Uma Proposta Distribuída para Detecção de Intrusão, Hierárquica, Multiagente e Consciente de Situação

Ricardo Almeida[1], Roger Machado[1], Diórgenes Yuri da Rosa[2], Lucas Donato[3], Adenauer Yamin[1], Ana Pernas[1]

{rbalmeida, rdsmachado, adenauer, marilza}@inf.ufpel.edu.br

diorgenes.yuri@ufpel.edu.br

lucas.donato@myemail.dmu.ac.uk

Gramado, abril de 2015

UNIVERSIDADE FEDERAL DE PELOTAS
RS - BRASIL

PPGC
Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Pelotas

ERAD 2015
XV Escola Regional de Alto Desempenho
22 a 24 de abril de 2015
Gramado - RS

Sumário

Sumário

Introdução

- Ambientes Distribuídos:
  - Segurança da Informação:

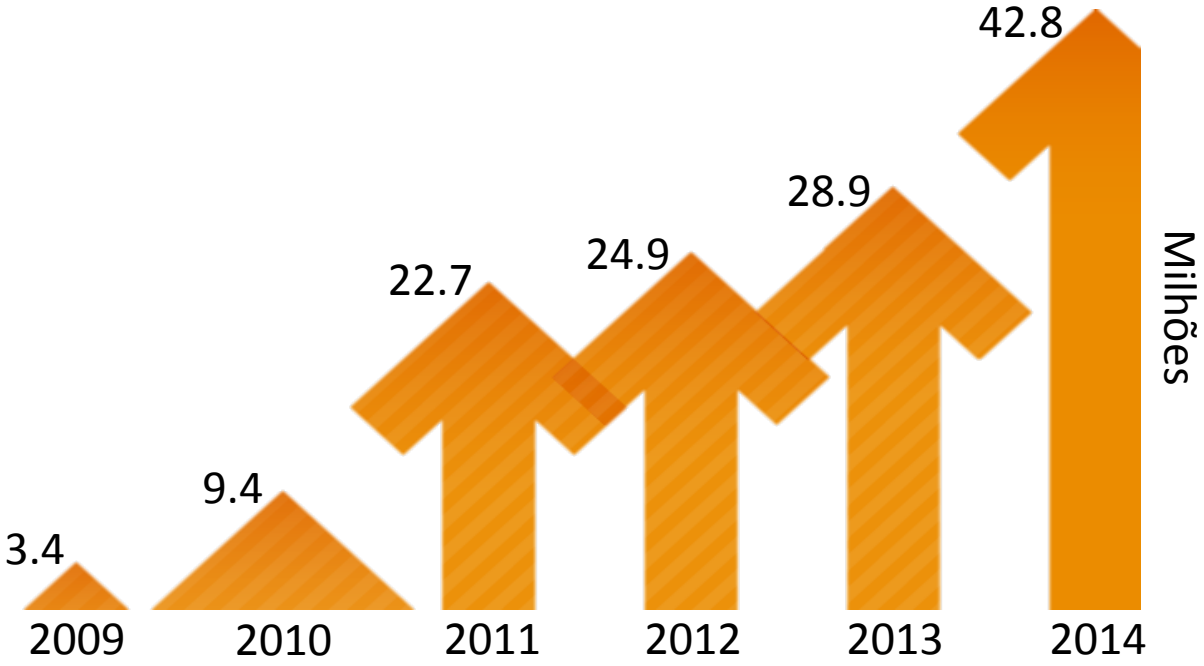

Figura 1 – Crescimento do número de incidentes [1]

Introdução

- Ambientes Distribuídos:
  - Segurança da Informação:
    - Aumento do custo do crime cibernético:
      - Federação Brasileira de Bancos: R$1,5 bilhão com fraudes eletrônicas em 2012 [2]
      - Fevereiro a Março de 2014 (ação do crime organizado - fraude nos boletos): $3,75 bilhões [3]
      - Custo anual com o crime cibernético para a economia global: $400 bilhões [4]

