Tolerância a Intrusões em Sistemas Distribuídos

alguma pesquisa actual

Miguel Correia
mpc@di.fc.ul.pt
www.di.fc.ul.pt/~mpc

Grupo Navigators, LASIGE
Faculdade de Ciências da Universidade de Lisboa

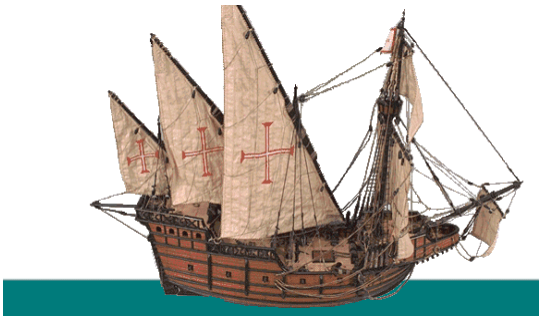
USFC – Florianópolis – 13 de Setembro de 2006

Navigators FCUL

Grupo Navigators

http://www.navigators.di.fc.ul.pt

20º aniversário em 2005 !



Tolerância a Faltas e Intrusões em Sistemas Distribuídos Abertos

- Membros permanentes:
  - Paulo Veríssimo, Nuno F. Neves, Miguel Correia
- Palavras chave:
  - Sistemas distribuídos, Segurança, Tolerância a faltas, Algoritmos distribuídos
- Projetos actuais:
  - **CRUTIAL - Critical UTility InfrastructurAL Resilience**
  - SecurIST - Security and Dependability R&D
  - ESFors – European Security Forum for services, software, systems
  - **Resist - Resilience for Survivability in IST**
  - RITAS - Randomized Intrusion Tolerance for Asynchronous Systems
  - AJECT - Attack Injection on Software Components

Tempo e Adaptação em Sistemas Confiáveis

- Membros permanentes:
  - Paulo Veríssimo, António Casimiro, José Rufino
- Palavras chave:
  - Sistemas distribuídos, Tempo-real, Sistemas embutidos, Tolerância a faltas, Adaptação
- Projetos actuais:
  - **HIDENETS - HIghly DEpendable ip-based NETworks and Services** (IST)
  - DARIO - Distributed Agency for Reliable Input/Output
  - TACID - Timely ACID Transactions in DBMS

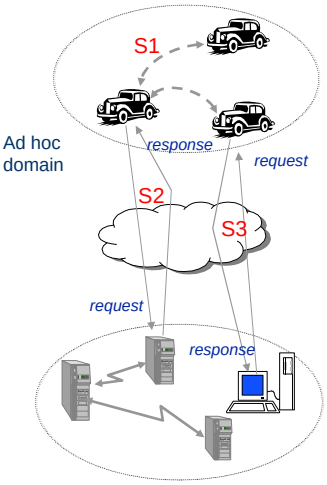
HIDENETS – HIghly DEpendable ip-based NETworks and Services

Challenges

- Dynamically changing communication
- Off-the-shelf, standard systems and components
- Services with high dependability and scalability requirements

Use-case of ad-hoc car-to-car communication with connectivity to infra-structure services

Develop and analyze end-to-end resilience solutions

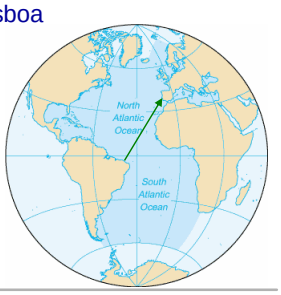


http://www.hidenets.aau.dk/

HIDENETS

Tolerância a Intrusões em Sistemas Distribuídos (TISD)

- Cooperação DAS/UFSC+PUC-PR com Univ. Lisboa
  - Projecto CAPES/GRICES
- Até agora…
  - 2 doutorados sanduíche
  - 1 aluna de doutorado brasileira na Univ. Lisboa
  - Vários artigos em comum
  - Minha viagem aqui…

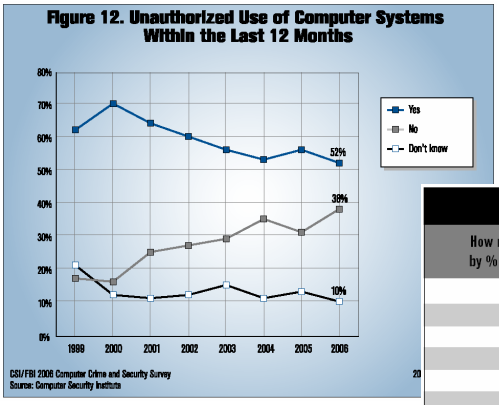


Sumário

- Motivação à TI
- Tolerância a Intrusões
- Wormholes e Replicação de Máquinas de Estados TI
- Protocolos Aleatórios Tolerantes a Intrusões
- Conclusões e outros trabalhos

Motivação

Custo de intrusões (I)



