On the use of admission control for better quality of security

Sobre o uso de controle de admissão para uma melhor qualidade de segurança

Svetlana Radosavac and Ulaş C. Kozat and James Kempf
Apresentado por: Eduardo da Silva

IEEE ICC 2009

Objetivo Geral

Propor uma **política de controle de admissão** que admita usuários o mais rápido possível, limitando o impacto de segurança na rede e a outros usuários.

Roteiro

- Introdução
- Trabalhos relacionados
- Modelo do sistema
- Política de controle de admissão
- Resultados das simulações
- Conclusão
- Análise crítica

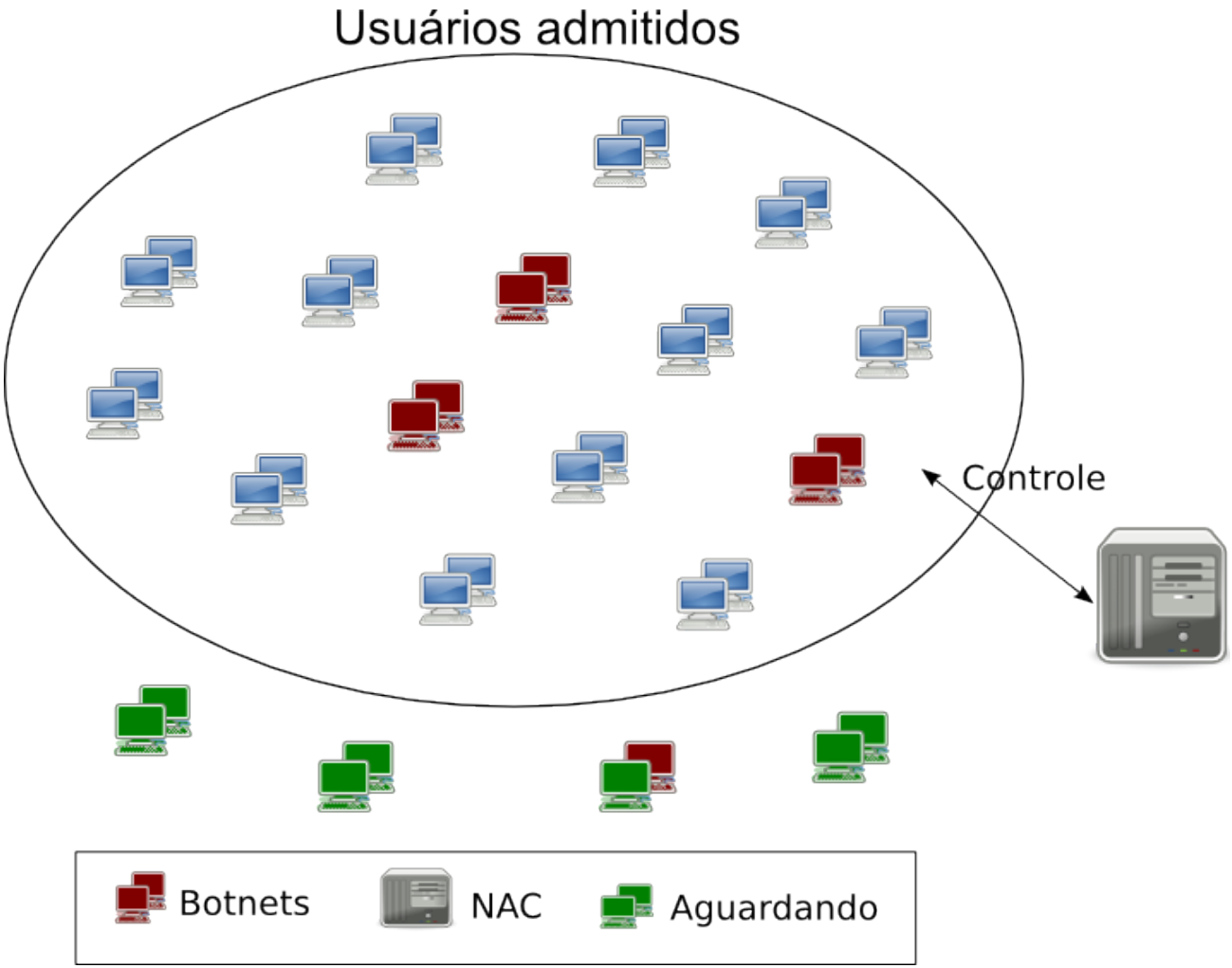
Introdução

Contextualização

- Rede de acesso pública **segura**
  - Acesso de usuário e tráfego **mais controlados** que a Internet
  - Indicada para transações seguras $\longrightarrow$ bancos
  - Entrada e saída de nós aumentam sua **vulnerabilidade**
- Segmentos de VLANs para usuários que retornam
  - Comum em redes corporativas
  - Controle de admissão estático
  - Gera um **atraso** muito longo
  - Atrasos longos: inaceitáveis para redes como WLAN e 3G
    - Usuários se conectam para transações curtas

Introdução

Risco de ataques



Introdução

Solução proposta

Para quantificar a probabilidade de um *botnet*

- Avalia a probabilidade um usuário se membro de um *botnet*
- Baseada na reputação do usuário
  - Histórico de comportamento
  - Inspeção de dispositivos e *scanning*
- Considera o prejuízo esperado/admissível da rede
- Pretende maximizar a soma das “utilidades” dos usuários admitidos
  - “Utilidade”: benefícios do usuário

Trabalhos relacionados

- Cunningham [1985]:
  - Considera ataque DDoS ótimo
  - “Robustez” da rede: resistência da rede a ataques de DDoS
