Formally Verified Byzantine Agreement in Presence of Link Faults

ULRICH SCHMID, BETTINA WEISS

Technische Universität Wien
Department of Automation
Treitlstraße 1, A-1040 Vienna
{*s, bw*}*@auto.tuwien.ac.at*

JOHN RUSHBY

SRI International
Computer Science Laboratory
Menlo Park CA 94025
Rushby@csl.sri.com

July 5, 2002

ICDCS'02

July 2–5, 2001, Vienna (Austria)

MOTIVATION (1)

Wireless ad hoc networks:

- Mobile computing nodes interconnected by wireless network
- Peer-to-peer communication without central authority (no base-stations)

$\Rightarrow$ **Distributed agreement required in certain cases**

- Many solutions do exist
- BUT: Tolerate node failures only

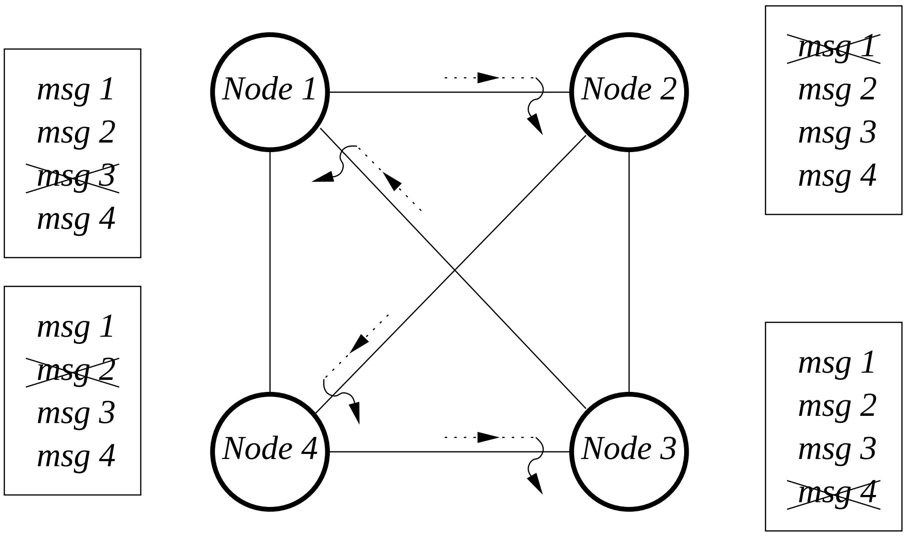
Characteristics of wireless connectivity:

- Incomplete communication graphs
- High link failure rates ($p = 10^{-2}$)
- Omission and even value failures (aggressive FEC)

MOTIVATION (2)

Is it safe to map link failures to node failures ? NO!

1. Worst case: n link failures sufficient to make all n nodes appearing faulty system-wide:



2. High probability that failure models like $f < n/2$ violated: $n = 80, p = 10^{-2}$ yields

$$\textbf{Prob}[\text{more than 40 nodes appear faulty}] \geq 0.33$$

MOTIVATION (3)

What about consensus under link failures ?

⇒ Consult Nancy Lynch's book

⇒ Oops:

Theorem 5.6. (Generals Paradox [Gray, 1978]): There is no deterministic algorithm that solves the coordinated attack problem in a synchronous two-node system with lossy links.

Last resort: Randomized algorithms ?

OUR RESULTS

Deterministic algorithms work perfectly well even in presence of $\mathcal{O}(n^2)$ link failures

Talk outline

- Refined ("perception-based") hybrid failure model for synchronous systems
- Refined analysis of a well-known Byzantine agreement algorithm
- Formal verification
- Analysis of assumption coverage
- Theoretical results on consensus under link failures
- Conclusions