CSI/FBI 2006 Computer Crime and Security Survey

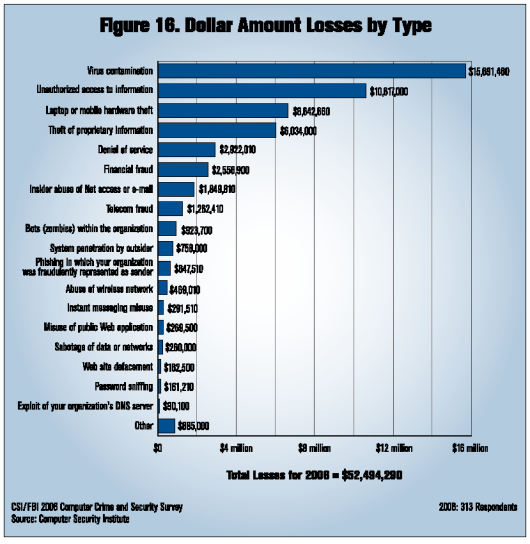
Inquéritos a empresas, agências governamentais, instituições financeiras, universidades

Table 1: How Many Incidents?

How many incidents, by % of respondents	1–5	6–10	>10	Don't know
2006	48	15	9	28
2005	43	19	9	28
2004	47	20	12	22
2003	38	20	16	26
2002	42	20	15	23
2001	33	24	11	31
2000	33	23	13	31
1999	34	22	14	29

CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute
2006: 341 Respondents

Custo de intrusões (II)



Para os custos "em dólares" há soluções não técnicas:

- tribunais
- seguros

mas os custos estão a deixar de ser apenas "em dólares"

Infraestruturas Críticas

- A nossa vida depende de um conjunto de infra-estruturas críticas controlados informaticamente: eléctrica, água, gás, esgotos,…
- Evoluíram de
  - Sistemas isolados baseados em hardware e software especializado, para
  - Sistemas distribuídos interligados por redes convencionais (TCP/IP, wireless) e hw/sw comuns
- Logo actualmente estão vulneráveis como os sistemas distribuídos convencionais…
- … mas a questão já não são "dólares"

Ataques a Infraestrut. Críticas

- Jan. 03, EUA – central nuclear Davis-Besse
  - O worm Slammer entrou na rede de gestão e depois na rede de controle através da rede de um fornecedor
  - Parou dois sistemas críticos de supervisão
- Dez. 00, EUA –
  - Um grupo de hackers atacaram os servidores de um fornecedor de energia eléctrica para jogarem jogos interactivos
  - Consumiram 95% da largura de banda
- Etc etc…

Fiabilidade de Sistemas Críticos

- O problema é semelhante à fiabilidade de sistemas críticos como: aviões, centrais nucleares, foguetes, submarinos…
  - Em caso de falha… vidas humanas
- Confiança no Funcionamento (CnF) / Dependability:
  - Prevenção de faltas
  - Tolerância a faltas
  - Supressão de faltas
  - Previsão de faltas

Infraestruturas Críticas

- Projecto CRUTIAL (EU-IST)
  - Critical UTility InfrastructurAL Resilience
  - CESI RIC. (It), KUL (Be), CNR-ISTI (It), CNIT (It), LAAS-CNRS (Fr), **FCUL (Pt)**
  - http://crutial.cesiricerca.it/
- Vamos usar **Tolerância a Intrusões (TI)** para *controlar o acesso* às redes de gestão e controle

  CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture.

  Paulo Veríssimo, Nuno F. Neves, Miguel Correia.

  CRITIS 2006

Tolerância a Intrusões

Tolerância a Intrusões

- O conceito surgiu no artigo:

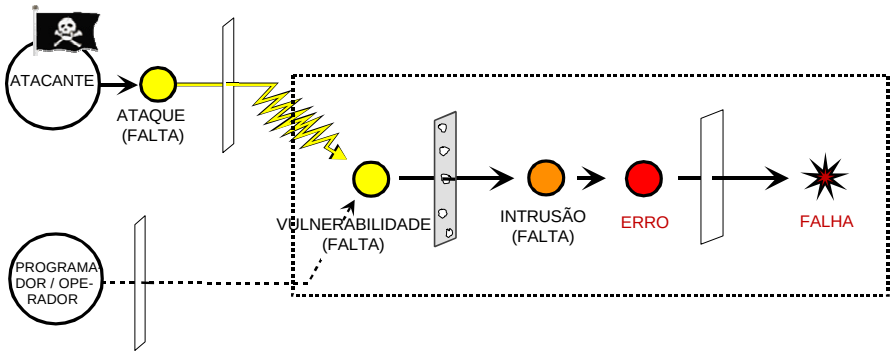
  Joni Fraga, David Powell.
  A fault- and intrusion-tolerant file system.
  Proc. Int'l Conf. on Computer Security, 1985

- Mas só por volta de 2000 a área "estourou"
  - ☞Projecto MAFTIA (UE), programa OASIS (EUA), etc.

