MTAT.07.007 Graduate seminar in cryptography

Using Adversary Structures to Analyze Network Models

Dan Bogdanov
University of Tartu
db@ut.ee

Outline of the talk

- Problems in distributed systems
- Adversary Structure - definition
- Communication and Connectivity
- Secure Message Transfer

Problems and results

- Byzantine Generals' Problem
- Byzantine faults
- Communication networks
- Goal of the research
- Some results

The network model

We will define:

- the adversary structure and it's properties
- the communication network
- message transmission protocols
- special connectivity properties
- secure message transmissions

Adversary types

There are two types of adversaries: *passive* and *active*.

- A passive adversary reads all the traffic going through corrupted parties

- An active adversary is computationally unbounded and can both control and read the traffic going through the corrupted parties.

Both types 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.

Adversary structure - definition

Let $\mathcal{P}$ be the set of parties in the network. Let $\Gamma_{\mathcal{P}}$ be a subset of the power set of $\mathcal{P}$. We call such a $\Gamma_{\mathcal{P}} \subset 2^{\mathcal{P}}$ an *access structure* on $\mathcal{P}$.

An access structure is *monotone* if and only if
$\emptyset \notin \Gamma_{\mathcal{P}}$ and $\forall A$ if $A \in \Gamma_{\mathcal{P}}, A \subseteq A' \subseteq \mathcal{P}$ then $A' \in \Gamma_{\mathcal{P}}$.

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

Adversary structure - combining them

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

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

is also an adversary structure.

We define $2\mathcal{Z} = \mathcal{Z} + \mathcal{Z}$ and $3\mathcal{Z} = \mathcal{Z} + \mathcal{Z} + \mathcal{Z}$.

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.

Message Transmission Protocols

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

At the beginning of the protocol the adversary randomly chooses a subset of $\mathcal{Z}$ (determines, which nodes to corrupt). At the end of the protocol π the receiver B outputs a message $M^B \in \mathcal{M}$. 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.

Reliability and privacy

Definition 1: *Let π be a transmission protocol. Let M^A be the message selected by A and M^B the message output by B. Let $\mathcal{Z}$ be an adversary structure.*

1. *We say that π is* $\mathcal{Z}$-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 π is* perfectly $\mathcal{Z}$-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. π *is* perfectly $\mathcal{Z}$-secure *if it is $\mathcal{Z}$-reliable and perfectly $\mathcal{Z}$-private.*

Separability of nodes

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

- *A and B are* $\mathcal{Z}$-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* $\mathcal{Z}$. *We say that* $\mathcal{Z}$ *separates A and B.*

- *A, B are* ($\mathcal{Z}$ + 1)-connected *if they are not* $\mathcal{Z}$*-separable in G.*

Note, that if $(A, B) \in E$ then A, B are $(\mathcal{Z} + 1) - connected$ for any $\mathcal{Z}$ on $V \backslash \{A, B\}$.

Connectivity - results

Theorem 1: *Let G = G(V,E) be a directed graph. Let A, B be nodes in G and* $\mathcal{Z}_1, \mathcal{Z}_2$ *be adversary structures on* $V \backslash \{A, B\}$*. 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.

Secure Message Transmissions - results

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 $\mathcal{Z}$ be an adversary structure on $V \setminus \{A, B\}$. We suppose, that the adversary is passive.*

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

Secure Message Transmissions - results (cont.)

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

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

To be continued...

Next time:

1. More results about the given model.

2. Possibly other models or approaches.

See you then!

End of talk

Thanks for listening!