



CONSTRUÇÃO E USO DE BASE DE DADOS SOBRE O FUNCIONAMENTO DE UMA REDE SEM FIO PARA CONTRIBUIR NO ENSINO NOS CURSOS DE COMPUTAÇÃO E ENGENHARIA

Ed' Wilson T. Ferreira – edwilson.ferreira@ifmt.edu.br

Ailton A. Shinoda – shinoda@dee.feis.unesp.br

Nelcileo Virgilio de Souza Araujo - nelcileo@yahoo.com.br

Universidade Estadual Paulista “Júlio de Mesquita Filho”

Avenida Brasil, 56 - Centro.

15385-000 - Ilha Solteira - SP

Valtemir E. Nascimento – valtemir.nascimento@cba.ifmt.edu.br

Douglas W. F. L. Vilela - douglas.vilela@blv.ifmt.edu.br

Instituto Federal de Mato Grosso

Rua Zulmira Canavarros, 95 - Centro.

78005-200 – Cuiabá – MT

***Resumo:** O emprego da tecnologia, como ferramenta de apoio e complemento às atividades pedagógicas, nos cursos de graduação, tem se tornado frequente e diversas propostas têm sido apresentados nos últimos anos. Este trabalho apresenta a experiência sobre a construção de uma base de dados, que representa o funcionamento de uma rede sem fio de computadores, com operação em condições normais e também em condições de ataques conhecidos. O objetivo é o emprego desta base nos cursos de engenharia e computação, como apoio nas disciplinas de comunicação de dados, redes de computadores e segurança da informação. O professor poderá explorar conceitos teóricos e relacionados à implementação de redes, bem como assuntos relacionados ao seu funcionamento. Como foi utilizada uma rede física, os alunos terão contato com dados que representam o caso real de um ambiente doméstico (cenário 1) e um ambiente corporativo (cenário 2). Uma vantagem importante desta proposta é a possibilidade do aluno realizar tarefas, baseados na base de dados aqui apresentada, fora do ambiente universitário, sendo necessário apenas um computador, além da facilidade de trabalhar com dados de redes reais, sem a necessidade de instalação física de uma rede de computadores. Espera-se que a abordagem proposta contribua com a melhoria do processo de aprendizagem e também incentive o aluno a realizar pesquisa e estudos dos aspectos teóricos relacionados a esta área de conhecimento.*

***Palavras-chave:** Ensino de engenharia, redes de computadores, segurança da informação, base de conhecimento.*

1. INTRODUÇÃO

Com as expressivas mudanças que ocorreram nos últimos anos, em diversas áreas do conhecimento, o processo de ensino aprendizagem também foi transformado. É fácil perceber



a crescente utilização de dispositivos como telefones inteligentes e *tablets*, que propiciam acesso à Internet, pela população em geral. Esta mudança também ocasionou alteração do perfil dos alunos. Mesmo com valor elevado dos serviços de telecomunicações no Brasil, os alunos mantem acesso diário às redes sociais e serviços que propiciam comunicação instantânea (chat) e compartilhamento de mídia (fotos e vídeos).

A mudança que a sociedade está passando, está forçando também alterações no perfil e na educação das pessoas. Conforme (ANDRADE, 1997), discussões e reformulações sem precedentes têm ocorrido no ensino de engenharia. O impacto do conhecimento tecnológico deve ser observado na educação, afinal tal situação exerce poder sobre a competitividade de empresas e organizações. Estas reformulações são influenciadas, em grande parte, pela tecnologia como aplicação do conhecimento científico ou ciência aplicada.

O conhecimento acumulado nas últimas décadas pela humanidade foi maior do que em toda sua história, segundo (BELHOT, 2005). O avanço do conhecimento foi exponencial, porém os modelos educacionais não acompanharam, pois a mudança foi numa escala linear, gerando problema para absorver tanto conhecimento. Todos estes aspectos considerados, além de questões relativas à baixa remuneração dos profissionais que trabalham na educação, são fatores que interferem na qualidade do sistema educacional do país.