Tolerância a Intrusões

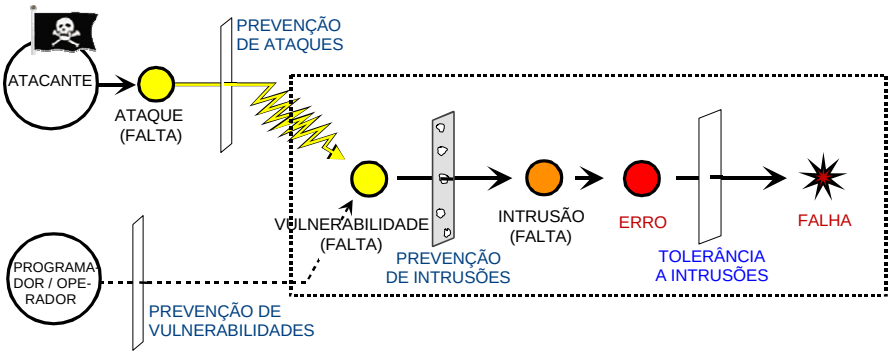
- A ideia consiste em *aplicar o paradigma da Tolerância a Faltas no domínio da Segurança*
  - ☞assumir e aceitar que o sistema permanece sempre mais ou menos vulnerável;
  - ☞assumir e aceitar que os componentes do sistema podem ser atacados e que alguns desses ataques terão sucesso;
  - ☞garantir que o sistema como um todo permanece seguro e operacional, ou seja, que não falha.

Modelo AVI– Processo de Falha



Projecto MAFTIA
www.maftia.org

Modelo AVI– Meios p/Evitar a Falha

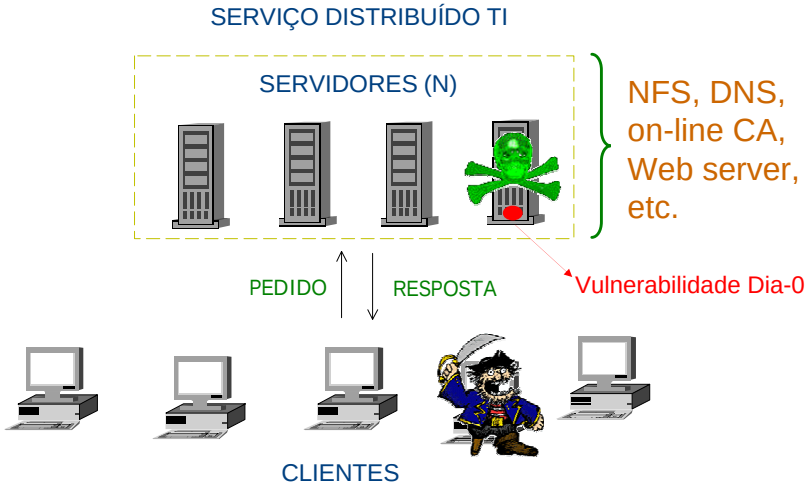


Meios de CnF e serv.dist.TI

- O projecto de serviços distribuídos TI envolve os quatro meios de CnF referidos:
- Prevenção, supressão e previsão de faltas são importantes mas não são específicos da TI
- Tolerância a faltas:
  - ☞a maior parte das soluções usam mascaramento de faltas: redundância de máquinas + protocolos tolerantes a faltas bizantinas
  - ☞processamento de erros: recuperação proactiva

TI não substitui os meios de Segurança!!

Ex: Serviços distribuídos TI



Wormholes e Replicação de Máquinas de Estados TI

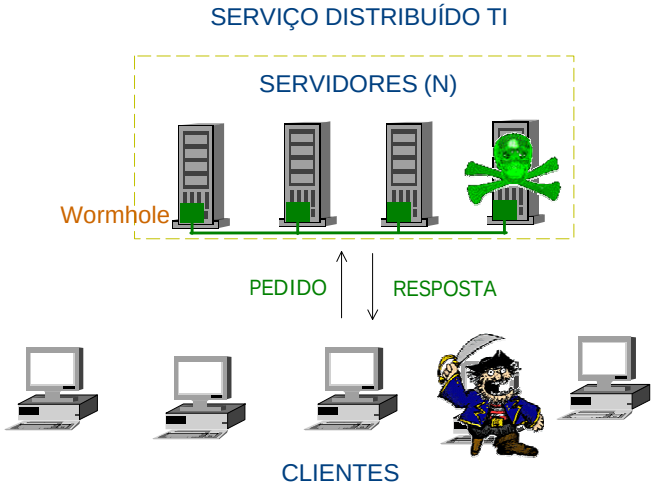
Trabalho com Nuno F. Neves e Paulo Veríssimo

How to Tolerate Half Less One Byzantine Nodes in Practical Distributed Systems. SRDS 2004

