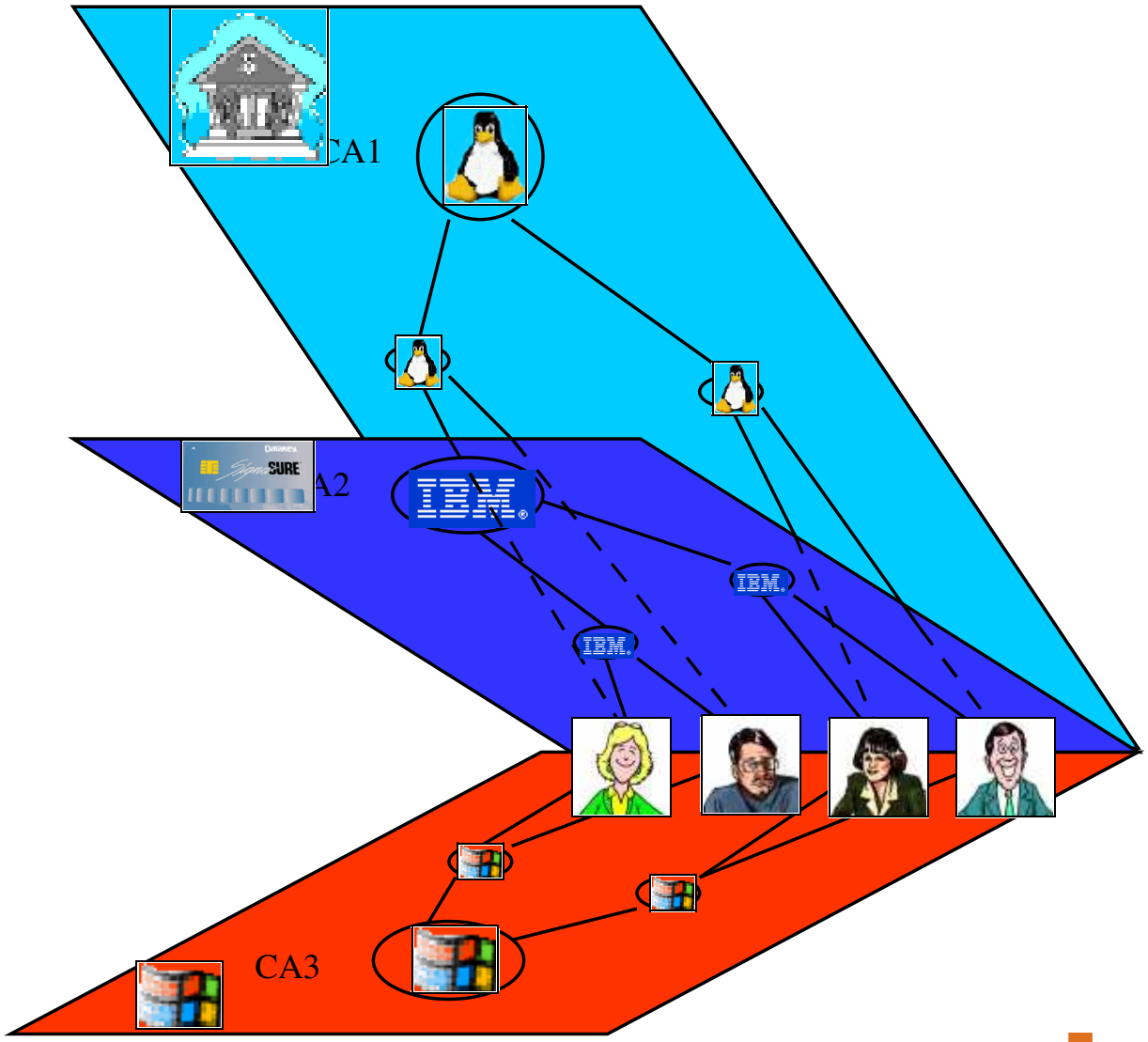
  In 1996 Burmester-Desmedt-Kabatianskii and independently in 1997 Reiter-Stubblebine pointed out that in the currently deployed PKI every node is a single point of failure (from a security viewpoint).