- Vários algoritmos propostos $\longrightarrow$ aumentar a robustez das redes
- Controles de Admissão de Rede, como Cisco NAC Appliance:
  - Executam verificação de segurança de dispositivo
  - Identidade
  - Segurança da rede
- Pesquisas recentes:
  - Tentam modelar e resolver os problemas de segurança
  - Usam modelagem de risco, economia de rede e incentivos
  - Métodos baseados em compensação
  - Técnicas tem sido pouco adotadas na prática [2007]

Modelo do sistema

- Usuário desconectado devido a um ataque
  - Sofre perdas financeiras
  - Operador da rede compensa o usuário
- Mais usuários admitidos $\rightarrow$ maior a “utilidade” da rede
- Assume-se:
  - Probabilidade de um usuário ser comprometido: independente dos outros usuários

- **Objetivo**
  - Admitir novos usuários rapidamente
  - Manter o prejuízo esperado abaixo de um patamar

Modelo do sistema

- Cada usuário u_i possui dois parâmetros
  - p_i: nível de confiança que a rede possui no usuário (entre 0 e 1)
  - r_i: taxa de injeção de tráfego

Quando usuário u_i solicita acesso à rede

O sistema ou operador da rede:

1. Determina sua reputação inicial $p_{i,0}$
2. Toma uma decisão de admissão baseado no risco total
3. Reputação do usuário: avaliada e atualizada em tempo real
   - $p_i = p_{i,0} + g(\tau_i)$
   - $g(\tau_i)$: função não-negativa não-descrescente do atraso de admissão τ_i
   - Assume-se: $g(\tau_i) = \alpha\tau_i$. α é uma constante positiva

Modelo do sistema

Prejuízo causado por um subconjunto B_i ($D(B_i)$)

- $B_i = u_{i1}, ..., u_{im}$: usuários admitidos e esperando por admissão
- Assim, $\sum_i = \sum_{j=1}^{m} r_{ij}$
- Sendo $f(\sum_i)$: função monótona não-descrescente
- Então $D(B_i) = f(\sum_i)$