Wormholes

- Muitos trabalhos em sistemas distribuídos consideram um sistema homogéneo: computadores interligados por uma rede:
  - ☞Todo o sistema manifesta a mesma incerteza *temporal, de segurança,…*
- Hoje em dia não precisa de ser assim, o sistema pode ser híbrido:
  - ☞Podem existir componentes com diferentes tipos/graus de incerteza
  - ☞Partes mais atempadas, *mais seguras*,… (p.ex., trusted computing)

Ex: Serviço distribuído TI



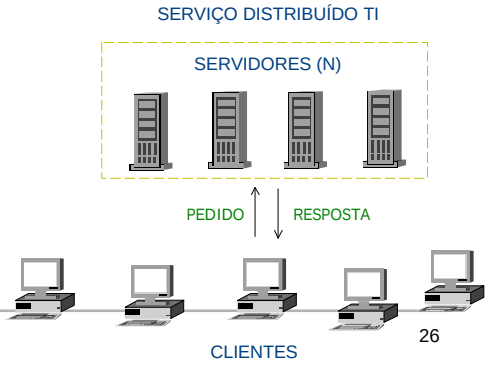
O que se ganharia tendo um Wormhole?

Nossa contribuição

- Em todos os modelos de sistemas distribuídos "práticos" (~ assíncrono), são necessários **3f+1** servidores para tolerar **f** falhados
- Com um *wormhole* seguro precisamos apenas de **2f+1**
  - ☞ Uma poupança de 25% a 33% no número de servidores…
  - ☞ … e um servidor é caro:
    - Necessidade de diversidade
    - Hardware, software, gestão

Replicação de Máq.de Estados

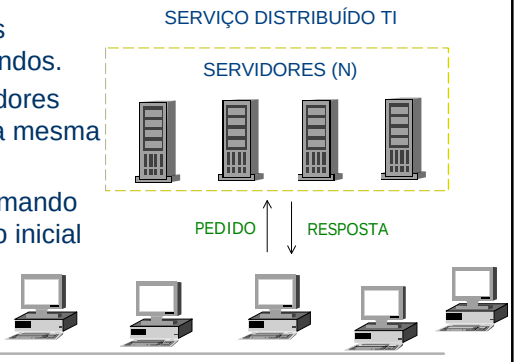
- …ou *replicação activa*
- solução genérica para a concretização de *serviços* tolerantes a faltas/intrusões
- cada servidor é uma máquina de estados definida por
  - ☞ variáveis de estado;
  - ☞ comandos atómicos



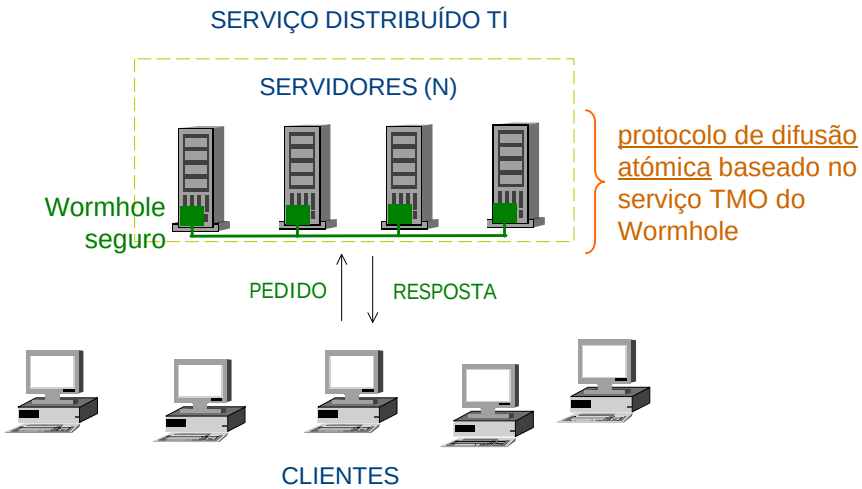
Replicação de Máq.de Estados

- todos os servidores seguem a mesma sequência de estados sse:
- Estado inicial. Todos os servidores começam no mesmo estado.
- Acordo. Todos os servidores executam os mesmos comandos.
- Ordem total. Todos os servidores executam os comandos pela mesma ordem.
- Determinismo. O mesmo comando executado no mesmo estado inicial gera o mesmo estado final.

