Avaliação do Classificador ARTMAP Fuzzy em redes 802.11 com Criptografia Pré-*Robust Security Network* (WEP e WPA)

Nelcileno Araújo[1], Ruy de Oliveira[2], Ailton Akira Shinoda[3], Ed'Wilson Tavares Ferreira[2], Valtemir Emerêncio do Nascimento[2]

[1]Instituto de Computação - Universidade Federal de Mato Grosso (UFMT) – Cuiabá, MT – Brasil

[2]Departamento de Informática - Instituto Federal de Educação. Ciência e Tecnologia de Mato Grosso (IFMT) – Cuiabá, MT – Brasil

[3]Departamento de Engenharia Elétrica - Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP) - Ilha Solteira, SP – Brasil

nelcileno@ic.ufmt.br,{ruy,ed,valtemir}@cba.ifmt.edu.br, shinoda@dee.feis.unesp.br

Abstract. *Recent years have seen strong growth in the use of 802.11 wireless technology (Wireless LAN) and the security mechanisms implemented by IEEE 802.11i e IEEE 802.11w amendments have been shown to be ineffective in combating attacks against the availability of WLAN services. This paper evaluates the performance of Fuzzy ARTMAP classifier in the detection of a group of denial of service (DoS) attacks in a real WLAN supporting WEP and WPA encryption. Fuzzy ARTMAP neural network was selected because it is able to retain previously acquired knowledge and adapt to new classification patterns. The results obtained in terms of detection rate and false alarms rate suggest that there is a need for a metaheuristic to provide more reliable parameters for the performance of the classifier and the selection of most representative features about intrusive behavior exists in DoS attacks.*

Resumo. *Nos últimos anos têm-se percebido um forte crescimento no uso da tecnologia sem fio 802.11 (Wireless LAN) e os mecanismos de segurança implementados pelas emendas IEEE 802.11i e IEEE 802.11w têm se mostrado pouco eficazes no combate a ataques contra a disponibilidade dos serviços da WLAN. Neste artigo avalia-se o desempenho do classificador ARTMAP Fuzzy na detecção de um grupo de ataques de negação de serviço (DoS) numa rede WLAN real com suporte a criptografia WEP e WPA. A rede neural ARTMAP Fuzzy foi escolhida pela sua capacidade de preservar o conhecimento anteriormente adquirido e adaptar-se a novos padrões de classificação. Os resultados obtidos demonstram que há a necessidade de uma metaheurística para fornecer parâmetros mais confiáveis para a execução do classificador e a seleção de atributos mais representativos do comportamento intrusivo existente nos ataques de DoS.*

1. Introdução

Os números apresentados pela IDC Brasil, onde 55% dos computadores vendidos em 2011 foram *notebooks*/*netbooks* e as vendas de *smartphones* em 2011 cresceram 84%

 ©2012 SBC — Soc. Bras. de Computação

com relação ao ano anterior [IDC - Brasil, 2012a][IDC - Brasil, 2012b] demonstram uma popularização de dispositivos com interface de comunicação sem fio 802.11, propiciando uma disseminação do uso de redes locais sem fio (WLAN) em ambientes que fornecem acesso à Internet para seus clientes, tais como: shopping centers, universidades, aeroportos, dentre outros.

No entanto, é bem conhecido que devido à natureza aberta do acesso sem fio, a segurança de uma WLAN levanta muitas considerações e um conjunto de extensões de segurança ao padrão IEEE 802.11 já foram propostas [IEEE 802.11, 1999], [IEEE 802.11i, 2004] e [IEEE 802.11w, 2009]. Contudo, estas extensões combatem com sucesso as vulnerabilidades relacionadas ao acesso não autorizado, integridade e a confidencialidade, mas deixam a desejar na proteção da disponibilidade dos serviços de redes numa WLAN [Ahmad e Tadakamadla, 2011].

Os ataques contra a disponibilidade dos recursos da rede são popularmente conhecidos como negação de serviço (DoS – *Denial of Service*). Uma das principais fontes para ataques de DoS numa WLAN são os quadros de gerenciamento e controle pois são responsáveis pela associação e controle de acesso ao meio sem fio entre os clientes da rede e o ponto de acesso [Bicakci e Tavli, 2009].

Uma contramedida para evitar os problemas de indisponibilidade na WLAN é a utilização de sistemas detectores de intrusão (IDS) como uma segunda camada de defesa que monitore constantemente as ondas de rádio, de forma a detectar possíveis explorações destas vulnerabilidades. O IDS pode analisar o tráfego monitorado a partir de um conjunto de assinaturas de ataques (detecção baseada em assinaturas) ou pela definição de um perfil esperado para um dispositivo pertencente à rede (detecção baseada em anomalia).