Probabilidade de dano de um subconjunto B_i

- $\pi_i = \prod_{j \in B_i} (1 - p_j)$
- $(1 - p_j)$: probabilidade de j se tornar malicioso

Modelo do sistema

Prejuízo esperado do sistema

- $E_B[D] = \sum_{i \in B} \pi_i D(B_i)$ ou $E_B[D] = \gamma \sum_{i=1}^{N} (1 - p_i) r_i$
- Política de controle de admissão garante $E_B[D] \leq \Gamma_{th}$
  - Γ_{th}: patamar baseado no dano tolerável para a rede

Por fim, assume-se

- Cada usuário possui uma função "utilidade" $U_i(\tau_i)$ concava e descrecente
  - Quanto menor o tempo de espera $\rightarrow$ usuário mais satisfeito
  - Longos atrasos de admissão $\rightarrow$ diminui a "utilidade" do usuário

Política de controle de admissão

- Decidir se admiti um usuário em um dado tempo

Atender às seguintes restrições

1. $max \sum_i^N U_i(\tau_i)$
2. $E_B[D] \leq \Gamma_{th}$

Maximizar a utilidade dos usuários admitidos

Utilidade de um usuário depende do seu atraso de admissão

- Usuário não precisa esperar até a finalização do *scanning* ou aplicação de *patches*
- Se o risco que ele adiciona ao sistema é aceitável:
  - Ele pode ser admitido imediatamente
  - *Scanning* e atualização da reputação continuam

Política de controle de admissão

- Aplicando a função de Lagrange nas equações
  - Para encontrar os valores de otimização
  - Sendo λ e μ_i como os multiplicadores de Lagrange
- Usando o teorema de Kuhn-Tucker
  - Para encontrar a solução ótima do problema, sujeito a restrições
- Sendo A, os usuário que foram admitidos antes de alcançar o nível máximo de reputação, o atraso de admissão é:

$$\tau_i = \begin{cases} (1 - p_{i0})/\alpha; i \notin A \\ U_i'^{-1}\left[-\alpha\gamma r_i \lambda\right]; i \in A \end{cases}$$

