Construção de Bases de Dados para Auxiliar a Avaliação de Sistemas de Detecção de Intrusos em uma Rede IEEE 802.11 com Criptografia WEP, WPA e WPA2 Habilitada

Douglas Willer Ferrari Luz Vilela[1], Ailton Akira Shinoda[2], Ed'Wilson Tavares Ferreira[3], Ruy de Oliveira[3], Valtemir Emerêncio do Nascimento[3], Nelcileno Araújo[4]

[1]Coordenação de Tecnologia da Informação- Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso (IFMT) – Cuiabá - MT – Brazil

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

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

[4]Instituto de Computação- Universidade Federal de Mato Grosso (UFMT) – Cuiabá - MT – Brazil

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

Abstract*. The growth in the use of wireless technology IEEE 802.11 has been taking large proportions over recent years and the security mechanisms implemented in the same have proved to be ineffective in protection against denial of service attacks. Thus, the use of IDS as helping to secure networks, has increased. However, in order for the training algorithm intrusion detection to be effective it is necessary to use a database representative of traffic in the wireless environment. Though, one of major challenges in intrusion detection systems in wireless networks is limited number of methodologies for building database. This paper details the construction of databases, in which the first database is represented from a similar scenario of a typical for domestic use using WEP and / or WPA enabled. The second uses a similar scenario to that of a corporative environment with WPA2 encryption enabled.*

Resumo. *O crescimento da utilização da tecnologia sem fio IEEE 802.11 tem tomado grandes proporções nos últimos anos e os mecanismos de segurança implantado na mesma têm se mostrado pouco eficazes no combate a ataques de negação de serviço. Sendo assim, a utilização de IDS, como auxílio à proteção de redes, tem aumentado. Entretanto, para que o treinamento do algoritmo de detecção de intrusos seja eficaz é necessária à* utilização *de uma base de dados representativa do tráfego no ambiente sem fio. No entanto, um dos grandes desafios em sistemas detectores de intrusão em redes sem fio é número reduzido de metodologias para construção de base de dados. Esse trabalho detalha a construção de bases de dados, nas quais a primeira base de dados é representada a partir da implementação de um cenário semelhante à de um ambiente de uso doméstico utilizando criptografia WEP e/ou WPA habilitadas. A segunda utiliza um cenário semelhante ao de um ambiente coorporativo com criptografia WPA2 habilitada.*

Introdução

Nos últimos anos houve um forte crescimento na utilização de redes móveis. O padrão IEEE 802.11 vem se destacando, como uma das tecnologias sem fio mais utilizadas na atualidade. Com o avanço na utilização das redes WLANs (*Wireless Local Área Networks*) começaram a surgir questionamentos sobre a eficácia dos mecanismos de segurança empregados nas mesmas. O primeiro protocolo de segurança lançado pela IEEE 802.11 foi o WEP (*Wired Equivalence Privacy*) em 1999. Este se mostrou muito vulnerável a ataques de negação de serviço e ataques de força bruta devido à chave de criptografia ser reduzida, reutilizada e estática. Em 2003 houve a primeira atualização na ementa de segurança do IEEE 802.11, sendo assim, foi implantado o protocolo WPA (*Wifi Protected Access*) apenas como solução temporária, enquanto o desenvolvimento da nova ementa era finalizado. Em 2004 foi lançado o IEEE 802.11i. O protocolo de segurança IEEE 802.11i trouxe melhorias relevantes, porém continuou não fornecendo proteção aos quadros de gerenciamento e controle, assim, mantendo as redes WLANs expostas a ataques de negação de serviço [Linhares e Gonçalves, 2008]. Em 2009, foi implementado padrão de segurança denominado IEEE 802.11w, este por sua vez adiciona proteção em alguns quadros de gerenciamento, mas ainda não protegia os quadros de controle [Ahmad e Tadakamadla, 2011].

As falhas existentes nas ementas de segurança do padrão IEEE 802.11 são evidentes. Isso mostra a necessidade em agregar outro mecanismo de segurança nas WLANs para minimizar as ameaças que exploram estas vulnerabilidades. A utilização de um IDS (*Intrusion Detection System*) é parte da solução de segurança. A detecção de intrusos é o processo de monitoramento de eventos que ocorre em um sistema computacional ou rede. Para que o IDS tenha um nível de eficiência alta é necessária uma capacidade de classificação correta, e isto se dá através de bases de dados coletadas para que o modelo de detecção possa aprender. Há uma grande dificuldade em encontrar este tipo de bases de conhecimento para redes IEEE 802.11, a maioria das bases existentes são voltadas para redes cabeadas LAN (*Local Área Network*) ou geradas em ambientes não realísticos [Shiravi et al, 2011].