Este artigo apresenta uma avaliação do classificador ARTMAP *Fuzzy* [Carpenter, G. *et al*., 1992] na tarefa de identificação de um grupo de ataques DoS por meio dos quadros de gerenciamento de uma rede WLAN real com criptografia Pré-RSN (*Robust Security Network*), ou seja empregam apenas os protocolos criptográficos WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*).

2. Trabalhos Relacionados

A proposta apresentada por [Ahmad, Abdullah e Alghamdi, 2010] mostra que o classificador ARTMAP Fuzzy na tarefa de detecção de intrusão possui um baixo desempenho nas avaliações realizadas, mas a base de dados utilizada nos experimentos é originada de uma rede cabeada e não utilizam nenhum mecanismo de otimização computacional para maximizar a classificação correta.

Já a proposta relatada por [Vilakazi e Marwala, 2007] emprega a técnica de algoritmos genéticos, como mecanismo de otimização computacional, para obter parâmetros de configuração que proporciona ao classificador ARTMAP Fuzzy alcançar um ótimo desempenho de 100% na fase de detecção. No entanto, a base de dados avaliada não representa uma rede local sem fio.

A abordagem relatada por [Santra, Nagaranjan e Jinesh, 2012] utiliza a rede neural ARTMAP Fuzzy na detecção de intrusão em redes heterogêneas sem fio e aplica a metaheurística otimização por enxame de partículas (PSO) para minimizar os erros da classificação. Apesar disso, o mecanismo proposto não se enquadra na identificação de ataques DoS em quadros de gerenciamento pois os autores utilizam sua proposta para fornecer um modelo de controle de acesso.

 ©2012 SBC — Soc. Bras. de Computação

3. Abordagem proposta para avaliação do classificador ARTMAP Fuzzy

Para avaliar o classificador ARTMAP Fuzzy, foram realizados experimentos num cenário controlado, cuja topologia é representada na Figura 1, para gerar a base de dados a ser empregada como base de conhecimento.

A rede analisada tinha a seguinte composição: três estações sem fio e um ponto de acesso (AP). A estação 1 injetava tráfego normal na rede (HTTP, FTP). A estação 2 utilizou a ferramenta *Aireplay* [Aireplay, 2011] para realizar, simultaneamente, os quatro ataques (*chopchop*, duração, deautenticação e fragmentação) pré-definidos. A estação 3 usou a ferramenta *Wireshark* [Wireshark, 2011] para realizar a captura do tráfego transeunte (normal e intruso) na rede.

A seguir, foi realizado um pré-processamento nos dados capturados para se extrair os seguintes campos do cabeçalho MAC (*Media Access Control*) dos quadros de gerenciamento: *protocol version*, *type*, *subtype*, *to DS*, *from DS*, *more fragment*, *retry*, *power managment*, *more data*, WEP, *order*, *duration*, *address1*, *address2*, *address3* e *sequence control*, , pois também faz parte da pesquisa ver o impacto destas informações na especificação de assinaturas para os ataques de DoS. Por último, inseriu-se em cada amostra sua respectiva categoria de reconhecimento.