Motivações

- Ambientes Distribuídos e Segurança da Informação:
  - Sistemas de Detecção de Intrusão (IDS) - desafios particulares:
    - Aumento da possibilidade de acesso não autorizado
    - Uso de recursos distribuídos
    - Variedade no formato de dados
    - Velocidade em que os dados devem ser tratados
    - Grande volume de dados
    - Visibilidade

Objetivos

- Concepção de uma arquitetura de IDS que contemple os desafios dos ambientes distribuídos, sendo ela:
  - Flexível e escalável:
    - Distribuída e hierárquica
    - Processamento de eventos complexos
  - Visibilidade:
    - Consciência de Situação
  - Autonomia:
    - Sistemas multiagentes

Sumário

Base Conceitual

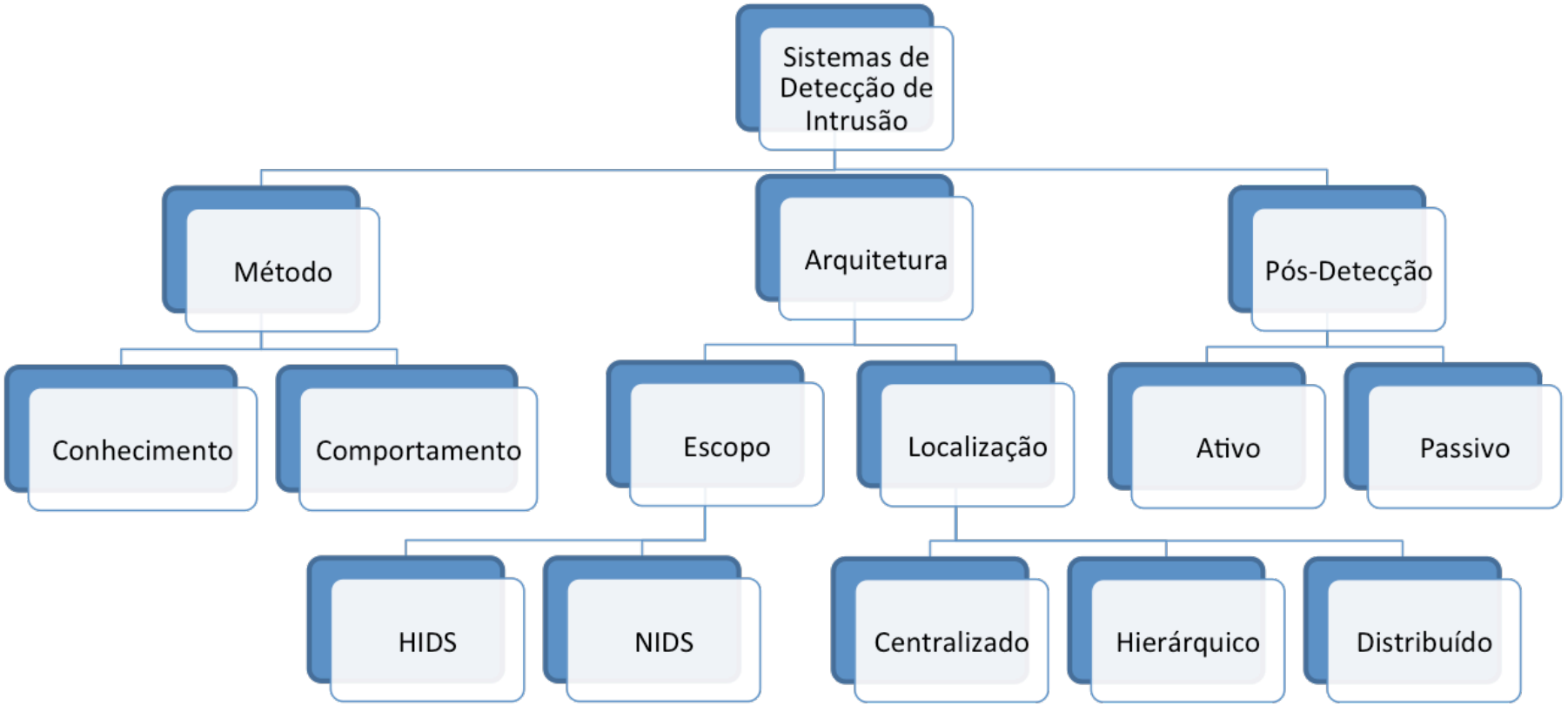

Figura 2 – Classificação dos Sistemas de Detecção de Intrusão [5]