Resultados

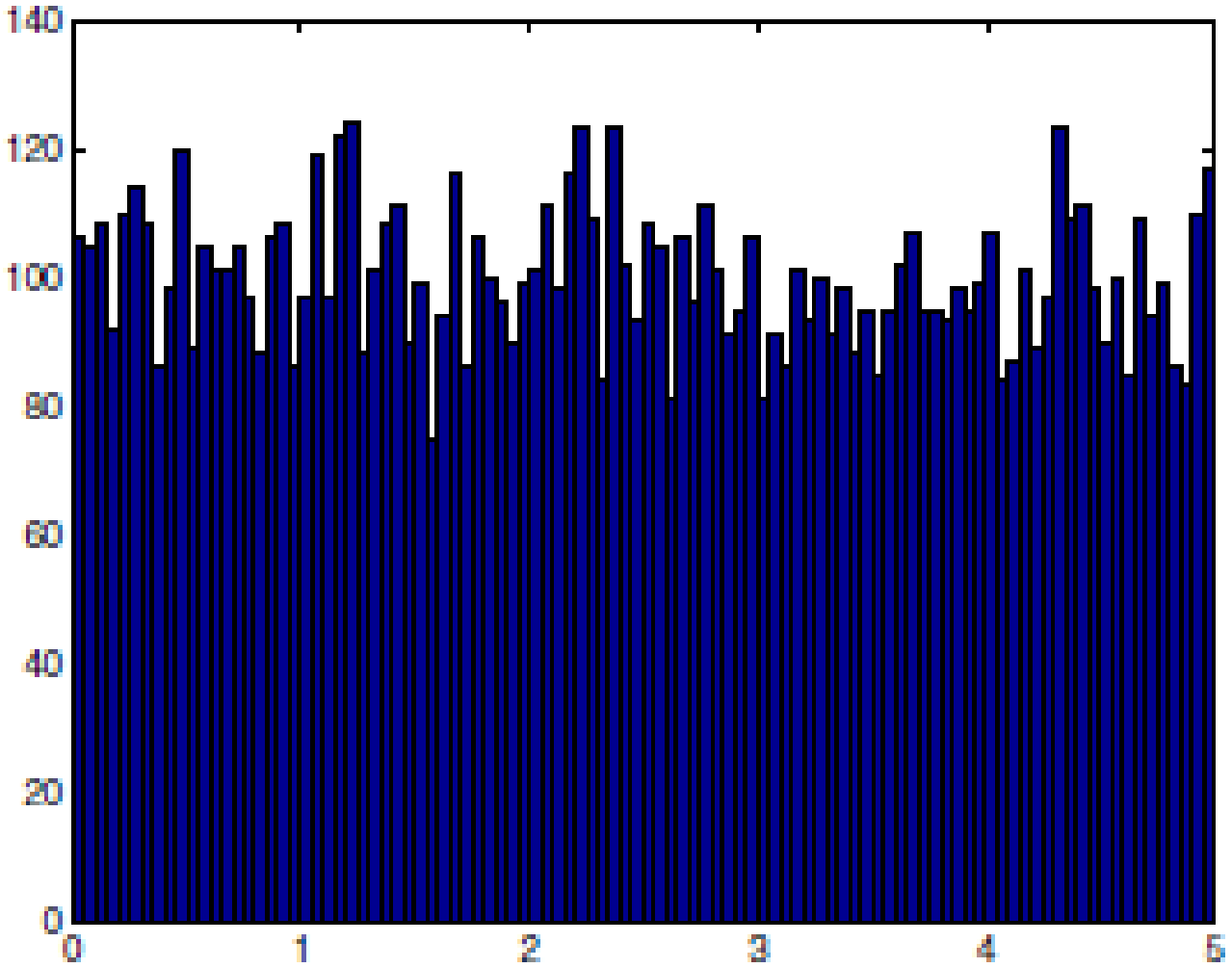
Cenários

- Avaliados:
  - Mecanismo de controle de admissão estático
  - Mecanismo de controle de admissão dinâmico

- Parâmetro $\alpha = 0,2$
- Reputação de usuário: máximo $p_{max} = 1$
- Taxa de chegada de usuários: **Poisson** com $\lambda = 10 \frac{\text{usuários}}{\text{segundo}}$
- Reputação inicial p_0: **uniforme** no intervalo $[0, 1]$
- Taxa de injeção de tráfego r_i: **aleatória** no intervalo $[100, 1000]$
- Tempo de vida de um usuário: **exponencial** com média 100 s.