  An alternative, also hierarchical in nature, as the current PKI was proposed by Burmester-Desmedt in a paper with title

  Is hierarchical public-key certification the next target for hackers?

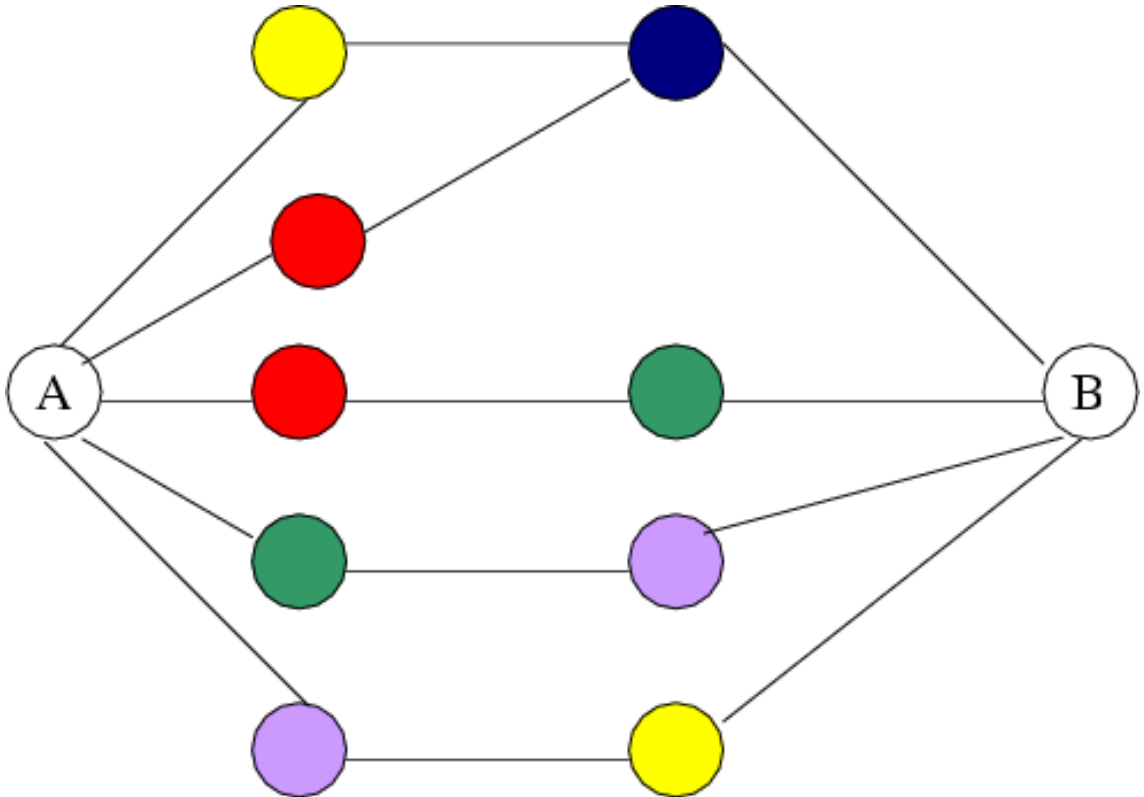
  in 2004 using “colors” to model CA platforms that could be hacked.

Each node's (CA's) platform is indicated by coloring the node. We proposed in particular:



- Building point-to-point networks with untrusted equipment
  - Node level:

    As earlier, we color the nodes dependent who built a particular router (or other node equipment). We introduced what we called a k-color adversary structure. However, we realized that we cannot require to build networks in a similar way as we proposed for PKI. So, Desmedt-Wang-Burmester (2005) considered networks as:



- ∗ Positive result: whether we can achieve privacy and/or reliability, fits within the results on general adversary structures.
- ∗ Negative result: Desmedt-Wang-Burmester (2006) showed that deciding whether a "colored" graph is k-color connected, is Co-NP-complete.