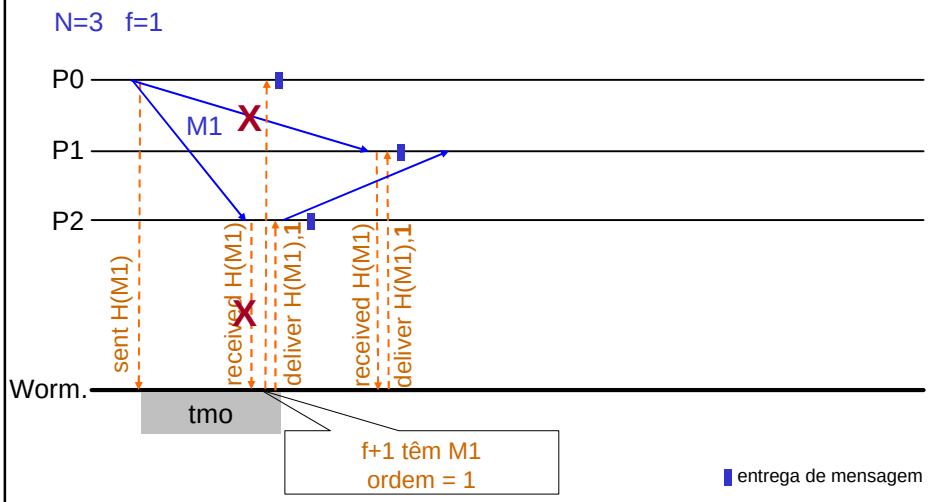
protocolo de difusão atómica



RME com Wormhole



Difusão atómica com o TMO



Serviço TMO

- Núcleo da solução
  - ☞Decide quando uma mensagem pode ser entregue
    - – se **f+1** servidores mostram que têm a mensagem, então pelo menos um correcto tem
  - ☞Define uma ordem sequencial para as mensagens
  - ☞Resultados são confiáveis pois o Wormhole é seguro
- Concretização do serviço TMO
  - ☞Quando há uma mensagem, Wormholes locais execut um *protocolo de acordo* para decidirem o nº de ordem
  - ☞Esse protocolo é executado num ambiente benigno, não tem de tolerar faltas bizantinas

Envio de pedidos

- Os clientes têm relógios locais (não confiáveis) Protocolo:
  - Enviar o pedido para um servidor protegido por um *vector de MACs*
  - Esperar por **f+1** respostas idênticas de servidores diferentes
  - Se T_{resend} depois do pedido ter sido enviado não tiverem sido recebidas as respostas, reenviar para **f** servidores adicionais

Protocolos Aleatórios Tolerantes a Intrusões

Trabalho com
Henrique Moniz, Nuno F. Neves, Paulo Veríssimo

Randomized Intrusion-Tolerant Asynchronous Services. DSN 2006.

Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols. SRDS 2006.

Protocolos aleatórios

- O **consenso** é um problema fundamental em sistemas distribuídos
  - Dado um conjunto de N processos distribuídos, cada um com um valor inicial
  - Como conseguir que todos escolham o mesmo valor entre esses?
- No modelo assíncrono em que os processos possam falhar, não existe solução determinística para o problema (FLP 1985)
- Mas existem soluções probabilísticas ou **aleatórias** (randomized)
  - Protocolos que "jogam uma moeda ao ar"

Nossa contribuição

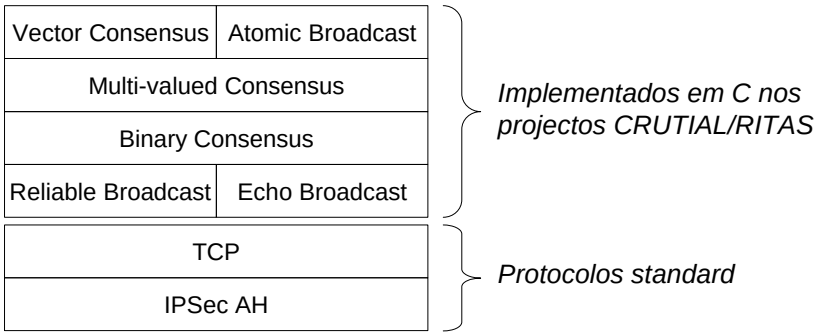
- Duas "lendas" do folclore de sistemas distribuídos:
- **Lenda 1**: os protocolos aleatórios são demasiado lentos para serem usados na prática
  - Foram publicados na área da *teoria dos SDs* mas quase não há publicações na área de *sistemas*
- **Lenda 2**: os protocolos aleatórios baseados em *moeda local* são mais lentos do que os baseados em *moeda partilhada*
- Mostrámos que em grande medida são infundadas
  - Projectos CRUTIAL e RITAS
    - Randomized Intrusion-Tolerant Asynchronous Services – http://ritas.di.fc.ul.pt

Lenda 1

"Os protocolos aleatórios são demasiado lentos para serem usados na prática"

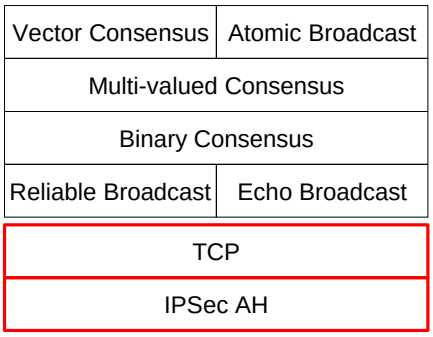
(artigo DSN 2006)

Pilha de protocolos TI RITAS



Os 3 protocolos do topo foram apresentados em "From Consensus to Atomic Broadcast: Time-Free Byzantine-Resistant Protocols without Signatures", M. Correia, N. Neves, P. Veríssimo. Computer Journal, Jan. 2006