PERCEPTION-BASED FAILURE MODEL

System-wide matrix of messages received in a round:

$$\begin{array}{cc} & \textit{... sender nodes ...} \\ \textit{receiver nodes} & \begin{pmatrix} \mathit{msg}_1^1 & \mathit{msg}_1^2 & \cancel{\mathit{msg}_1^3} & \mathit{msg}_1^4 \\ \cancel{\mathit{msg}_2^1} & \mathit{msg}_2^2 & \mathit{msg}_2^3 & \mathit{msg}_2^4 \\ \mathit{msg}_3^1 & \mathit{msg}_3^2 & \mathit{msg}_3^3 & \cancel{\mathit{msg}_3^4} \\ \mathit{msg}_4^1 & \cancel{\mathit{msg}_4^2} & \mathit{msg}_4^3 & \mathit{msg}_4^4 \end{pmatrix} \end{array}$$

Faulty *msg* either due to (sender-)node or link failure

Traditional failure model:

- $f =$ # columns with fault in ANY row $= 4$ (excessively many)

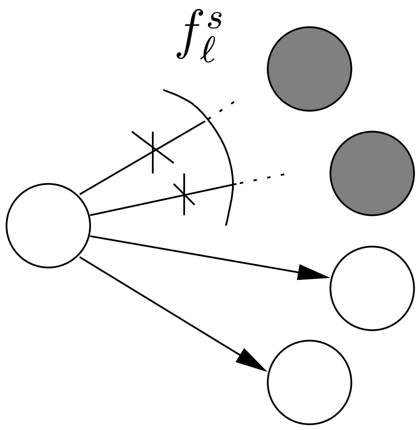
What does consensus really need?

(A) How many faults seen by any SINGLE receiver q ?
$\Rightarrow f_\ell^r =$ # columns with fault in q's row $= 1$

(V) How many receivers perceive fault from SAME sender p ?
$\Rightarrow f_\ell^s =$ # rows with fault in p's column $= 1$

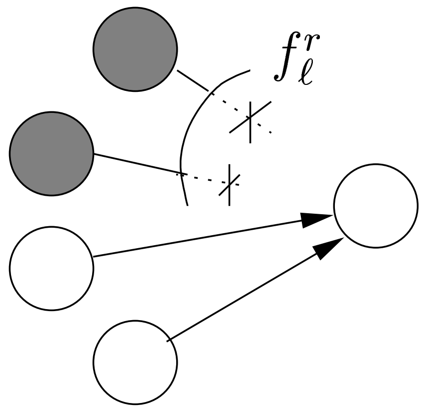
HYBRID PERCEPTION-BASED LINK + NODE FAILURE MODEL

Send link failures:



$f_\ell^{sa} \leq f_\ell^s$ arbitrary ones

Receive link failures:

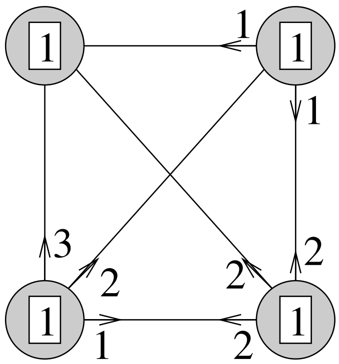


$f_\ell^{ra} \leq f_\ell^r$ arbitrary ones

If more than f_ℓ^s resp. f_ℓ^r link failures $\Rightarrow$ (hybrid) node failure:

f_m manifest faults
(no output to all)

f_a arbitrary faults
(Byzantine)



f_o omission faults
(correct or no output)

f_s symmetric faults
(wrong but consistent)

HYBRID ORAL MESSAGES ALGORITHM (1)

Properties Byzantine Agreement:

- Disseminate dedicated transmitter's value v to all nodes p_i, delivering v_{p_i}
- (*Agreement*): Non-faulty nodes p, q deliver $v_p = v_q$
- (*Validity*): Non-faulty node p delivers
  - $v_p = v$ if transmitter non-faulty
  - $v_p = E$ if transmitter manifest faulty
  - $v_p = v$ or $v_p = E$ if transmitter omission faulty
  - $v_p = X$ if transmitter symmetric faulty