– Link level:

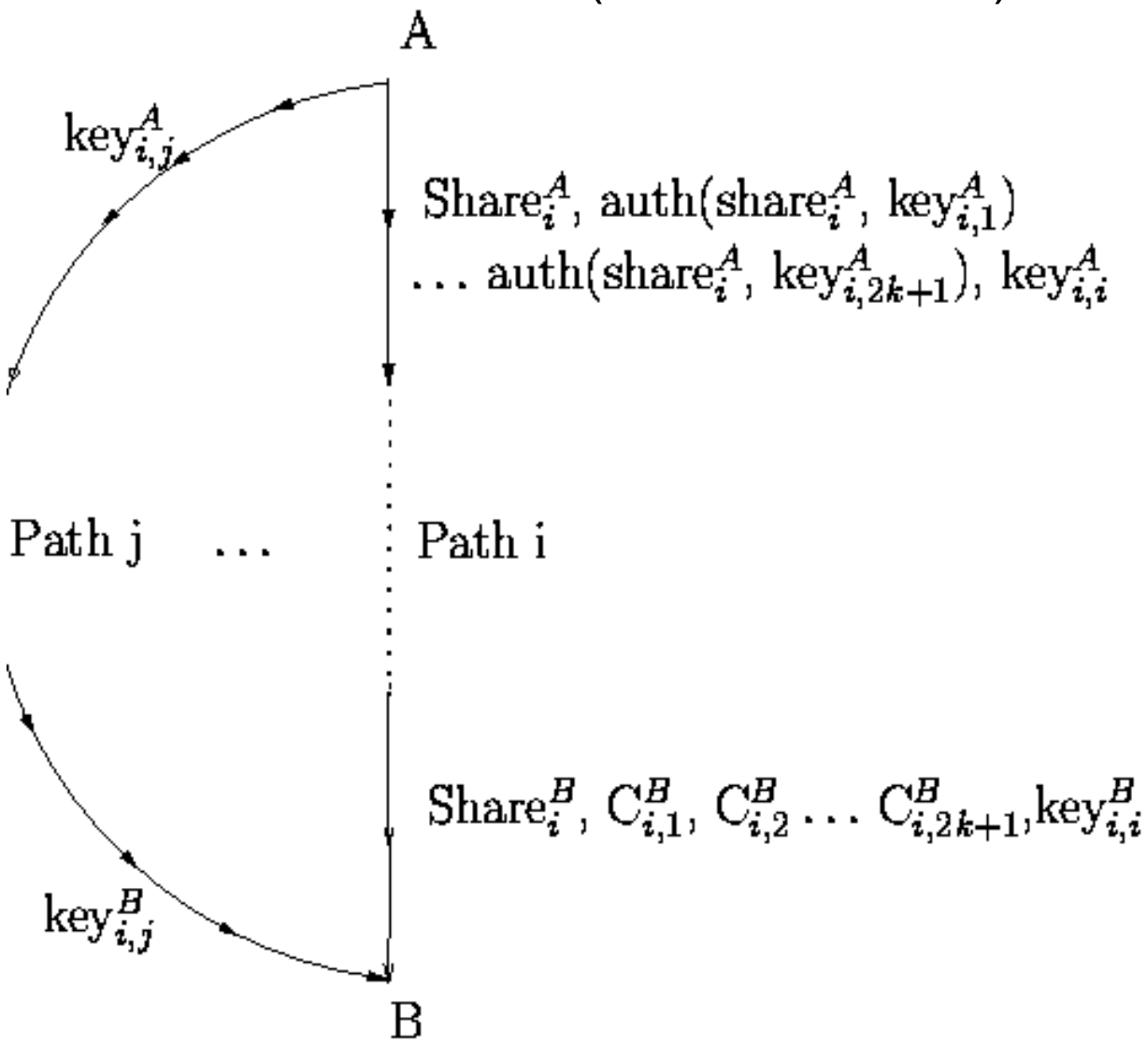
The issue that has been addressed (Wang-Desmedt 2011) is fail-and-stop in which $k+1$ different modem technology is being used and t of these might fail one day.