Pilha de protocolos TI RITAS



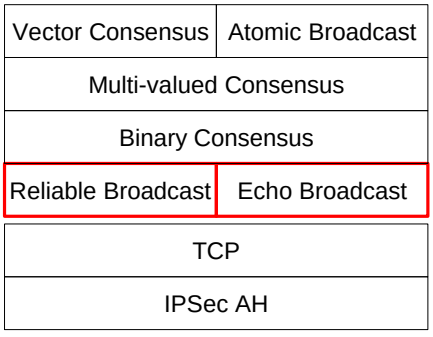
Reliable Channels

Fornecem 2 propriedades:

- **Integridade**: IPSec Authentication Header (AH) protocol

- **Fiabilidade**: TCP

Pilha de protocolos TI RITAS



Reliable Broadcast

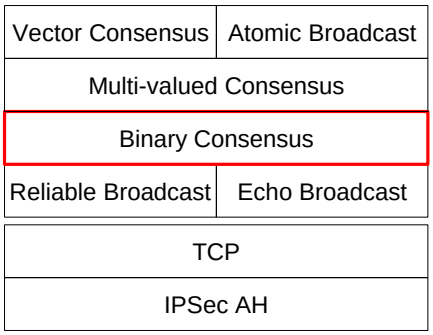
Garante que todos os processos correctos entregam a mesma mensagem (ou nenhuma). Bracha 83

Echo Broadcast

Mais fraco mas mais eficiente do que o anterior

Garante que os processos correctos *que entregam a mensagem,* entregam a mesma mensagem. Toueg 84, Reiter 96

Pilha de protocolos TI RITAS



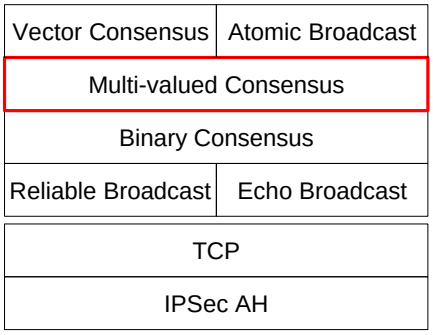
(Randomized) Binary Consensus

Permite aos processos correctos fazerem *consenso* sobre um valor binário (0 ou 1)

O protocolo usado foi o proposto por G. Bracha em 1983

- Não usa criptografia
- Corre num nº de ciclos esperado de 2^{n-f}

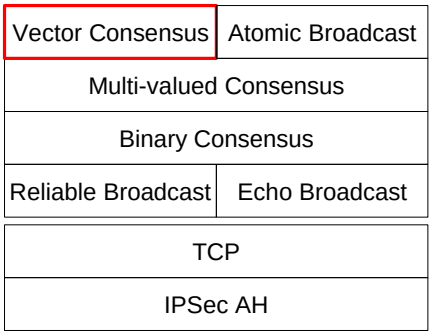
Pilha de protocolos TI RITAS



Multi-valued Consensus

Permite aos processos correctos fazerem *consenso* sobre um valor de tamanho arbitrário (não apenas binário)

Pilha de protocolos TI RITAS

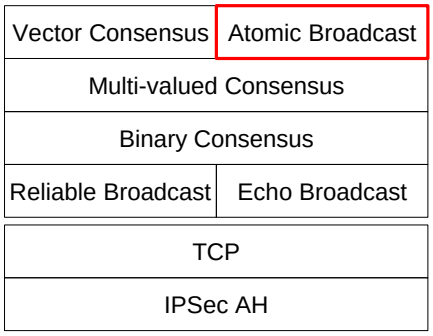


Vector Consensus

Permite aos processos correctos fazerem *consenso* sobre um *vector* com um valor por cada processo (o valor inicial do processo ou um valor especial)

Pelo menos f+1 valores do vector são de processos correctos

Pilha de protocolos TI RITAS



Atomic Broadcast

Difusão atómica ou com ordem total

Lembrar que é a base da replicação de máquinas de estados!

Logo poderíamos usar estes protocolos para concretizar qualquer serviço distribuído TI

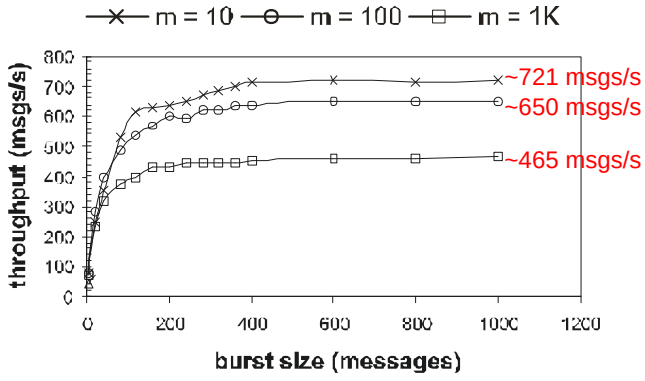
…mas a resistência seria **3f+1**

Latência de execuções isoladas

	w/ IPSec (μs)
Echo Broadcast	1724
Reliable Broadcast	2134
Binary Consensus	8922
Multi-valued Consensus	16359
Vector Consensus	20673
Atomic Broadcast	23744

