# MTAT.07.007 Graduate seminar in cryptography
# Using Adversary Structures to Analyze Network Models

Dan Bogdanov

March 1st, 2006

## Abstract

This survey gives an overview of some of the adversary structures used in the analysis of network communication. It is based mostly on the work of Desmedt, Wang and Burmester [3].

## 1 Introduction

In network applications connections are made between nodes to exchange data. The need for secure data transfer is common to all communication models and network structures. In real life situations the nodes are usually not directly connected with secure channels. Intermediate nodes are used to route traffic between nodes.

The protocols must be designed in such a way, that multiparty communication can be carried out in the presence of faults at intermediate nodes. Models are being researched to determine restrictions for these networks and their nodes in order to fulfil these requirements.

## 2 General Terms and Previous Results

A *Byzantine fault* is any failure that can happen during the execution of an algorithm in a distributed system (communication network). The name is inspired by the Byzantine Generals' Problem. In the scenario, generals of the Byzantine army must unanimously decide, which enemy army to attack. Generals and armies are scattered over land and envoys are relaying messages between them.

If the generals fail to reach the same conclusion, the attack will be a failure, because the combined strength of all armies is required to defeat the enemy. Envoys might get lost or bribed by the enemy - these are examples of Byzantine faults. The same scenario can be applied to real-life systems (for example, peer-to-peer networks).

Let G = G(V,E) be a graph. If we can choose and remove any k - 1 edges from this graph and the graph remains connected, the graph is *k-connected*.

Some of the first results regarding security in communication networks were achieved by Dolev, Dwork, Waarts and Yung [1]. In the case of $k$ Byzantine faults:

1. If all communications links (edges in a graph) are two-way, reliable and private communication is achievable if and only if the communication network is 2k + 1 connected.

2. If all communications links are one-way (and there is no feedback), then 3k + 1 connectivity is necessary and sufficient for reliable and private communications.

An advancement in the area came with the proposal of the *adversary structure* by Hirt and Maurer [2]. The adversary is characterized by a structure of subsets of the set of parties. These subsets contain nodes, which the adversary can corrupt. The model reflects the real world, because in the real world adversaries such as viruses and trojans can gain control of many nodes who share the same platform/operating system.

The goal of the research in this area is to reduce the requirements to network connectivity. The results described in this survey were proposed by Desmedt, Wang and Burmester [3].

# 3 The Network Model

## 3.1 The Adversary

### 3.1.1 Definitions

We model the adversary by the *adversary structure*. Let $P$ be the set of parties in the network. Let $\Gamma_P$ be a subset of the power set of $P$. We call such a $\Gamma_P \subset 2^P$ an *access structure* on P.

An access structure is *monotone* if and only if $\emptyset \notin \Gamma_P$ and $\forall A$ if $A \in \Gamma_P, A \subseteq A' \subseteq 2^P$ then $A' \in \Gamma_P$.

**Example:** Let $P = \{A, B, C\}$. Then:

$$\Gamma_P = \{\{A, B, C\}, \{A, B\}, \{B, C\}, \{B\}\}$$

is an access structure, but

$$\Gamma_P{}' = \{\{A, B, C\}, \{A, B\}, \{B, C\}, \{B\}, \{C\}\}$$

is not, because $\{C\} \subset \{A, C\}$ and $\{A, C\} \not\subset \Gamma_P{}'$.

We call $Z \subset 2^P$ an *adversary structure*, if $Z^c = 2^P \backslash Z$ is a monotone access structure.

**Example:** Given the set of parties $P$ and the access structure $\Gamma_P$ from the previous example, a legal adversary structure would be

$$Z_P = 2^P \backslash \Gamma_P = \{\{A, C\}, \{A\}, \{C\}\, \{\emptyset\}\}.$$

### 3.1.2 Properties

If $Z_1$ and $Z_2$ are adversary structures, then

$$Z_1 + Z_2 = \{z_1 \cup z_2 : z_1 \in Z_1, z_2 \in Z_2\}$$

is also an adversary structure.

**Example:** Given the previously defined adversary structure $Z_P$ and another adversary structure

$$Z_{P'} = \{\{A, B\}, \{A\}, \{B\}, \{\emptyset\}\}$$

we see that

$$Z_P + Z_{P'} = \{\{A, B, C\}, \{A, B\}, \{B, C\}, \{A, C\}, \{A\}, \{B\}, \{C\}, \{\emptyset\}\}.$$

To prove, that it is an adversary structure, we check if the complement is a monotone access structure.

$$Z^c = 2^P \backslash Z_P = \emptyset.$$

$Z^c$ is a monotone access structure, because it satisfies the necessary conditions.

We define $2Z = Z + Z$ and $3Z = Z + Z + Z$.

A set of parties $z \in Z$ is *maximal* if $z' \supset z \Rightarrow z' \notin Z$.