Segundo (BELHOT, 2005), tal situação gera expectativas sobre mudanças que devem ocorrer no ensino, inclusive na engenharia. Portanto questionamentos surgem a respeito de possíveis soluções para melhorar a qualidade sobre a transferência de conhecimento e facilitar a aquisição e uso pelo aluno. Neste contexto, enquanto as pendências não são resolvidas, o professor deve utilizar mecanismos que desperte, no aluno, o interesse pela aquisição de conhecimento, considerando a realidade onde eles estão imersos em um mundo de conectividade e comunicação instantânea.

O emprego da Tecnologia da Informação - TI, nesta era digital, como apresentado por (BARBOSA, 2010), presume-se que o aluno saiba trabalhar com a abundância de recursos disponíveis, então o professor torna-se um orientador no processo. Não é possível afirmar que a TI seja mais eficaz ou relevante do que outras ferramentas para melhorar o processo de ensino, porém, seu emprego em diversas áreas do conhecimento tem demonstrado ganhos consideráveis, portanto, é natural o seu uso no ensino.

Este artigo propõe o emprego de uma base de dados, que representa o funcionamento de uma rede sem fio de computadores, originada através da captura do tráfego de uma rede real. Sugere-se a utilização desta base como apoio no ensino das disciplinas de comunicação de dados e redes, nos curso de computação e engenharia.

O artigo está organizado em seções: na segunda seção são apresentados os trabalhos relacionados e na terceira a metodologia empregada na construção da base. A seção 4 contém sugestões de uso da base e finalmente na seção 5 são expostos os comentários finais.

2. TRABALHOS RELACIONADOS

De acordo com (BELHOT, 2001), a transmissão de conhecimento é utilizada no modelo tradicional de ensino em engenharia, baseado em conceitos sobre os aspectos de diversas teorias. O incentivo à memorização é utilizado para reprodução desses conhecimentos, através da prática repetitiva dos mecanismos e da lógica de funcionamento dos modelos conceituais. Surge um novo conceito, baseado em conjunto de ideias, semelhante a um sistema, com partes interagentes, interdependentes e inter-relacionadas. A proposta consiste na simulação de tal sistema, com a simplificação da realidade.



A proposta do uso de simulação, para melhorar o processo de ensino, não é novidade, porém acredita-se que estudantes dotados de conhecimento e experiências possuem mais facilidade para compreensão da realidade. E mais, a experiência do estudante com a formulação, análise e solução de problemas permitirá sua interação direta com problemas que descrevem a realidade. Tal abordagem também é proposta como reforço em diversas áreas, a exemplo de ensino de modelos gasosos (BALEN & NETZ, 2012), engenharia de software (SOUZA *et al.*, 2010), física (de OLIVEIRA *et al.*, 2010), engenharia de produção (MOLINA *et al.*, 2010) e medicina (REYNOLDS *et al.*, 2011), entre outras.

Com a transformação dos discentes, que anteriormente, eram passivos no processo de ensino, para uma postura interativa, (do CARMO & PONTES, 2012) propõe o emprego de ferramentas disponibilizadas pela web 2.0, especificamente o uso de blogs, para o aluno socializar experiências, tornando fonte de aprendizagem para outros estudantes. Esta simples ferramenta permite diversas vertentes de exploração, seja com abordagem que explora seus recursos (disponibilização de informações pelo professor) ou estratégia pedagógica (portfólio digital, espaço de intercâmbio e colaboração). A pesquisa experimental realizada no curso de Engenharia de Produção da Universidade Federal Rural do Semi-Árido - UFERSA constatou que os blogs possuem potencial para promover a socialização do conhecimento e a interação entre os alunos. Verificou-se que partes das potencialidades foram cumpridas: comunicação entre alunos, registro de visitas técnicas, algumas discussões. Mas alguns aspectos foram negativos, pois se observou que para garantir o desenvolvimento e construção do conhecimento é necessário criar um espaço de confiança entre os alunos.

As simulações de sistemas de engenharia são tarefas que abrange muito conhecimento, tal característica permite seu emprego em Sistemas Baseados em Conhecimento. A proposta apresentada por (PEPPLOW, 2010) refere-se ao desenvolvimento de uma base de conhecimento aplicada para orientar o projeto de sistemas de engenharia, com capacidade de representação de sistemas físicos por meio de utilização de modelos matemáticos. Tal abordagem permite a simulação de sistemas e análise do comportamento dinâmico. Foi comprovado o ganho no aprendizado dos alunos, relativos aos conhecimentos gerais, bem como em modelagem e simulação, área de conhecimento desconhecida pela maioria dos alunos.