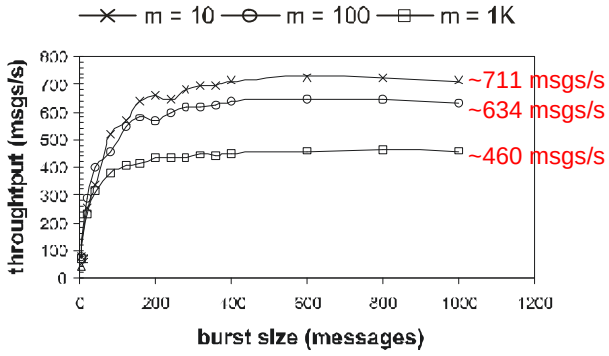
Débito da difusão atómica (I)

- Sem faltas, n=4



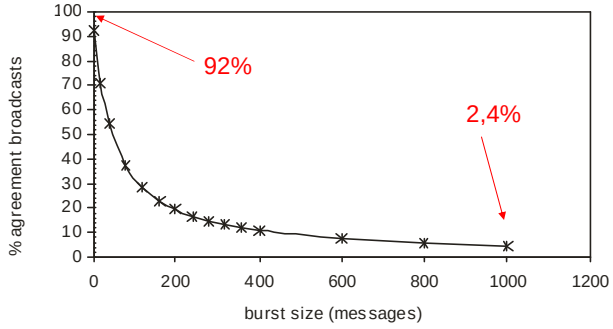
Débito da difusão atómica (II)

- **f** processos maliciosos
  - ☞Desempenho quase não é afectado pelos ataques



Justificação da eficiência

- O modelo do adversário considerado nos artigos teóricos é pouco realista quando se vai medir o desempenho
  - ☞ Assume controle do escalonamento das mensagens
- Os protocolos não são executados no meio de nada
  - ☞ *Percentagem de difusões que são devidas a consensus (e não à difusão atómica em si):*



Lenda 2

"Os protocolos aleatórios baseados em *moeda local* são mais lentos do que os baseados em *moeda partilhada*"

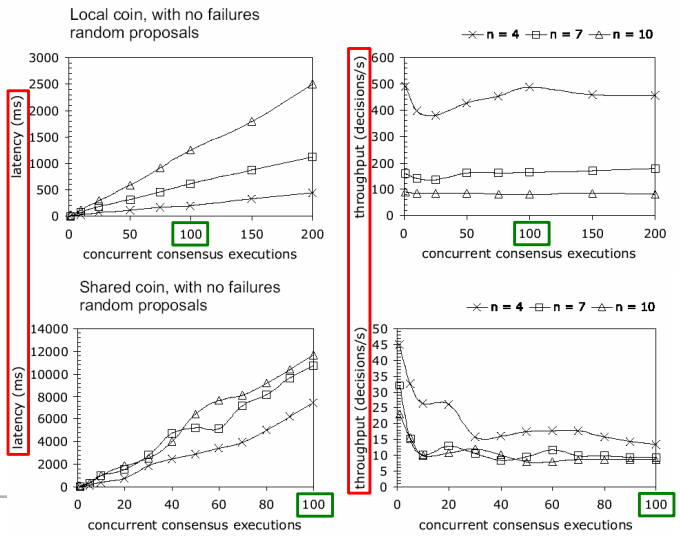
(artigo SRDS 2006)

Dois tipos de protoc. aleatórios

- Protocolos de consenso binário; moeda vale 0 ou 1
- **Moeda local**: cada processo pode gerar números aleatórios locais, ou seja, *atira a sua moeda ao ar*
  - Testámos o protocolo de Bracha 1983
  - Terminação esperada em 2^{n-f} ciclos
- **Moeda partilhada**: todos os processos têm acesso aos mesmos valores da *moeda*
  - Testámos o protocolo mais eficiente disponível, ABBA (Cachin, Kursawe, Shoup 2001)
  - Termina sempre em 1 ou 2 rounds!
  - Mas usa cripto assimétrica ("pesada")

Latência média (burst) e débito

Moeda local



Moeda global

- A moeda local bateu sempre a global (LAN)
- Latência do burst, não de 1 msg

Número de ciclos

	Local Coin		
	$n = 4$	$n = 7$	$n = 10$
failure-free	1,004 (0,42)	1,005 (0,14)	1,009 (0,19)
fail-stop	1,000 (0)	1,000 (0)	1,000 (0)
Byzantine	1,462 (1,52)	1,569 (1,69)	2,289 (2,79)