O objetivo do artigo é apresentar a construção de bases de conhecimento para modelos de detecção de intrusos. As bases foram geradas a partir da implementação de uma rede IEEE 802.11 com criptografia WEP, WPA e WPA2 (*Wifi Protected Access 2*) habilitada em ambiente realístico. Em seguida, foram coletadas amostras de tráfego normal e tráfego anômalo da rede. Os ataques empregados para coleta do tráfego anômalo são do tipo negação de serviço, que tem como finalidade indisponibilizar os recursos e serviços da rede.

Este artigo está organizado em seções. A seção 2 apresenta os trabalhos relacionados encontrados na literatura. A seção 3 aborda como foram montados os experimentos para construção das bases de dados. A seção 4 apresenta as considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

Em [Bicakci e Tavli, 2008], os autores fazem uma revisão teórica sobre ataques de negação de serviço que exploram vulnerabilidades da camada física e MAC das redes IEEE 802.11, com criptografia WEP, WPA e WPA2 habilitada. Ficaram evidentes as fragilidades apresentadas nos quadros de gerenciamento e controle, quando

submetidos a ataques de disponibilidade de serviço. Apesar de o trabalho explorar as vulnerabilidades não foi desenvolvido nenhum mecanismo para auxiliar na proteção das WLANs.

Na abordagem apresentada por [Shiravi et al, 2011], os autores relatam a escassez de bases de detecção de intrusos públicas. Apesar de existirem importantes contribuições como a da DARPA e KDD99, sua precisão e capacidades vêm sendo criticadas, devido ao fato de não terem sido construídas em ambientes reais. A fim de superar estas deficiências foi feita uma abordagem para gerar uma base de dados em um ambiente real, voltado para redes cabeadas, para analisar, testar e avaliar os sistemas de detecção de intrusos. Mesmo sendo construída uma base em ambiente real, ela não contém características específicas das redes sem fio, podendo influenciar na capacidade de detecção do IDS sem fio.

A proposta de [El-Khatib 2010], é gerar uma base de dados obtidos de uma rede sem fio com criptografia WEP e WPA habilitada. O autor menciona que para ter um melhor desempenho, precisão e confiabilidade no sistema de detecção de intrusos sem fio, é necessário extrair os cabeçalhos dos quadros para construção do algoritmo de detecção de intrusos. O trabalho foi realizado em um ambiente sem fio, mas não contempla ataques no padrão IEEE 802.11i.

A construção das bases de dados propostas neste artigo será gerada a partir de uma topologia de rede IEEE 802.11, aplicada em ambiente realístico, com criptografia WEP, WPA e WPA2 habilitada.

3. Metodologia

Os experimentos realizados na rede WLAN, para captura de pacotes e construção das bases de dados, são descritos nessa seção. Para geração da base de dados foram construídos dois cenários reais em ambientes controlados. A subseção 3.1 detalha o primeiro cenário que apresenta características semelhantes à de uma rede utilizada em um ambiente doméstico. No entanto, a subseção 3.2 apresenta o segundo cenário com características mais robustas semelhantes a uma rede utilizada em ambientes coorporativos.

3.1. Construção da Base de Dados para Detecção de Intrusos em uma Rede IEEE 802.11 com Criptografia WEP/WPA Habilitada

Para construção da primeira base de dados, como apresenta a Figura 1, foi montada uma topologia de rede sem fio em um ambiente controlado, com características semelhantes a uma rede de uso doméstico, os seguintes mecanismos de segurança foram habilitados: criptografia WEP e WPA.

A topologia de rede foi constituída por: um ponto de acesso (AP), três estações sem fio. A estação tipo 1 inoculava tráfego de rede normal do tipo (HTTP, FTP). A estação tipo 2 empregou o uso da ferramenta Airplay [Aircrack, 2011]para executar os seguintes ataques de negação de serviço de maneira simultânea (*Chopchop*, deautenticação, fragmentação e duração). A estação do tipo 3 empregou o uso da ferramenta Wireshark [Wireshark, 2011] para executar a coleta das amostras e a ferramenta Tshark [Tshark, 2011]para pré-processar os dados.

Figura 1 – Topologia de rede WLAN aplicada no cenário 1.

Fonte: Elaborado pelo próprio autor.