9. SOME TECHNIQUES

Point-to-point: threshold adversary

Dolev-Dwork-Waarts-Yung (1993) non-interactive solution uses $3t+1$ vertex disjoint paths. The sender uses $t+1$-out-of-$3t+1$. The receiver regards it as a Reed-Solomon code.

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



Partial broadcast: Franklin-Yung **Algorithm**

A is the sender and B is the receiver.

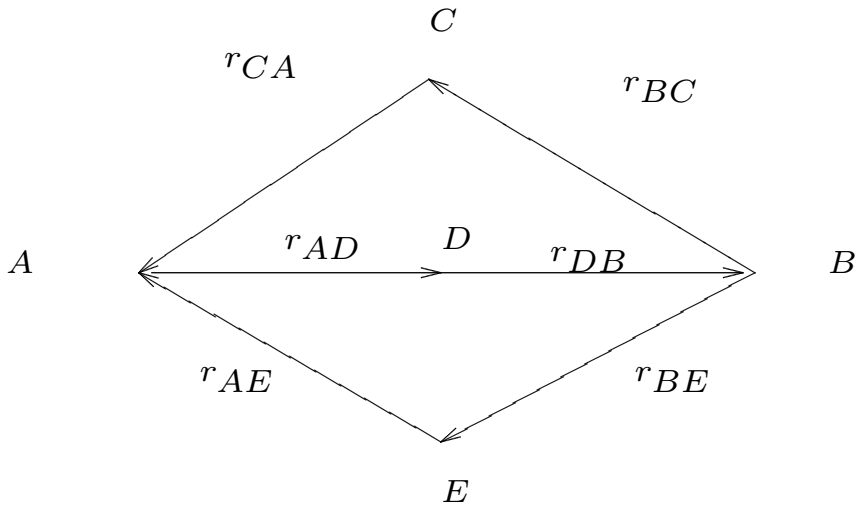
Step 1 For each hyperedge e where u is the originator, u chooses a random message r_e and sends it to the recipients of that hyperedge.

Step 2 Every node computes the sum of messages it has received and substracts the sum of messages it has sent out. If the node is the actual sender A, then it adds to this total the messsage 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.

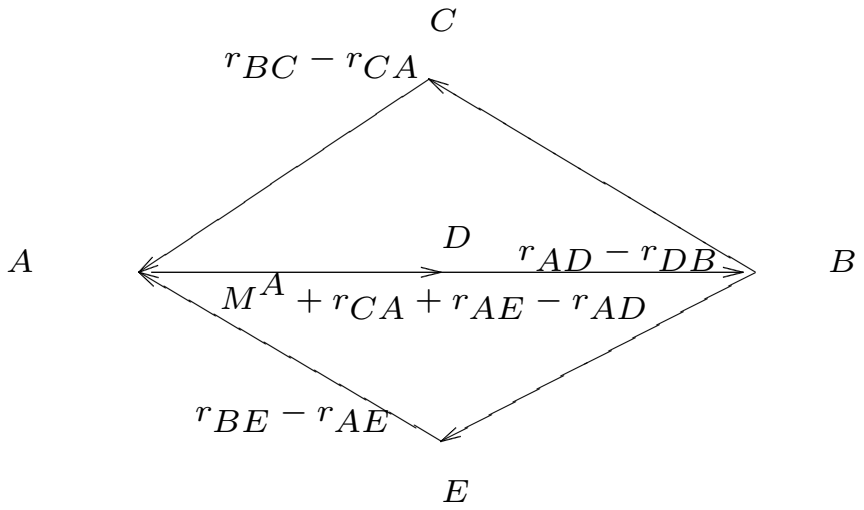
Step 3 B adds all final results, including his. The result is the message M^B.

Example:

Step 1



Step 2



Step 3 Easy to verify.

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 $\mathcal{A}_V$.

Observation (Desmedt-Wang-Burmester 2005): protocol is independent of adversary structure.

10. TECHNIQUES FOR GENERAL ADVERSARY STRUCTURES

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 2. 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.