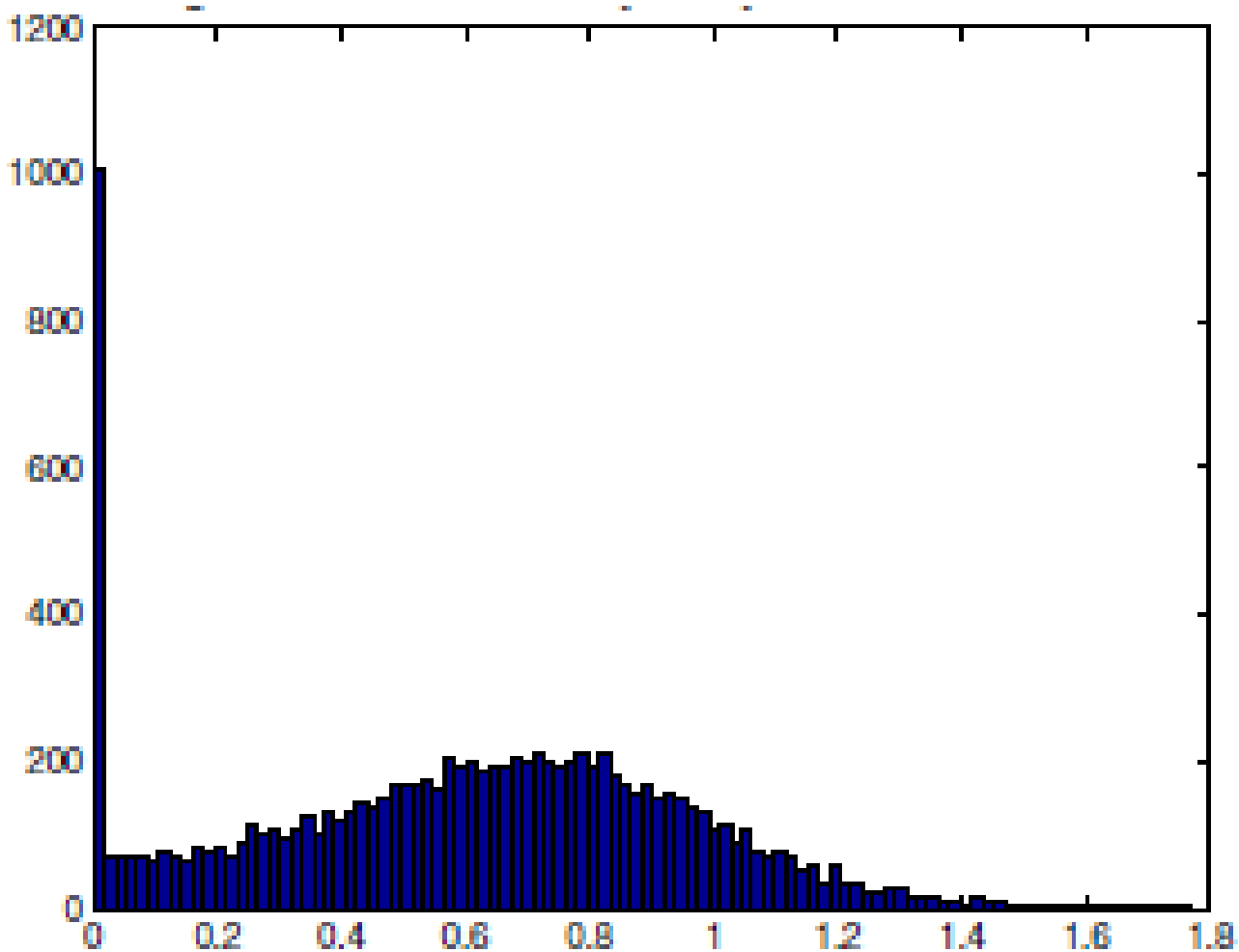
Resultados

Mecanismo de admissão estático



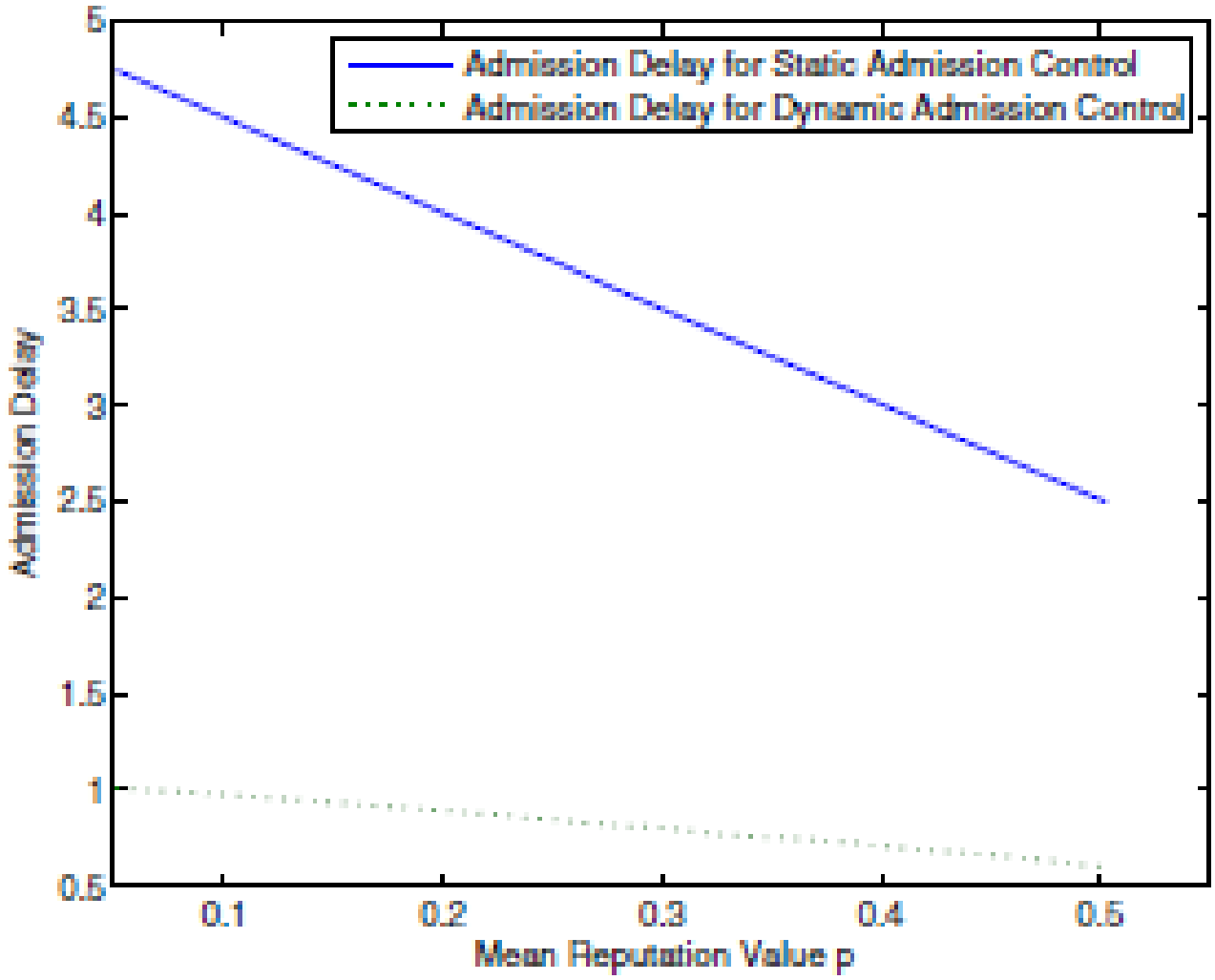
Resultados

Mecanismo de admissão dinâmico - algoritmo proposto



Resultados

Comparação: variando a distribuição de reputação inicial



s

Conclusão

- Proposta uma política para controle de admissão
  - Garantir segurança às redes de acesso público
  - Restrição: maximização da “utilidade”
  - Busca diminuir o atraso de admissão
- Solução proposta
  - Restringe os riscos de segurança impostos pelos usuários admitidos
  - Determina quando um usuário é admissível
- Resultados sugerem que a proposta melhora o atraso de admissão

Análise crítica

- A ideia de diminuir o atraso de admissão e permitir que os usuários sejam admitidos antes do término da avaliação é atrativa
- **Porém**
  - O artigo possui pontos confusos
  - Alguns parâmetros surgem sem ser explicados
  - Na avaliação, alguns parâmetros importantes não são informados ou não estão claros
  - A proposta não foi avaliada diante de ataques de DDoS
  - Nomenclatura confusa, algumas vezes
  - São apresentados poucos trabalhos relacionados
  - Poderia ter mais referências
  - Foi difícil perceber que alguns termos vinham da “teoria de economia”

OBRIGADO!