Base Conceitual

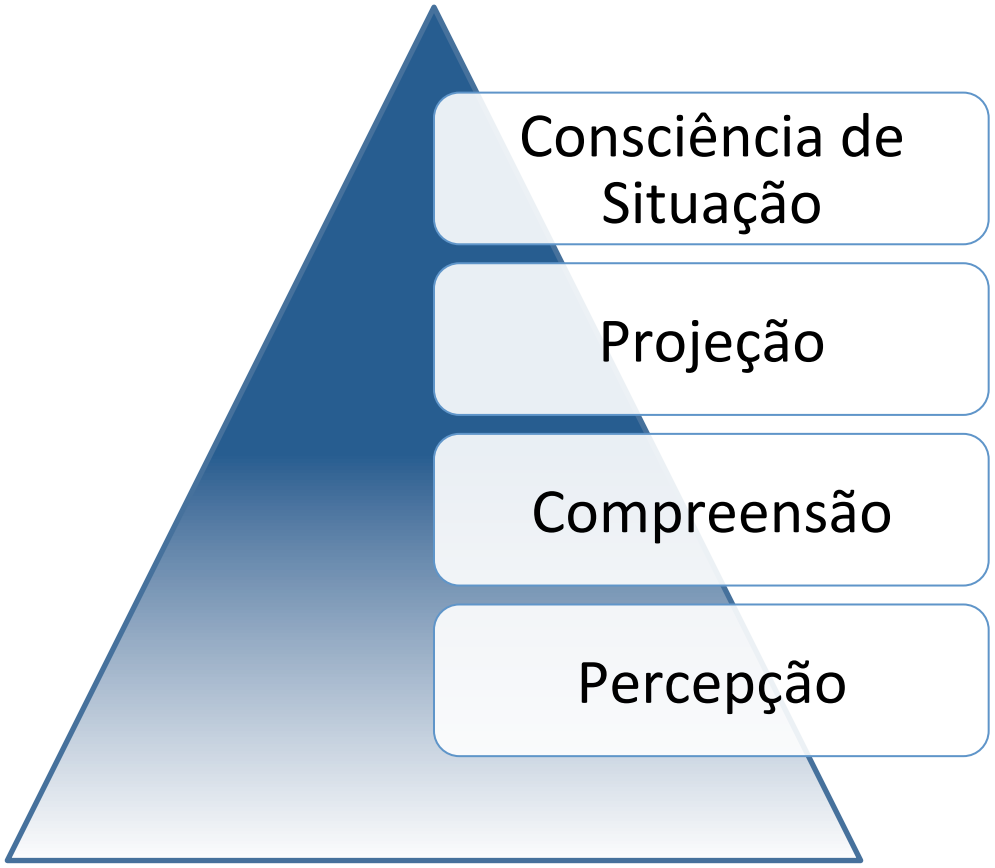

Figura 2 – Consciência de Situação

Sumário

Proposta

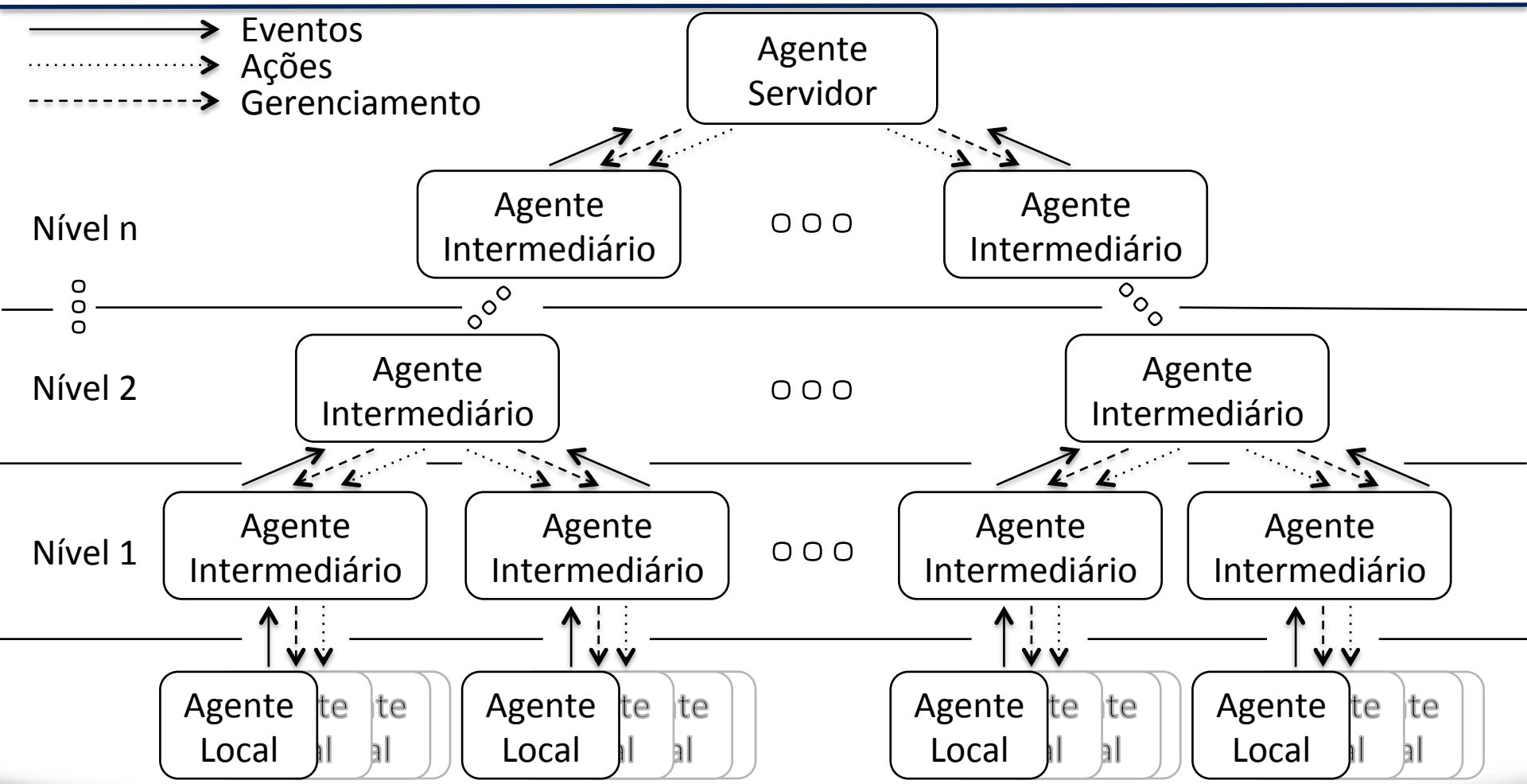

Figura 3 – Hierarquia dos componentes de software

Proposta

- Agente Local
  - Coleta de eventos
  - HIDS e NIDS
  - Conhecimento e Comportamento
  - Ações ativas e passivas
- Agente Intermediário
  - Recebimento de eventos e situações
  - Repasse dos eventos e situações
  - Filtragem e correlação

Proposta

- Agente Servidor
  - Recebimento dos eventos e situacões
  - Correlação
  - Armazenamento
  - Interface com o usuário
  - Visão aprimorada do ambiente

Sumário

Trabalhos Relacionados

- WU et al., 2006 - **Dynamic Hierarchical Distributed Intrusion Detection System Based on Multi-Agent System** [6]
  - Multiagentes
  - Arquitetura hierárquica dinâmica
  - Baseado em conhecimento
  - Abordagem teórica