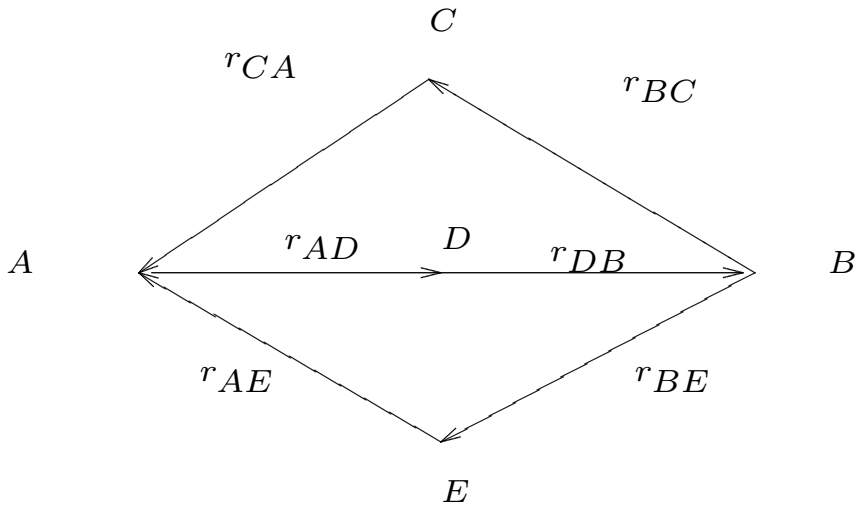
Step 1 For each edge e where u is the originator, u chooses a random message r_e and sends it to the recipient of that edge.

Step 2 Every node computes the sum of messages it has received and substracts the sum of messages it has sent out. If the node is the actual sender A, then it adds to this total the messsage 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.

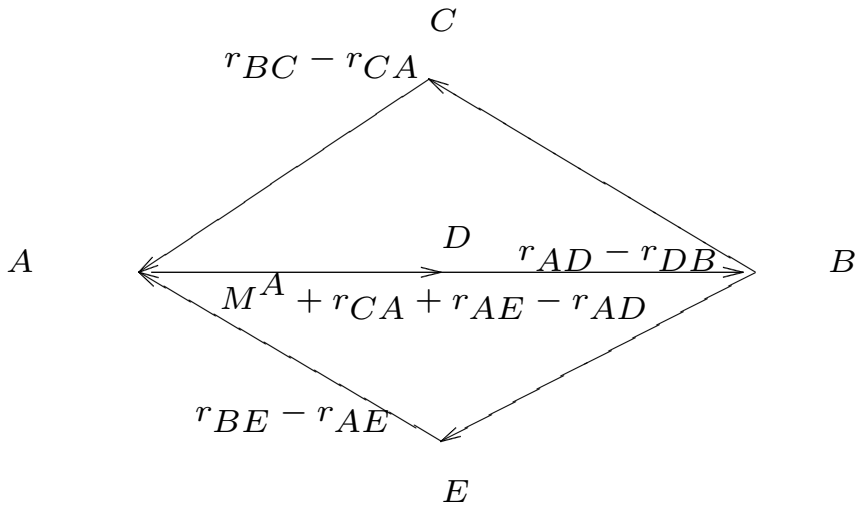
Step 3 B adds all final results, including his. The result is the message M^B.

Example:

Step 1



Step 2



Step 3 Easy to verify.

Active adversary, no privacy

Lemma 1. *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 2. *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: $M^B = M^A$.