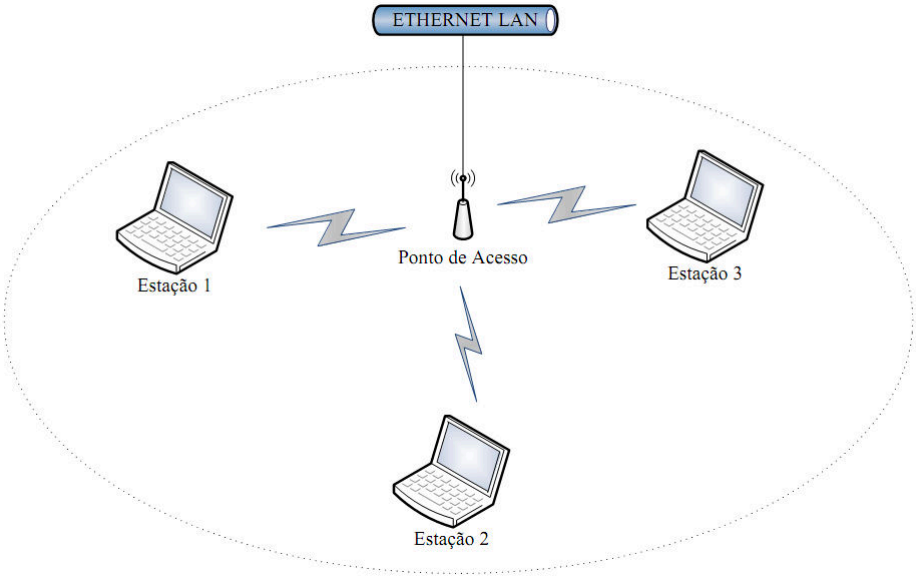


Figura 1. Topologia da rede WLAN aplicada na geração da base de dados

A base de dados empregada na avaliação do classificador é criada pela captura de quadros de gerenciamento da rede WLAN utilizada nos experimentos, em que a rede esteve sob condição "normal", sem ataques, e sob os ataques *Chopchop* [Bittau, Rendley e Lackey, 2006], deautenticação [Bellardo e Savage, 2003], duração [Bellardo e Savage, 2003] e fragmentação [Bittau, Rendley e Lackey, 2006].

Essas quatro categorias usadas na geração dos ataques foram escolhidas porque elas exploram de forma efetiva as vulnerabilidades de disponibilidade nas redes 802.11 com criptografia Pré-RSN. Os ataques de duração e deautenticação afetam a capacidade da estação base de gerenciar o acesso à infraestrutura da rede [Berlado e Savage, 2003]. Os ataques de *chopchop* e fragmentação exploram as vulnerabilidades dos mecanismos

 ©2012 SBC — Soc. Bras. de Computação

criptográficos (WEP e WPA) para indisponibilizar os serviços da rede [Bittau, Rendley e Lackey, 2006].

A base de dados gerada pelos dados coletados nos experimentos foi dividida em três conjuntos: treinamento, validação e teste.

O conjunto de treinamento é formado por 9600 amostras com a seguinte constituição: 6000 amostras de tráfego normal e 3600 amostras de tráfego intruso. A validação da rede neural ARTMAP Fuzzy ocorre pela aplicação de um conjunto de validação formado por novas 6400 amostras, constituída de 4000 amostras de tráfego normal e 2400 amostras de tráfego intruso. Após a rede treinada e validada obtêm-se os parâmetros da rede neural ARTMAP Fuzzy, os quais são: parâmetro de escolha (α) = 0.01, parâmetro de vigilância da rede ART_a (ρ_a) = 0.7, parâmetro de vigilância da rede ART_b (ρ_b) = 1, parâmetro de vigilância do mapa associativo (ρ_{ab}) = 0.99 e taxa de treinamento (β) = 1. A partir disso, pode-se entrar com o conjunto de teste para que o classificador diagnostique suas saídas. O conjunto de teste possui novas 8200 amostras divididas em 5000 amostras de tráfego normal e 3200 amostras de tráfego intruso.

Para avaliar o desempenho do classificador ARTMAP Fuzzy, os seus resultados foram comparados com outros três classificadores: *Suport Vector Machine* (SVM), Rede Neural *Multilayer Perceptron* com treinamento *Backpropagation* (MPBP) e Rede Neural *Radial Basis Function* (RBF).

A ferramenta WEKA [WEKA, 2011] é a solução computacional utilizada para implementar a avaliação do classificador ARTMAP Fuzzy com os outros classificadores devido ao fácil manuseio e uma biblioteca rica de técnicas de classificação de padrões.

Os critérios de avaliação de um classificador de padrões na detecção de intrusão podem ser realizados pelo cálculo das seguintes métricas: Verdadeiros Positivos (TP) - identifica uma atividade intrusiva corretamente; Verdadeiro Negativo (TN) - identifica uma atividade não-intrusiva corretamente; Falso Positivo (FP): identifica uma ação não-intrusiva como sendo intrusiva; Falso Negativo (FN): identifica uma atividade intrusiva como sendo não-intrusiva.

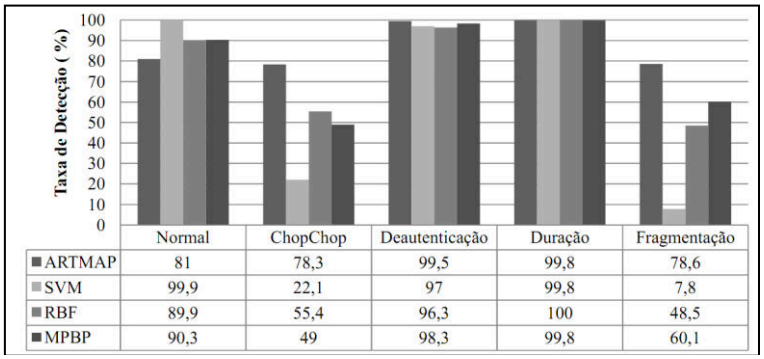
As métricas mais populares na avaliação de desempenho de um IDS são taxa de detecção e taxa de falsos alarmes [Wu e Banzhaf, 2010]. A taxa de detecção é definida como TP/(TP+FN) e por fim, a taxa de falsos alarmes é definida como FP/(TN+FP).Um classificador de padrões obtém um bom desempenho na detecção de intrusão quando atinge uma alta taxa de detecção e uma baixa taxa de falsos alarmes [Wu e Banzhaf, 2010]. A seguir, apresentam-se os resultados obtidos nesta avaliação de desempenho.