Foram coletadas amostras de dados para construção da base conhecimento que será utilizada em treinamento de algoritmos de detecção de intrusos. É necessário executar um pré-processamento dos dados, para extrair apenas os campos do cabeçalho MAC dos quadros de gerenciamento, os respectivos campos são: *protocol version*, *type*, *subtype*, to DS, from DS, *more fragment*, *retry*, *power managment*, *more data*, WEP, *order*, *duration*, *address1*, *address2*, *address3* e *sequence control.* O pré-processamento se faz necessário, pois os ataques empregados nesse experimento exploram vulnerabilidades dos quadros de gerenciamento. Portanto a base de conhecimento a ser aplicada na avaliação do classificador deve ser composta pelos quadros de gerenciamento da rede WLAN utilizada nos experimentos, em que a rede esteve sob condição "normal", sem ataques, e sob os ataques *chopchop*, deautenticação, duração e fragmentação.

Esses ataques são do tipo DoS (*Denial of Service)* e exploram vulnerabilidades nos quadros de gerenciamento que afetam a disponibilidade dos recursos e serviços das redes IEEE 802.11 com criptografia pré-RSN. Os ataques de duração e deautenticação prejudicam a capacidade da estação base de gerenciar o acesso à infraestrutura da rede [Bellardo e Savage, 2003]. Os ataques de *chopchop* e fragmentação exploram as fragilidades dos mecanismos de criptografia (WEP e WPA) para deixar o serviço da rede indisponível [Bittau et al, 2006].

A base de dados foi criada utilizando captura por espaço amostral ao invés de captura por dias devido à restrição de recursos e mão de obra. As amostras foram divididas em três conjuntos: treinamento, validação e teste. A Tabela 1 apresenta a distribuição das amostras nos três conjuntos da base de dados e nas categorias de reconhecimento analisadas nos estudos.

A base é formada por 24200 amostras, estes valores foram reproduzidos a partir da base de conhecimento gerada no trabalho desenvolvido por [El-Khatib, 2010] que utiliza espaço amostral para captura dos dados, é constituído da seguinte forma: 9600 amostras conjunto de treinamento, sendo 6000 de tráfego normal e 3600 amostras de tráfego anômalo. O conjunto de validação é formado por 6400 amostras, sendo 4000 amostras de tráfego normal e 2400 amostras de tráfego anômalo. O conjunto de teste é

formado por 8200 amostras, sendo 5000 amostras de tráfego normal e 3200 amostras de tráfego anômalo.

Conjunto das bases de dados			
	Treinamento	Validação	Teste
Normal	6000	4000	5000
ChopChop	900	600	800
Deautenticação	900	600	800
Duração	900	600	800
Fragmentação	900	600	800
Total de Amostras	9600	6400	8200

Tabela 1 – Distribuição das amostras nos conjuntos da base de dados cenário 1.

Fonte: Adaptado de [El-Khatib, 2010].

3.2. Construção da Base de Dados para Detecção de Intrusos em uma Rede IEEE 802.11 com Criptografia WPA2 Habilitada

Para construção da segunda base de dados para detecção de intrusos foi montada uma rede IEEE 802.11, com criptografia WPA2 habilitada, associação segura e mecanismo de autenticação 802.1x (Park et al, 2012). Este tipo de cenário é semelhante ao utilizado em ambientes coorporativos, cuja topologia é representada na Figura 2.

A topologia de rede foi constituída por: cinco estações sem fio, dois pontos de acesso (AP) e um servidor RADIUS. As estações tipo 1,2 e 3 injetavam tráfego normal na rede (HTTP, FTP). A estação tipo 4 utilizou a ferramenta Airplay [Aircrack, 2011], Hping3 e Fake AP [Fakeap, 2007]para realizar os seguintes ataques aleatoriamente, (autenticação falsa, *synflooding*, de autenticação e AP falso). A estação tipo 5 utilizou a ferramenta Wireshark [Wireshark, 2011] para realizar a coleta e a ferramenta Tshark [Tshark, 2011] para realizar o pré-processar os dados. Servidor RADIUS realizava o controle de acesso a rede.

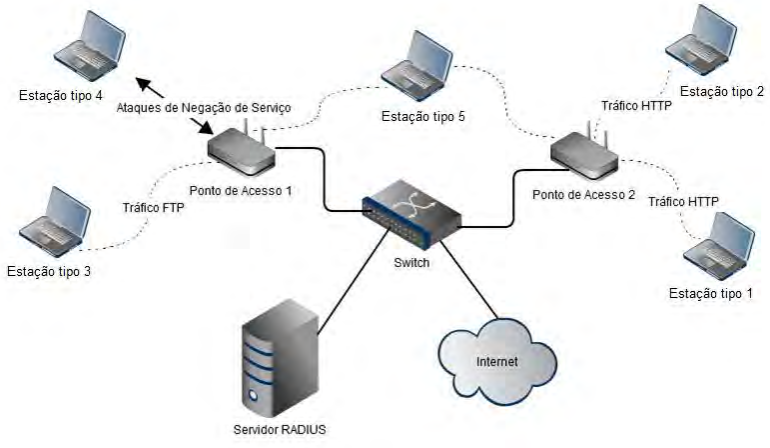

Figura 2 – Topologia de rede WLAN aplicada na geração da base de dados WPA2 habilitada.