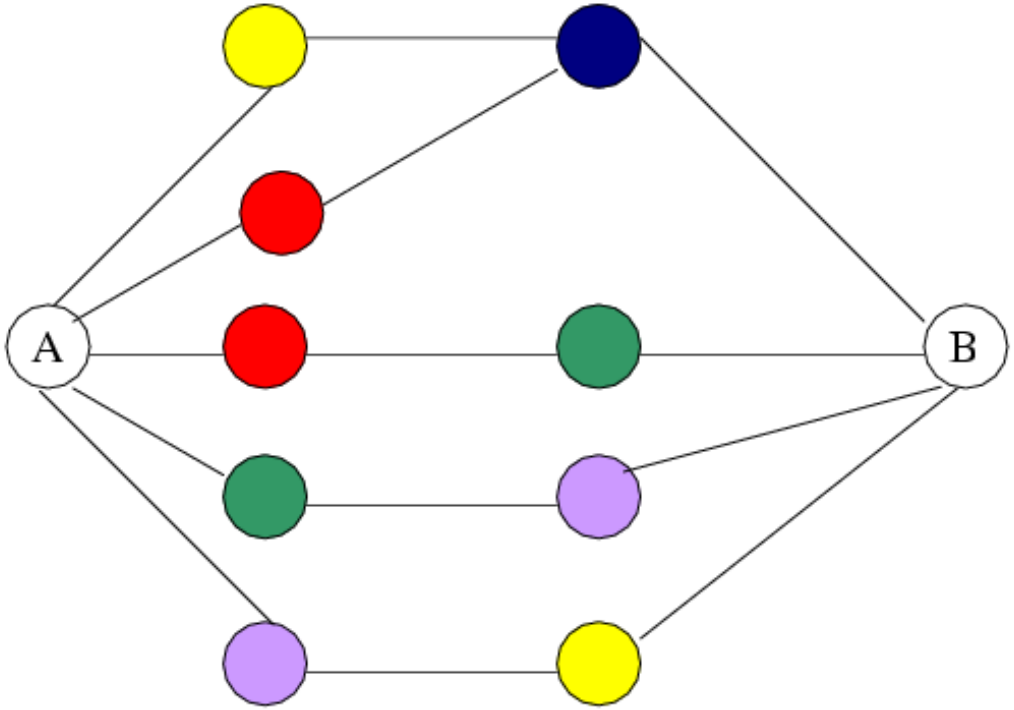
Indeed, Suppose that the adversary selects $Z_2 \in \mathcal{Z}$. We have: by Lemma 1 that since A, B are $(2\mathcal{Z}+1)$-connected, there will be a path $p_0 \in S_{Z_1}$ free from nodes of Z_2. On this path $M_{p_0}^B = M^A$. Since B receives the same message from all paths in S_{Z_1}, we must have

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

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.


A
B

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 3. 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 3. *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).*

11. IMPLEMENTATIONS

1. Desmedt-Erotokritou-Kearney (unpublished) tried to implement the 1993 non-interactive solution of Dolev-Dwork-Waarts-Yung. The amazing problem we encountered is that:
   - the 1993 internet technology would had allowed a 1993 implementation,
   - the current internet technology no longer allows to implement this. Reasons:
     - to guarantee $3t + 1$ vertex disjoint paths, we must specify the path a data packet has to follow. Today any packet that uses the standard TCP/IP option to specify the path is dropped by modern routers!!

- companies want to keep the layout of the network private, which causes another difficulty!

2. Desmedt-Cheney (unpublished) designed and implemented a Thunderbird extension using mail servers, as gmail, hotmail, yahoo, etc. For example, gmail and hotmail are considered as intermediary nodes between the sender and receiver. So, we consider Google and Microsoft as potential adversaries, not working together.

12. WHAT VALUE SHOULD WE HAVE FOR t?

In some totalitarian countries the government has good control of the network. So, if you do not trust your government, in that case it seems that requiring to have paths that are not under control of the government will fail!

Solution 1: use postal service.

In many countries, the government controls the postal service.

Solution 2: use pigeons!

2009 test in South-Africa showed how a pigeon could transfer a 4GB flash.

13. Conclusions

Building inexpensive operating systems and outsourcing communication equipment comes at a price: one can no longer trust them!

However, for several decades solutions have been under research. Unfortunately, they come at a cost: such as the need for redundancy, and the need to reconsider the design of routers.

The cost of communication is getting low. Indeed, Google's Gigabit fiber has arrived in e.g., Austin (now also AT&T). Sony is offering 2 Gigabit in the Tokyo area. So, (P)SMT, i.e., Perfectly Secure Message Transmission technology should be considered seriously. Moreover, it is easy today to have multiple providers (landline and

mobile).