Trabalhos Relacionados

- ZHAI; HU; WEIMING, 2014 - **Multi-Agent Distributed Intrusion Detection System Mo- del Based on BP Neural Network** [7]
  - Detecção e resposta distribuída
  - Multiagentes
  - Rede neural artificial com o algoritmo *backpropagation*
  - Testes do algoritmo – melhoria da precisão e redução da carga do nodo central
  - Não são realizados testes em ambiente de produção

Trabalhos Relacionados

- JUN and CHI, 2014 - **Design of Complex Event-Processing IDS in Internet of Things** [8]
  - Processamento de Eventos Complexos (CEP) – baseado em conhecimento
  - Comparação entre CEP e abordagem tradicional
  - Distribuição do CEP

Sumário

Considerações Finais

- Nova abordagem:
  - Multiagentes
  - Processamento de Eventos Complexos
  - Consciência de Situação
  - Arquitetura hierárquica multinível

Considerações Finais

- Próximos passos:
  - Concluir a concepção da arquitetura:
    - Definir armazenamento de dados (distribuição, abordagem híbrida)
    - Protocolos para troca de dados entre os componentes da arquietura
  - Modelagem
  - Prototipação
  - Casos de uso
  - Avaliação e testes

Referências

[1] PricewaterhouseCoopers. The Global State of Information Security Survey 2015.

[2] GOMES, H. Folha de São Paulo - Bancos perdem R$1,5 bilhão com fraudes. Acesso em 20 abr 2015. Disponível em: http://www1.folha.uol.com.br/mercado/1161832-bancos-perdem-r-15-bilhao-com-fraudes.shtml.

[3] Cybercrime Scheme Uncovered in Brazil. Acesso em 20 abr 2015. Disponível em: http://www.nytimes.com/2014/07/03/technology/cybercrime-scheme-aims-at-payments-in-brazil.html.

[4] McAfee. Center for Srtategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime - Economic Impact of cybercrime II. 2014.

[5] STÊNICO, J. W.; Lee, L. L. The State of the Art in Intrusion Prevention and Detection. Capítulo 2. 2014.

[6] WU, J.; WANG, C.-J.; WANG, J.; CHEN, S.-F. Dynamic Hierarchical Distributed Intrusion Detection System Based on Multi-Agent System. In: WEB INTELLIGENCE AND INTELLIGENT AGENT TECHNOLOGY WORKSHOPS, 2006. WI-IAT 2006 WORKSHOPS. 2006 IEEE/WIC/ACM INTERNATIONAL CONFERENCE ON, 2006. **Anais. . .** [S.l.: s.n.], 2006. p.89–93.

Referências

[7] ZHAI, S.; HU, C.; WEIMING, Z. Multi-Agent Distributed Intrusion Detection System Mo- del Based on BP Neural Network. **Institute of Advanced Engineering and Science**, [S.l.], v.Vol 3, No 3 (2014), 2014.

[8] JUN, C.; CHI, C. Design of Complex Event-Processing IDS in Internet of Things. In: MEASURING TECHNOLOGY AND MECHATRONICS AUTOMATION (ICMTMA), 2014 SIXTH INTERNATIONAL CONFERENCE ON, 2014. **Anais. . .** [S.l.: s.n.], 2014. p.226–229.

Uma Proposta Distribuída para Detecção de Intrusão, Hierárquica, Multiagente e Consciente de Situação

Ricardo Almeida[1], Roger Machado[1], Diórgenes Yuri da Rosa[2], Lucas Donato[3], Adenauer Yamin[1], Ana Pernas[1]

{rbalmeida, rdsmachado, adenauer, marilza}@inf.ufpel.edu.br

diorgenes.yuri@ufpel.edu.br

lucas.donato@myemail.dmu.ac.uk

Gramado, abril de 2015

UNIVERSIDADE FEDERAL DE PELOTAS
RS - BRASIL

PPGC
Programa de Pós-Graduação em Ciência da Computação
Universidade Federal de Pelotas

ERAD 2015
XV Escola Regional de Alto Desempenho
22 a 24 de abril de 2015
Gramado - RS