	Shared Coin		
	$n = 4$	$n = 7$	$n = 10$
failure-free	1,013 (0,23)	1,018 (0,27)	1,010 (0,20)
fail-stop	1,000 (0)	1,000 (0)	1,000 (0)
Byzantine	1,016 (0,25)	1,017 (0,26)	1,012 (0,22)

Conclusões e outros trabalhos

Conclusões (I)

- Usando um *wormhole* é possível concretizar serviços distribuídos TI reduzindo consideravelmente o número de réplicas (logo o custo)
- Outras contribuições para a TI do uso de wormholes:
  - ☞protocolos simples e eficientes
  - ☞dispensar hipóteses temporais sobre o sistema "normal"
  - ☞contornar impossibilidade de fazer recuperação proactiva em sistemas assíncronos (Sousa, Veríssimo, Neves)

Conclusões (II)

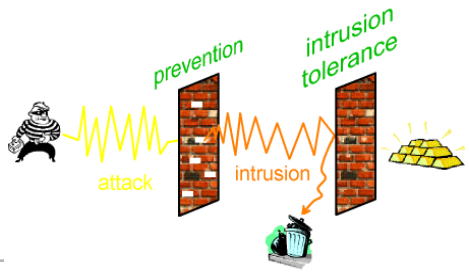
- Os protocolos aleatórios podem ser eficientes sob condições realistas
  - Existe uma diferença considerável entre os resultados teóricos e a prática
  - Num protocolo útil como a difusão atómica, o custo do consenso pode ser diluído quando o débito aumenta
- Protocolo de moeda local teve sempre melhor desempenho do que os de moeda partilhada
  - LANs, até 10 processos
  - Aumentando o tempo de comunicação ou o nº de processos isso pode mudar (PlanetLab)

Outro trabalho

- Injecção de ataques em serviços distribuídos
  - c/ João Antunes, Nuno Neves, P. Veríssimo
- Detecção de intrusões em redes Ethernet/STP
  - c/ Pan Jieke, João Redol (Siemens)
- Gestão de *buffers* em sistemas distribuídos tolerantes a intrusões
  - c/ Giuliana Santos, Lau Lung (PUCPR)
- Problemas de segurança em software para processadores de 64 bits
  - c/ Ibéria Medeiros

Perguntas?

- Página pessoal
  http://www.di.fc.ul.pt/~mpc
- Grupo Navigators:
  http://www.navigators.di.fc.ul.pt/
- Email:
  mpc@di.fc.ul.pt



Para saber mais...

- Sobre tolerância a intrusões no geral
  - M. P. Correia. **Serviços Distribuídos Tolerantes a Intrusões: resultados recentes e problemas abertos**. V SBSeg - Livro Texto dos Minicursos, 2005
  - P. Veríssimo and N. F. Neves and M. Correia. **Intrusion-Tolerant Architectures: Concepts and Design.** In *Architecting Dependable Systems*, LNCS 2677, Springer, 2003
- Artigos em revistas
  - M. Correia, N. F. Neves, L. C. Lung, P. Veríssimo. **Worm-IT - A Wormhole-based Intrusion-Tolerant Group Communication System**. Journal of Systems & Software, Elsevier, 2006. to appear
  - M. Correia, N. F. Neves, P. Veríssimo. **From Consensus to Atomic Broadcast: Time-Free Byzantine-Resistant Protocols without Signatures**. Computer Journal. vol. 41, n. 1, pp 82-96, January 2006
  - N. F. Neves, M. Correia, P. Veríssimo. **Solving Vector Consensus with a Wormhole**. IEEE Transactions on Parallel and Distributed Systems, Volume 16, Issue 12, Dec. 2005
  - M. Correia, N. F. Neves, L. C. Lung, P. Veríssimo. **Low Complexity Byzantine-Resilient Consensus**. Distributed Computing, vol. 17, n. 3, pp. 237--249, March 2005.
- Artigos recentes em conferências
  - P. Veríssimo, N. F. Neves and M. Correia. **CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture**. *In CRITIS'06 1st International Workshop on Critical Information Infrastructures Security.* August 30 - September 2, 2006.
  - H. Moniz and N. F. Neves and M. Correia and P. Veríssimo. **Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols**. *27th IEEE Symposium on Reliable Distributed Systems*. October 2006
  - H. Moniz and N. F. Neves and M. Correia and P. Veríssimo. **Randomized Intrusion-Tolerant Asynchronous Services**. *International Conference on Dependable Systems and Networks (DSN),* June 2006.
  - N. F. Neves and J. Antunes and M. Correia and P. Veríssimo and R. Neves. **Using Attack Injection to Discover New Vulnerabilities**. *International Conference on Dependable Systems and Networks (DSN),* June 2006.
  - A.N.Bessani and M.Correia and J.S.Fraga and L.C.Lung. **Sharing Memory between Byzantine Processes using Policy-Enforced Tuple Spaces**. *26th International Conference on Distributed Computing Systems,* July 2006.