Hybrid Oral Messages (OMH) alg. [Lincoln & Rushby, 1993]:

- Extends oral messages algorithm of [Lamport, Shostak & Pease, 1982] to hybrid node failures
- No changes in the algorithm [except more nodes and one additional round] required for tolerating link failures

HYBRID ORAL MESSAGES ALGORITHM (2)

Execution of OMH:

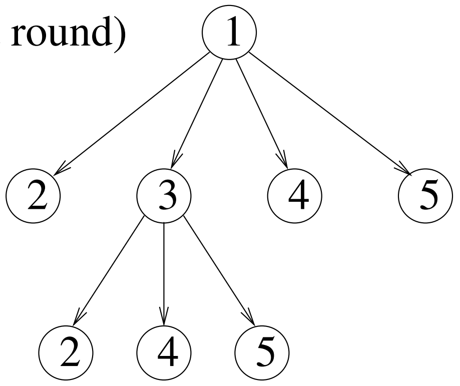
- round-based, constant number of rounds m
- exponential number of messages with $\mathcal{O}(m)$ size
- recursive two-"phase" algorithm:

  Phase 1: forward received values ("downstream")

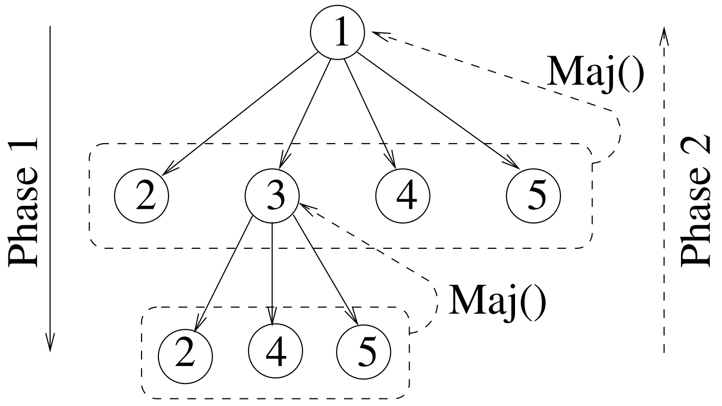
  Phase 2: compute result ("upstream")

Sender's view:

(first round)



Receiver's view:



ANALYSIS RESULTS

Lemma 1 (Validity) *For any $m \geq \min\{1, f_\ell^s\}$, OMH($m$) satisfies validity if $n > 2f_\ell^s + f_\ell^r + f_\ell^{ra} + 2(f_a + f_s) + f_o + f_m + m$.*

Proof by induction:

- Base case $m = 1$ for $f_\ell^s > 0$ is the critical part
- Sufficiently many nodes [due to $2f_\ell^s$] to get enough identical values as input to OMH(0)
- Suff. many nodes [due to $f_\ell^{ra}+f_\ell^r$] to win majority in OMH(1)

Theorem 1 (Agreement and Validity) *For any $m \geq f_a + f_o + \min\{1, f_\ell^s\}$, OMH($m$) satisfies agreement and validity for $n > 2f_\ell^s + f_\ell^r + f_\ell^{ra} + 2(f_a + f_s) + f_o + f_m + m$.*

Proof by induction:

- Transmitter arbitrary or omission faulty only interesting cases
- Proceeding for $f_a + f_o$ additional rounds ensures at least one round with non-arbitrary or omission faulty transmitter

Formal Verification

Results developed through several iterations of

- manual proof
- formal verification

Formal verification

- using PVS
- challenging exercise [Rushby 2001]

Verification benefits:

- Strong assurance for correctness of results despite of extensive case analysis
- Refinement/generalization of failure model and properties
- Detection of erroneous conjecture w.r.t. *uniform* agreement

ANALYSIS OF ASSUMPTION COVERAGE

Is limiting f_ℓ^s and f_ℓ^r in real systems justified ?

