Aprendizado de Máquina em Sistemas de Detecção de Intrusão em Rede baseados em Anomalia

Thiago R. C. De Lima

30 de Junho de 2015

Universidade Federal do Paraná

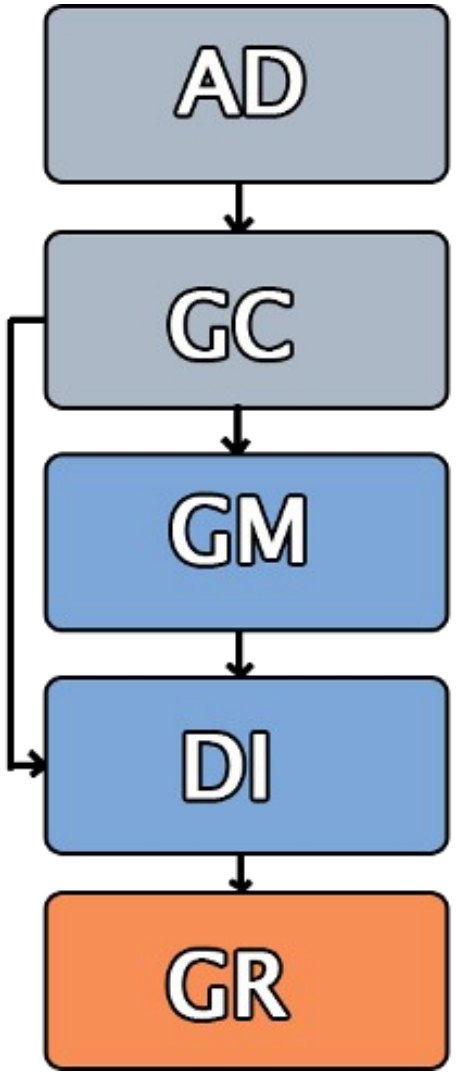
Sumário

- Sistemas de Detecção de Intrusão
- Aprendizado de Máquina
- Dados
- Algoritmos
- Testes
- Conclusão

Introdução


/cgi-bin/login" METHOD
PE=TEXT NAME=USER
ASSWORD=
VALUE="su
//XHTML 1.0 Tra
xml:lang="da"

Arquitetura



Aquirir Dados

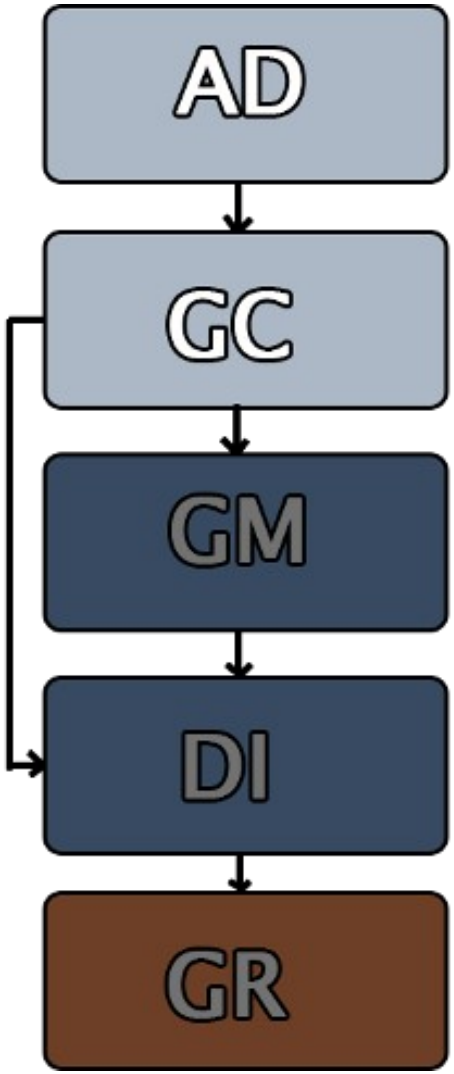
Gerar Características

Gerar Modelo (Treinar)

Detectar Intrusão (Classificar)

