Consensus With Written Messages Under Link Faults

BETTINA WEISS

ULRICH SCHMID

{bw,s}@auto.tuwien.ac.at

Vienna University of Technology

Department of Computer-Aided Automation

SRDS'01

October 28-31, 2001, New Orleans, USA

http://www.auto.tuwien.ac.at/Projects/W2F/

Motivation

Project W2F

- design a wireline/wireless fieldbus which should be fault-tolerant and secure

  ⇒ we need consensus as a basic service, which can be based on byzantine agreement

- wireless networks suffer from link faults (channel faults, receive buffer overruns, corrupted data bits, ...)

  ⇒ analyze what happens to existing algorithms when there are link faults (impossibility result of Gray)

- we want secure services

  ⇒ analyze algorithms which use authentication and check if they perform better

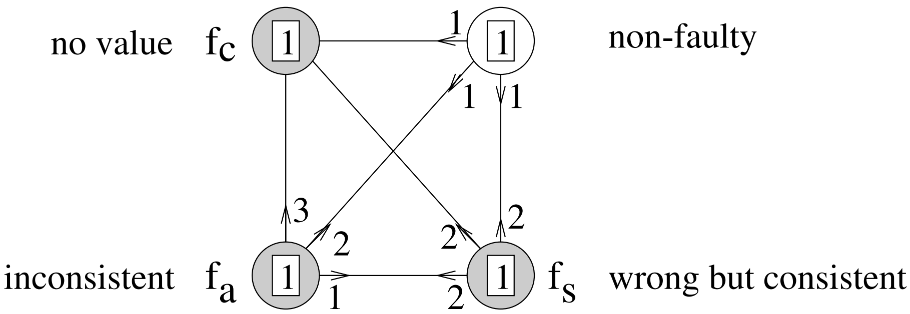
⇒ the authenticated algorithms OMHA and ZA of Gong, Lincoln & Rushby 1995 have everything we need

but: do they work with link faults?

Fault Model

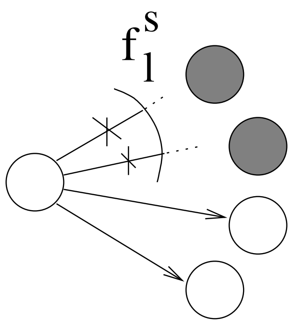
Process Faults: hybrid model, static

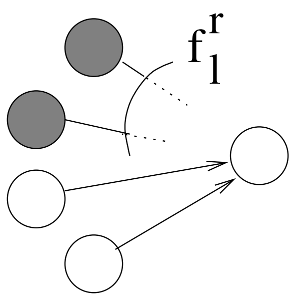
f_s symmetric, f_a arbitrary, f_c manifest faults



Link Faults: dynamic

f_l^s sender link faults f_l^r receiver link faults





The link faults are per node and may change in every send/receive operation.

Impossibility result of Gray is circumvented by restricting the number of link faults.

OMHA & ZA

presented in Gong, Lincoln & Rushby 1995

- solve byzantine agreement problem
- use authenticated messages (signatures)
- derived from unauthenticated algs OMH (Lincoln & Rushby 1993) and Z (Thambidurai & Parks 1988)
- have been analyzed under a hybrid process fault model (Gong, Lincoln & Rushby 1995)

Questions:

- do they also work with link faults?
- does authentication help with link faults?

Results of Analysis

Both algorithms work with link faults!

Number of rounds m:

Validity	$m \geq \min\{1, f_l^s\}$
Agreement	$m \geq f_a + \min\{1, f_l^s\}$

Number of nodes n:

OMH	$2f_l^s + f_l^r + f_l^{ra} + 2(f_a + f_s) + f_c + m + 1$
OMHA	$2f_l^s + f_l^r + 2(f_a + f_s) + f_c + m + 1$
ZA	$f_l^s + f_l^r + f_a + f_s + f_c + 2$

$\Rightarrow$ OMHA benefits from authentication in the presence of link faults, but only slightly

$\Rightarrow$ ZA is much better than OMHA

Broken Signatures

Without authentication:

OMHA $\Rightarrow$ OMH, requires f_l^{ra} nodes more

ZA $\Rightarrow$ Z, has been shown to be flawed

With f_b broken signatures:

affected nodes may behave like arbitrary faulty nodes
$\Rightarrow$ broken signatures are like arbitrary faults

$\Rightarrow$ for f_b broken signatures we get for ZA:

$$m \geq f_a + f_b + min\{1, f_l^s\}$$

$$n > f_l^s + f_l^r + f_a + f_b + f_s + f_c + 1$$

Conclusions

- Both OMHA and ZA work with link faults if the link faults are restricted.
- Algorithm OMHA benefits slightly from authentication.
- Algorithm ZA performs a lot better than OMHA.
- Broken signatures can be handled by assuming that the affected nodes are arbitrary faulty.

Future Work

- Wireless $\Rightarrow$ look at algorithms with constant number of messages (Biely, Schmid 2001).
- Improve the fault model.
- Look at asynchronous algorithms.