- ANY broadcast / reception must obey f_ℓ^s / f_ℓ^r for correctness
- Many, many broadcasts during the execution of OHM

Compute assumption coverage in our simple probabilistic setting:

- Independent link failures with typical wireless probability $p = 0.01$
- Compute probability of failure Q_m that number of link failures in some broadcast resp. reception during OMH(m) exceeds f_ℓ^s resp. f_ℓ^r

ASSUMPTION COVERAGE RESULTS OMH

Theorem 2 (Assumption Coverage OMH) *For $n-m-f_\ell-2 \geq 1$ and $np < 1$ sufficiently small, the probability of failure Q_m of OMH(m) satisfies $Q_m \leq Q'_m$ with*

$$Q'_m \leq \left(1+\frac{1}{n-m-f_\ell-2}\right)[n-1]_{m+f_\ell+1}\frac{p^{f_\ell+1}}{(f_\ell+1)!} = \mathcal{O}\left(n^m (np)^{f_\ell+1}\right)$$

Numerical results for $n = 4f_\ell + 3m + 1$ and $p = 0.01$:

f_ℓ	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$
1	0.01	0.3	1	1	1	1
2	0.002	0.04	1	1	1	1
3	0.0002	0.006	0.3	1	1	1
5	2.10^{-6}	0.00009	0.005	0.3	1	1
7	2.10^{-8}	1.10^{-6}	0.00009	0.007	0.6	1
10	2.10^{-11}	2.10^{-9}	2.10^{-7}	0.00002	0.002	0.2
15	2.10^{-16}	2.10^{-14}	3.10^{-12}	4.10^{-10}	5.10^{-8}	8.10^{-6}
20	2.10^{-21}	2.10^{-19}	4.10^{-17}	7.10^{-15}	1.10^{-12}	2.10^{-10}

THEORETICAL RESULTS (1)

Lower-bound for consensus under omission link failures:

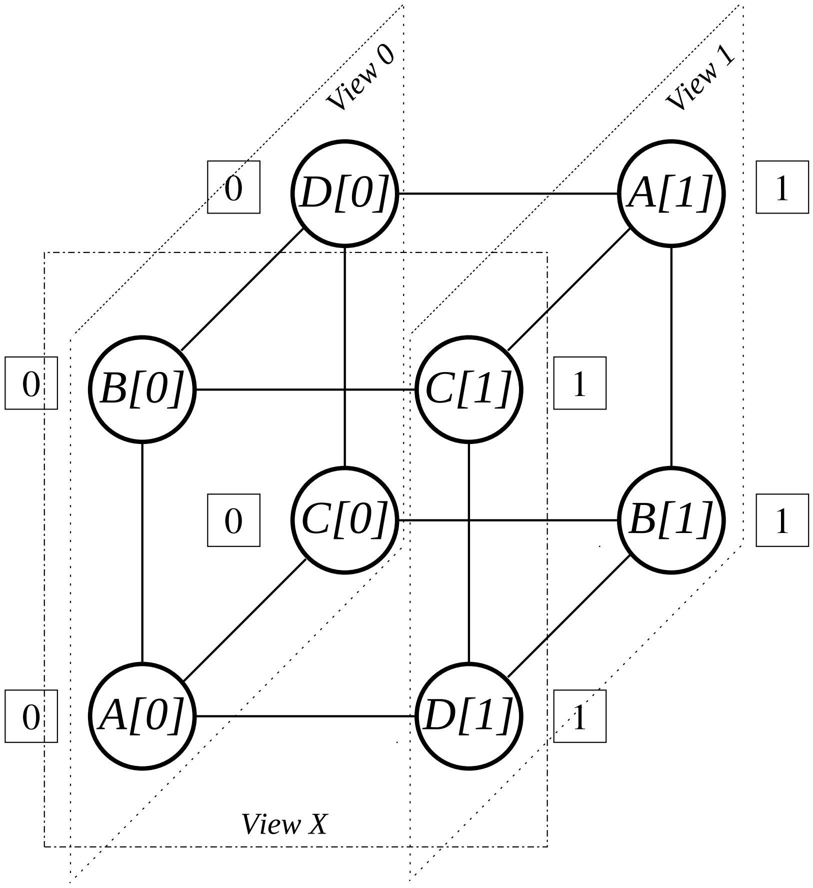
- $n > f_\ell^s + f_\ell^r$
- lower bound is tight since matched by algorithm ZA [Schmid & Weiss, 2001/2002]
- For $f_\ell^s = f_\ell^r$: Reducible to Gray's impossibility result
- For arbitrary f_ℓ^s, f_ℓ^r: Bivalence proof similar to impossibility of consensus in asynchronous systems [Schmid & Weiss, 2002]