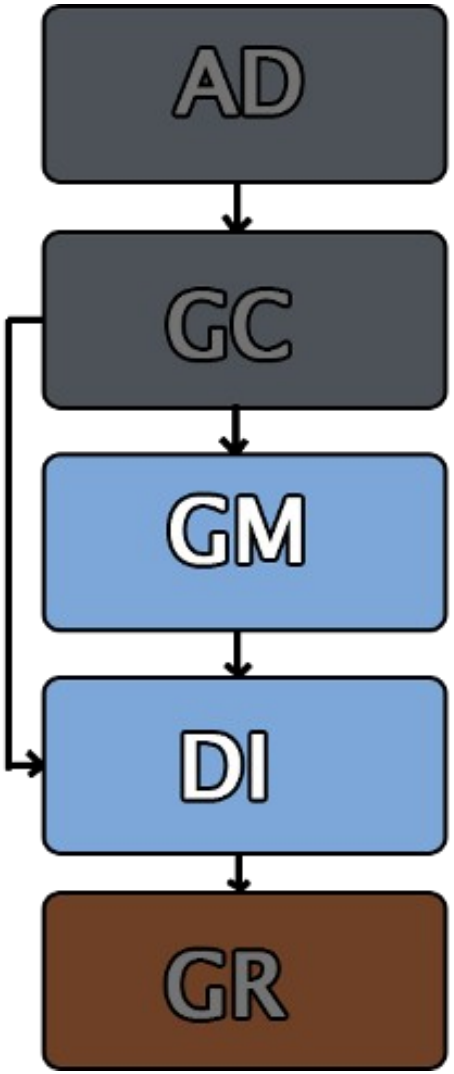
Gerar Resposta

Dados



- Cabeçalho
- Corpo
- Conexão Única (SCD)
- Conexões Múltiplas (MCD)
- Redução

Algoritmos



- Rede de Bayes
- Cadeia de Markov
- Redes Neurais
- SVM
- Árvore de Decisão

Representabilidade

	Tamanho Treino	Tamanho Teste	Tempo	Precisão
1	10%	90%	16h13m	92.22%
2	20%	80%	24h02m	94.54%
3	30%	70%	27h32m	95.65%
4	40%	60%	32h11m	98.62%
5	50%	50%	38h45m	99.64%

Imprevisibilidade

- Inicial:
  - Treino – 258880
  - Teste – 275204
- Análogo:
  - 148343
- Desconhecido:
  - 276548

Imprevisibilidade

	DT				
	TP_{rate}	FP_{rate}	Tempo	Acertos	Precisão
Inicial	0.982	0.018	6.92s	98.18%	0.982
Análogo	0.912	0.856	3.73s	91.23%	0.885
Desconhecido	0.503	0.497	6.95s	50.29%	0.751

	SVM				
	TP_{rate}	FP_{rate}	Tempo	Acertos	Precisão
Inicial	0.971	0.029	15h13min	98.43%	0.984
Análogo	0.902	0.845	8h12min	90.27%	0.891
Desconhecido	0.52	0.484	15h29min	50.78%	0.753

Seleção de Atributos

	DT				
	TP_{rate}	FP_{rate}	Tempo	Acertos	Precisão
Inicial	1.0	0.0	5.75s	99.98%	1.0
Análogo	0.848	0.429	3.1s	84.82%	0.914
Desconhecido	0.499	0.501	5.78s	49.86%	0.414

	SVM				
	TP_{rate}	FP_{rate}	Tempo	Acertos	Precisão
Inicial	0.503	0.502	14h45min	50.3%	0.75
Análogo	0.068	0.068	7h56min	6.78%	0.937
Desconhecido	0.5	0.5	14h51min	50.0%	0.75

Conclusão

- Resultados
- Open Issues
- Dúvidas

Referências

[1] R. Sommer e V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. *Security and Privacy (SP), 2010 IEEE Symposium on*, páginas 305–316, May de 2010.

[2] Remco R. Bouckaert, Eibe Frank, Mark A. Hall, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, e Ian H. Witten. Weka—experiences with a java open-source project. *J. Mach. Learn. Res.*, 11:2533–2541, dezembro de 2010.

[3] Carlos A. Catania e Carlos García Garino. Automatic network intrusion detection: Current techniques and open issues. *Comput. Electr. Eng.*, 38(5):1062–1072, setembro de 2012.

[4] Jonathan J. Davis e Andrew J. Clark. Data preprocessing for anomaly based network intrusion detection: A review. volume 30, páginas 353–375, Oxford, UK, UK, setembro de 2011. Elsevier Advanced Technology Publications.