4. Resultados Obtidos

Para verificar o desempenho do classificador de padrões foram aplicadas 8200 amostras do conjunto de teste nos dois cenários de comparação apresentados neste artigo.

A Figura 2 apresenta o primeiro cenário, usado na avaliação da taxa de detecção dos classificadores, segundo as categorias relatadas na base de dados para reconhecimento. Observa-se que o classificador ARTMAP Fuzzy possui um baixo desempenho na identificação de tráfego normal, enquanto no reconhecimento dos ataques de DoS apresentados na base de conhecimento atingiu desempenho igual ou superior aos classificadores avaliados.

 ©2012 SBC — Soc. Bras. de Computação

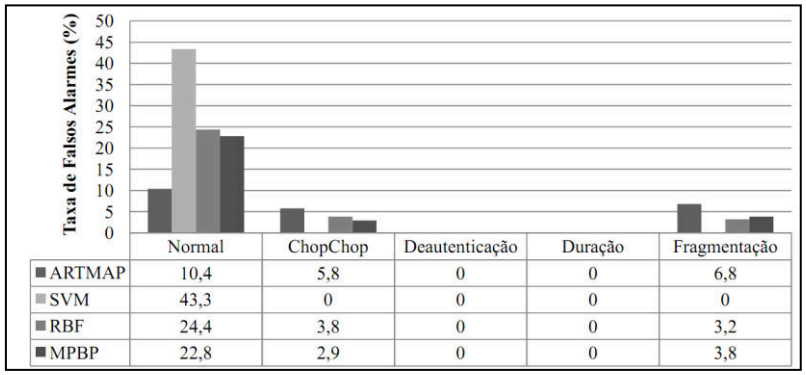


	Normal	ChopChop	Deautenticação	Duração	Fragmentação
ARTMAP	81	78,3	99,5	99,8	78,6
SVM	99,9	22,1	97	99,8	7,8
RBF	89,9	55,4	96,3	100	48,5
MPBP	90,3	49	98,3	99,8	60,1

Figura 2. Taxa de detecção dos classificadores

A baixa eficiência na detecção de atividade normal pode ser ocasionada por não ocorrer uma seleção de atributos mais representativos nas instâncias pertence aos registros auditados ou por não implementar um mecanismo de otimização que ofereça melhores valores para os parâmetros de configuração da rede ARTMAP Fuzzy.

A avaliação da taxa de falsos alarmes apresentada pelos classificadores, ilustrado na Figura 3, demonstra que o classificador ARTMAP Fuzzy apresenta a maior taxa de falsos alarmes entre os classificadores avaliados no reconhecimento dos quatro ataques de DoS executados no cenário. Uma possível razão para este baixo desempenho do classificador ARTMAP Fuzzy é os campos do quadro MAC serem insuficientes para especificar assinaturas bem definida das categorias de ataques representadas nos experimentos.



	Normal	ChopChop	Deautenticação	Duração	Fragmentação
ARTMAP	10,4	5,8	0	0	6,8
SVM	43,3	0	0	0	0
RBF	24,4	3,8	0	0	3,2
MPBP	22,8	2,9	0	0	3,8

Figura 3. Taxa de falsos alarmes dos classificadores

Um dos maiores entraves no aumento da classificação correta da rede neural ARTMAP Fuzzy refere-se à sua sensibilidade à sobreposição estatística entre as classes. A sensibilidade pode ocasionar crescimento descontrolado da quantidade de categorias de reconhecimento, causando aumento na complexidade de memória e computacional. Como também, possível degradação na classificação correta [Lerner e Guterman, 2008].

6. Conclusões

Neste artigo é relatada uma avaliação do classificador ARTMAP Fuzzy na detecção de um grupo de ataques DoS (*chopchop*, deautenticação, duração e fragmentação) numa rede WLAN real com suporte a criptografia WEP e WPA. Esta avaliação ocorre por meio de uma comparação do classificador estudado com um grupo de classificadores comumente empregados na literatura para detecção de intrusos.