Although for today's Internet we have implementation problems, for dedicated networks, PSMT is highly recommended. Example: China's Quantum Network gives at best the same security as link encryption, with all its security problems. (It requires all employees in the nodes to be trusted!) PSMT would avoid that problem. Similar solutions could be used for dedicated highly reliable and private communication networks.

14. REFERENCES

[1] M. Burmester and Y. G. Desmedt. Is hierarchical public-key certification the next target for hackers? *Communications of the ACM*, 47(8), pp. 68–74, August 2004.

[2] M. Burmester, Y. Desmedt, and G. Kabatianskii. Trust and security: A new look at the Byzantine generals problem. In R. N. Wright and P. G. Neumann, editors, *Network Threats, DIMACS, Series in Discrete Mathematics and Theoretical Computer Science, December 2–4, 1996, vol. 38*. AMS, 1998.

[3] Y. Desmedt. Unconditionally private and reliable communication in an untrusted network. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, Proceedings*, pp. 38–41, October 16–19, 2005. Awaji Island, Japan.

[4] Y. Desmedt and Y. Wang. Maximum flows and critical vertices in and/or graphs. In O. H. Ibarra and L. Zhang, editors, *Computing and Combinatorics, 8th Annual International Conference, COCOON 2002 (Lecture Notes in Computer Science 2387)*, pp. 238–248. Springer-Verlag, 2002. Singapore, August 15-17.

[5] Y. Desmedt and Y. Wang. Perfectly secure message transmission revisited. In L. Knudsen, editor, *Advances in Cryptology — Eurocrypt 2002, Proceedings*

(Lecture Notes in Computer Science 2332), pp. 502–517. Springer-Verlag, 2002. Amsterdam, The Netherlands, April 28–May 2.

[6] Y. Desmedt, Y. Wang, and M. Burmester. A complete characterization of tolerable adversary structures for secure point-to-point transmissions without feedback. In X. Deng and D. Du, editors, *Algorithms and Computation, 16th Annual International Conference, ISAAC 2005, (Lecture Notes in Computer Science 3827)*, pp. 277–287, 2005. December 19 - 21, 2005, Sanya, Hainan, China.

[7] Y. Desmedt, Y. Wang, R. Safavi-Naini, and H. Wang. Radio networks with reliable communication. In L. Wang, editor, *Computing and Combinatorics, 11th Annual International Conference, COCOON, Proceedings (Lecture Notes in Computer Science 3595)*, pp. 156–166, 2005. Kunming, Yunnan China, August 16-19, 2005.

[8] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *Journal of the ACM*, 40(1), pp. 17–47, January 1993.

[9] S. Erotokritou and Y. Desmedt. Human perfectly secure message transmission protocols and their applications. In I. Visconti and R. De Prisco, editors, *SCN*,

volume 7485 of *Lecture Notes in Computer Science*, pp. 540–558. Springer, 2012.

[10] M. Franklin and M. Yung. Secure hypergraphs: Privacy from partial broadcast. *SIAM J. Discrete Math.*, 18(3), pp. 437–450, 2004.

[11] M. K. Franklin and M. Yung. Secure hypergraphs: Privacy from partial broadcast. In *Proceedings of the twenty seventh annual ACM Symp. Theory of Computing, STOC*, pp. 36–44, 1995.

[12] M. Kumar, P. Goundan, K. Srinathan, and C. Rangan. On perfectly secure communication over arbitrary networks. In *Proceedings of the Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 193–202, 2002.

[13] K. Kurosawa and K. Suzuki. Truly efficient 2-round perfectly secure message transmission scheme. *IEEE Transactions on Information Theory*, 55(11), pp. 5223–5232, 2009.

[14] M. K. Reiter and S. G. Stubblebine. Path independence for authentication in large scale systems. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pp. 57–66, April 1997. Zurich.

[15] Y. Wang and Y. Desmedt. Perfectly secure message transmission revisited. *IEEE Transactions on Information Theory*, 54(6), pp. 2582–2595, 2008.

[16] Y. Wang and Y. Desmedt. Edge-colored graphs with applications to homogeneous faults. *Information Processing Letters*, 111(13), pp. 634–641, July 2011.