**Example:** The maximal set of parties for $Z_P$ is

$$P_P = \{A, B, C\} \in Z_P.$$

There are two types of adversaries: *passive* and *active*. A passive adversary reads all the traffic of parties in $Z$. An active adversary is computationally unbounded and can both read the traffic from and control the parties in $Z$. Both kinds of adversaries have complete knowledge of the protocol, the message space and structure of the network. The described model considers only static adversaries i.e. ones, who select the set of parties to corrupt before the start of the protocol.

## 3.2 The Communication Network

The communication network is modelled by using a directed graph $G = G(V, E)$. Each node $v \in G$ is a communication party. Each edge $(u, v) \in E$ is a point-to-point private reliable communication channel between the two parties.

## 3.3 Message Transmission Protocols

Let $\pi$ be a message transmission protocol, let $A$ be the sender and $B$ the receiver ($A, B \in P$). Let $Z$ be an adversary structure. The sender $A$ selects a $m^A$ drawn from a message space $M$ with a certain probability distribution.

At the beginning of the protocol the adversary randomly chooses a subset of $Z$ (determines, which nodes to corrupt). At the end of the protocol $\pi$ the receiver $B$ outputs a message $m^B \in M$. For any message transmission protocol $adv(M, r)$ is the view when $m^A = m$ and $r$ is the sequence of coin flips used by the adversary.

**Definition 1:** *Let $\pi$ be a transmission protocol. Let $m^A$ be the message selected by $A$ and $m^B$ the message output by $B$. Let $Z$ be an adversary structure.*

1. *We say that $\pi$ is Z-reliable, if B outputs $m^B = m^A$ with probability 1 (taken over the choices of $m^A$ and the coin flips of all parties).*

2. *We say that $\pi$ is perfectly Z-private if for any two messages $m_0, m_1$ and for any coin tosses r, we have $\Pr[adv(m_0, r) = c] = \Pr[adv(m_1, r) = c]$. The probabilities is taken over the coin flips of the honest parties).*

3. *We say that $\pi$ is perfectly Z-secure if it is Z-reliable and perfectly Z-private.*

### 3.4 Connectivity

**Definition 2:** *Let G(V,E) be a directed graph, A, B be nodes in G(V,E) and Z be an adversary structure on $V\backslash\{A, B\}$.*

- *A, B are* Z-separable *in G, if there is a set $X \in Z$ 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 (Z + 1)-*connected *if they are not Z-separable in G.*

Note, that if $(A, B) \in E$ then $A, B$ are $(Z+1)-connected$ for any Z on $V\backslash\{A, B\}$. There is also the following result.

**Theorem 1:** *Let G = G(V,E) be a directed graph. Let A, B be nodes in G and $Z_1, Z_2$ be adversary structures on $V\backslash\{A, B\}$. Then A, B are $(Z_1 + Z_2 + 1) - connected$ if, and only if: for all sets $X_1 \in Z_1$ 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 $X_1$,
- for every $X_2 \in Z_2$ there is at least one path in $S_{Z_1}$ that is free from nodes of $X_2$.

### 3.5 Secure Message Transmissions

The following results set constraints needed for secure message transmissions in the given network.

**Theorem 2:** *Let G = G(V,E) be a directed graph. Let A, B be nodes in G and Z be an adversary structure on $V\backslash\{A, B\}$. We suppose, that the adversary is passive.*

1. *We have polynomial time (with regard to graph size) Z-reliable message transmission from A to B if, and only if, A, B are $(\{\emptyset\} + 1)$-connected in G.*

2. *We have polynomial time (with regard to graph size) perfectly Z-secure message transmissions from A to B if and only if, A, B, are (Z + 1)-connected in G.*

**Theorem 3:** *Let G = G(V,E) be a directed graph. Let A, B be nodes in G and Z be an adversary structure on $V\backslash\{A, B\}$. We have Z-reliable message transmission from A to B if, and only if, A, B, are (2Z + 1)-connected in G.*

**Theorem 4:** *Let G = G(V,E) be a directed graph. Let A, B be nodes in G and Z be an adversary structure on $V\backslash\{A, B\}$. If there are no directed paths from B to A, then we have perfectly Z-secure message transmission from A to B if and only if, A and B are (3Z + 1)-connected in G.*

## 4 Conclusion

The goal of this survey is to give an introduction to analysing network models. Another survey will be presented to explain other results from the referred article and other works in this area.

## References


[1] D. Dolev, C. Dwork, O. Waarts and M. Yung. "Perfectly secure message transmission." Journal of the ACM, 40(1), pages 17-47, 1993.

[2] M. Hirt and U. Maurer. "Player Simulation and General Adversary Structures in Perfect Multiparty Computation." Journal of Cryptology 13(1), pages 31-60, 2000.

[3] Y.Desmedt, Y.Wang and M.Burmester. "A complete characterization of tolerable adversary structures for secure point-to-point transmissions." Proceedings of the 16th ISAAC, LNCS 3827, pages 277-287, 2005.