 ©2012 SBC — Soc. Bras. de Computação

A rede neural ARTMAP Fuzzy apresenta um baixo desempenho no reconhecimento de atividade normal e uma alta de taxa de falsos alarmes na identificação do grupo de ataques DoS analisados. Isto demonstra que os campos do quadro MAC utilizados são insuficientes para gerar assinaturas confiáveis para a identificação dos ataques, necessitando um processo de seleção de atributos que possa escolher características mais representativas do comportamento intrusivo existente nos ataques DoS estudados. Além disso, a ausência de uma técnica de otimização computacional para a geração dos parâmetros de configuração do classificador pode ter contribuído para o baixo desempenho dele, visto que em trabalhos, tais como [Vilakazi e Marwala, 2007] e [Santra, Nagaranjan e Jinesh, 2012], o uso de uma metaheurística auxilia na definição dos parâmetros da rede neural ARTMAP Fuzzy.

Na fase atual da pesquisa pretende-se tratar o problema da sensibilidade da rede neural ARTMAP Fuzzy implementando a técnica de metaheurística baseada em inteligência de enxame para obter melhores parâmetros de configuração para o classificador. Como também implementar as emendas de segurança IEEE 802.11i e IEEE 802.11w na WLAN para ver o desempenho do classificador no reconhecimentos de ataques de DoS referente a este tipo de emendas.

Referências

Ahmad, I., Abdullah, A. e Alghamdi, A. (2010) “Towards the selection of best neural network system for intrusion detection”, International Journal of the Physical Sciences, vol. 5, n. 12, p. 1830-1839.

Ahmad, M. S., Tadakamadla, S. (2011) “Short paper: security evaluation of IEEE 802.11w specification”, Proceedings of the fourth ACM conference on Wireless network security, p. 53 - 58.

Aircrack (2011), http://www.aircrack-ng.org/.

Bellardo, J. e Savage, S. (2003) “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions”, Proceedings of the 12th Conference on USENIX Security Symposium, vol. 12, p. 15-28.

Bicakci, K. e Tavli, B. (2009) “Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks”, Computer Standards & Interfaces, v. 31, n. 5, p. 931-941.

Bittau, A., Handley, M. e Lackey, J. (2006) “The Final Nail in WEP's Coffin”, Proceedings of the 2006 IEEE Symposium on Security and Privacy, p. 386-400.

Carpenter, G., Grossberg, S., Markuzon, N., Reynold, J. e Rosen, D. (1992) “Fuzzy ARTMAP: A neural network for incremental supervised learning of analog multidimensional maps”, IEEE Transactions on Neural Network, vol. 3, n. 5, p. 689-713.

IDC – BRASIL (2012) “Estudo da IDC revela que foram vendidos aproximadamente 9 milhões de smartphones no Brasil em 2011”, http://www.idclatin.com/news.asp?ctr=bra&year=2012&id_release=2213, Abril.

IDC – BRASIL (2012) “Brasil comercializa 15,4 milhões de computadores em 2011 e se consolida na terceira posição do mercado mundial, segundo pesquisa da IDC”, http://www.idclatin.com/news.asp?ctr=bra&year=2012&id_release=2200, Abril.

 ©2012 SBC — Soc. Bras. de Computação

IEEE Std. 802.11 (1999) “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, p. 1-512.

IEEE Std. 802.11 (2004) “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements ”, p. 1-175.

IEEE Std. 802.11w (2009) “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Protected Management Frames”, p. 1-92.

Lerner, B. e Guterman, H. (2008) “Advanced Developments and Applications of the Fuzzy ARTMAP Neural Network in Pattern Classification”, In *Studies in Computational Intelligence*, vol. 137, p. 77-107, Spring-Verlag.

Santra, A. K., Nagarajan, S. e Jinesh, V. N. (2012) “ Intrusion Detection in Wireless Networks using FUZZY Neural Networks and Dynamic Context-Aware Role based Access Control Security (DCARBAC)”, International Journal of Computer Applications, vol. 39, n. 4, p. 23-31.

Vilakazi, C. e Marwala, T. (2007) “Application of Feature Selection and Fuzzy ARTMAP to Intrusion Detection”, Proceedings of the Conference International on Systems, Man and Cybernetics, p. 4880-4885.

Weka (2011), http://www.cs.waikato.ac.nz/ml/weka/.

Wireshark (2011), http://www.wireshark.org/.

Wu, S. e Banzhaf, W. (2010) “The Use of Computational Intelligence in Intrusion Detection Systems: A Review”, In *Applied Soft Computing*, vol.10, p. 1-35.

 ©2012 SBC — Soc. Bras. de Computação