Fonte: (Araújo, 2012).

Foi realizado um pré-processamento nos dados capturados para se extrair somente os campos do cabeçalho MAC (*protocol version*, *type*, *subtype*, to DS, from DS, *more fragment*, *retry*, *Power managment*, *more data*, WEP, *order*, *duration*, *address1*, *address2*, *address3* e *sequence control*). A rede esteve sob condição "normal", sem ataques, e sob os ataques autenticação falsa, *synflooding*, deautenticação e AP falso.

A base de dados gerada pelos dados coletados nas experiências segue o método de particionamento de dados *holdout*, desenvolvido por [Smith, 1994], que aloca o espaço amostral dos registros capturados numa proporção de 75% e 25%, respectivamente, nas bases de treinamento e teste.

Conjunto das bases de dados		
	Treinamento	Teste
Normal	4500	1500
Deautenticação	750	250
Autenticação Falsa	750	250
AP Falso	750	250
SynFlooding	750	250
Total de Amostras	7500	2500

Tabela 2 - Distribuição das amostras coletadas nos conjuntos da base de dados cenário 2.

Fonte: Adaptado de [Bishop, 1995].

4. Considerações finais e Trabalhos Futuros

Neste trabalho foram geradas duas bases de conhecimento que possuem potencial no treinamento de algoritmos de detecção de intrusos em redes IEEE 802.11. Isso gera a possibilidade do desenvolvimento de novos modelos de detecção utilizando as características das duas bases propostas. A intenção é que seja explorado o potencial das bases.

A contribuição do trabalho é a construção das bases de dados, que serão utilizadas para ajudar no treinamento de IDS para redes sem fio padrão IEEE 802.11, focando principalmente no problema dos ataques de negação de serviço. Além disso, espera-se que o trabalho estimule uma série de novos estudos na construção de bases de conhecimento por parte de pesquisadores da área.

Conclui-se que muito trabalho ainda pode ser feito. Como a implementação de novos de ataques de negação de serviço. A construção de uma nova topologia de rede, utilizando mecanismo de segurança 802.11w.

Referências

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

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

Araújo, N., Oliveira, R., Shinoda, A., A., Ferreira, E., T. e Nascimento, V. E. (2012), "A Avaliação do Classificador ARTMAP Fuzzy em Redes 802.11 com Criptografia Pré-Robust Security Network (WEP e WPA)", Anais do XII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, p. 310-316.

Bellardo, J. e Savage, S. (2003) "802.11 Denial-of-Service Attacks: RealVulnerabilities 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, vol. 31, p. 931-941.

Bishop, C. M. (1995), Neural Networks for Pattern Recognition. Oxford University Press, 1st edition.

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.

El-Khatib, K. (2010) "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", IEEE Transactions on Parallel and Distributed Systems, vol. 21, n. 8, p. 1143-1149.

Guennoun, M., Lbekkouri, A. e El-Khatib, K. (2008)."Optimizing the feature set of wireless intrusion detection systems". International Journal Of Computer Science And Network Security, S.l., p. 127-131.

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

IEEE Std. 802.11i (2004). "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)", p. 175.

IEEE Std. 802.1X (2001). "IEEE Standard for local and metropolitan area networks - port-based network acess control".

Linhares, A. G. e Gonçalves, P. A. D. S (2008). "Uma Análise dos Mecanismos de Segurança de Redes IEEE 802.11: WEP, WPA, WPA2 e IEEE 802.11w". Universidade Federal de Pernambuco, p. 17.

Park, K., Y., Kim, Y., S. e Kim, Y. (2012). "Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router", Advanced Communication Technology (ICACT), 14th International Conference on. p. 549 – 553.

Shiravi, A., Shiravi, H., Tavallae, M. e Ghorbani, A., A. (2012), "Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection", Computers & Security, vol. 31, p. 357 – 374.

Smith, P., A. (1994). Autocorrelation in logistic regression modeling of species. Global Ecology and Biogeography letters, 4, p. 47-61

Welch, D. e Lanthrop, S. (2003). "Wireless security threat taxonomy", Proceedings of the 2003 IEEE workshop on information assurance**.** p. 76 - 83.

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