Lower-bound for consensus under arbitrary link failures:

- $n > f_\ell^s + f_\ell^{sa} + f_\ell^r + f_\ell^{ra}$
- lower bound is tight since matched by OMH
- For $f_\ell^s = f_\ell^{sa} = f_\ell^r = f_\ell^{ra}$: Reducible to generalization of the Byzantine Agreement's $n > 3f$ "easy impossibility proof" of [Fischer, Lynch & Merrit, 1986]

THEORETICAL RESULTS (2)

Theorem 3 (4-Node Impossibility) *There is no deterministic algorithm that solves consensus for a single arbitrary link failure in a 4-node system.*



THEORETICAL RESULTS (3)

What characterizes Byzantine node failure (in case of OMH) ?

- Any node's send link failures can be viewed as "restricted" Byzantine node failure with inconsistency at most f_ℓ^s
- Consider $f_a = f_s = f_o = f_m = 0$, $f_\ell^r = f_\ell^{ra} > 0$ and fix $n > 2f_\ell^r + 1$ in OMH's major result.

$\Rightarrow$ Two-round algorithm OMH(1) can tolerate f_ℓ^r "restricted" Byzantine node failures with inconsistency

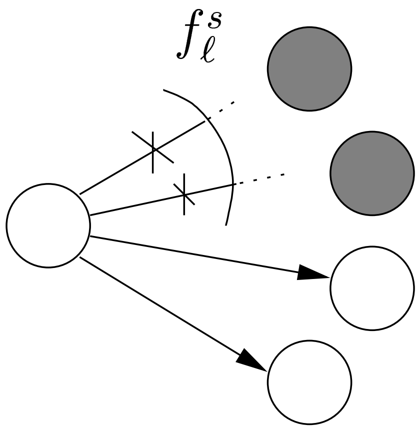
$$f_\ell^s \leq \lfloor n/2 \rfloor - 1 - f_\ell^r$$

$\Rightarrow$ no need to count Byzantine faulty node in f_a (and hence in number of rounds m!) if at least $\lceil n/2 \rceil + 1$ non-faulty receivers get correct information.

- Simplistic impossibility proof of [Gray, 1978] for $n = 2$ obstructed this fact ...

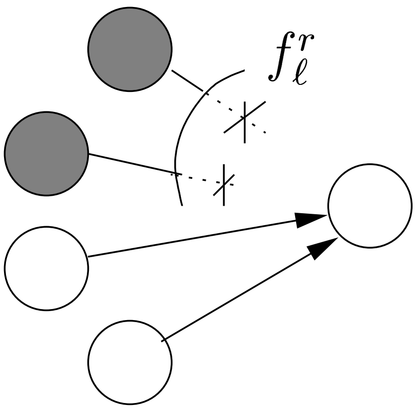
HYBRID PERCEPTION-BASED LINK + NODE FAILURE MODEL

Send link failures:



$f_\ell^{sa} \leq f_\ell^s$ arbitrary ones

Receive link failures:

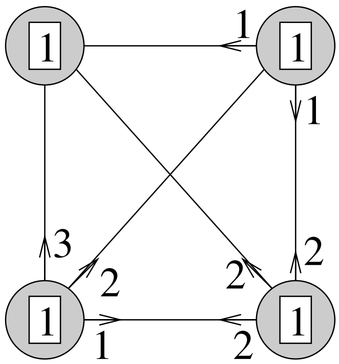


$f_\ell^{ra} \leq f_\ell^r$ arbitrary ones

If more than f_ℓ^s resp. f_ℓ^r link failures $\Rightarrow$ (hybrid) node failure:

f_m manifest faults
(no output to all)

f_a arbitrary faults
(Byzantine)



f_o omission faults
(correct or no output)

f_s symmetric faults
(wrong but consistent)

CONCLUSIONS

Accomplishments:

- Perception-based hybrid failure model for node and link failures
- Consensus under link failures is possible: $\mathcal{O}(n^2)$ link failures tolerable per round system-wide
- Very reasonable assumption coverage
- Formally verified correctness proof for OMH
- Many theoretical results related to link faults

Other work on link failures:

- Authenticated consensus & theory [Weiss & Schmid, 2001/2002]
- Consensus with polynomial messages [Biely & Schmid, 2001]
- Randomized asynchronous consensus [Schmid & Fetzer, 2002]

Hybrid Oral Messages Algorithm (OMH)

OMH(0):

- Transmitter sends v to every receiver
- Receiver p delivers v_p as received from the transmitter, or E in case of no or a manifestly erroneous value

OMH(m), $m > 0$**:**

- Transmitter sends v to every receiver
- Let w_p be the value received by p from the transmitter, or E in case of no or a manifestly bad value

  p acts as the transmitter in Algorithm OMH($m-1$) to communicate $R(w_p)$ to all receivers [including itself]
- Let w_p^q be the value p delivers as the result of OMH($m-1$) initiated by q, or else E if no or a manifestly bad value was delivered

  p calculates the majority among all $w_p^q \neq E$ and applies R^{-1}, delivering the result as v_p

ASSUMPTION COVERAGE RESULTS $\overline{\text{OMH}}$

Modified variant $\overline{\textbf{OMH}}$ where all round R-messages of OMH are packed into a single message

Theorem 4 (Assumption Coverage $\overline{\textbf{OMH}}$) *For $n-m-f_\ell-2 \geq 1$ and $np < 1$ sufficiently small, the probability of failure $\overline{Q}_m$ of $\overline{\text{OMH}}(m)$ satisfies $\overline{Q}_m \leq \overline{Q}'_m$ with*

$$\overline{Q}'_m \leq \frac{[n+1]_{f_\ell+3} - [n-m]_{f_\ell+3}}{f_\ell+3} \cdot \frac{p^{f_\ell+1}}{(f_\ell+1)!} = \mathcal{O}\big(n(np)^{f_\ell+1}\big)$$

Numerical results for $n = 4f_\ell + 3m + 1$ and $p = 0.01$:

f_ℓ	$m=1$	$m=2$	$m=3$	$m=4$	$m=5$	$m=6$
1	0.04	0.1	0.4	0.9	1.	1.
2	0.004	0.02	0.04	0.1	0.2	0.4
3	0.0004	0.002	0.004	0.01	0.02	0.04
5	$5.\,10^{-6}$	0.00002	0.00005	0.0001	0.0002	0.0005
7	$5.\,10^{-8}$	$2.\,10^{-7}$	$5.\,10^{-7}$	$1.\,10^{-6}$	$3.\,10^{-6}$	$5.\,10^{-6}$
10	$5.\,10^{-11}$	$2.\,10^{-10}$	$4.\,10^{-10}$	$1.\,10^{-9}$	$3.\,10^{-9}$	$6.\,10^{-9}$
15	$4.\,10^{-16}$	$1.\,10^{-15}$	$4.\,10^{-15}$	$1.\,10^{-14}$	$2.\,10^{-14}$	$5.\,10^{-14}$
20	$4.\,10^{-21}$	$1.\,10^{-20}$	$3.\,10^{-20}$	$9.\,10^{-20}$	$2.\,10^{-19}$	$5.\,10^{-19}$