Percebe-se que a utilização de computadores, softwares de simulação, enfim, os recursos disponibilizados pela Tecnologia da Informação tornou-se importante ferramenta de apoio pedagógico, cujo objetivo é incentivar a busca do conhecimento pelos alunos, onde o professor assume o papel de orientador. Colaborando com este cenário, neste artigo é apresentada uma proposta do uso da tecnologia, para as disciplinas de comunicação de dados e redes de computadores, nos cursos de engenharia e computação.

3. METODOLOGIA EMPREGADA NA CONSTRUÇÃO DA BASE DE DADOS

Foram realizados experimentos com o emprego de uma rede sem fio de computadores. A rede foi projetada, instalada e configurada conforme o uso comum em ambiente doméstico (de usuário) e cenários corporativos (empresas). O objetivo do ensaio realizado foi permitir a captura de todo o tráfego na rede, para armazenamento em um banco de dados, como descrito em (VILELA *et al.*, 2013).

Com o objetivo de criar ambientes com grau de complexidade distinta, foram criados dois cenários de experimentos, um modelo simples baseado em WEP e WPA e outro mais complexo que faz uso de WPA2.

3.1 Cenário 1: Base de Dados com Criptografia WEP/WAP Habilitada

A topologia escolhida, para o cenário 1, é apresentada na Figura 1. Este cenário possui características típicas de uma rede de ambiente doméstico.

A *Wired Equivalent Privacy* - WEP, ou privacidade equivalente à rede cabeada foi projetada para prover nível de segurança às redes sem fio equivalente as redes cabeadas, através do algoritmo RC4. Porém, diversas fragilidades foram descobertas nesta implementação, como apresentado por (LASHKARI *et al.*, 2009) e (KUMKAR, 2012), mas a configuração foi utilizada por questões pedagógicas e para manter os aspectos históricos.

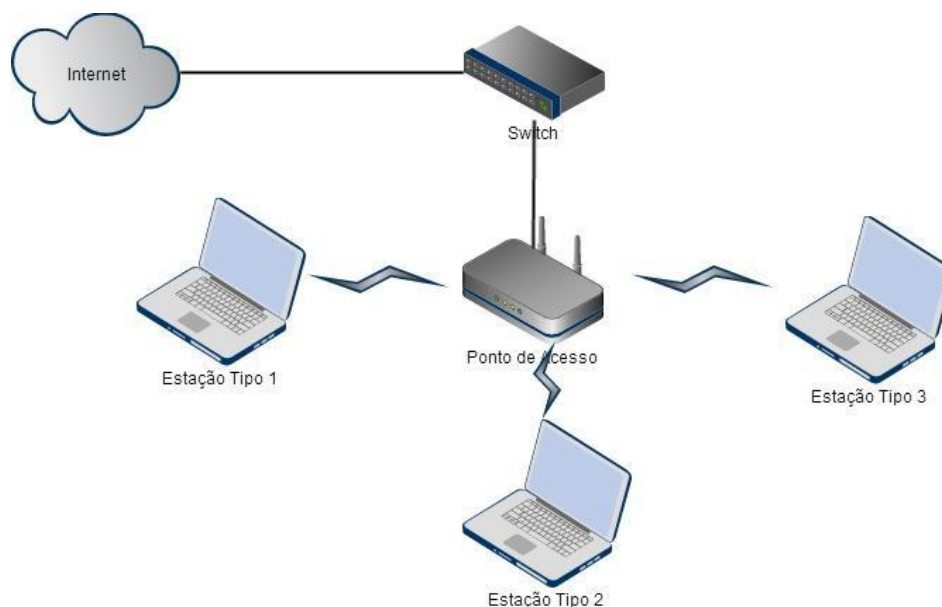


Figura 1: Topologia da rede, cenário 1

A *WiFi Protected Access* - WPA, foi desenvolvida com objetivo de resolver os problemas de falhas de segurança encontrados na WEP, sem a necessidade de substituição do hardware existente, (LEITÃO *et al.*, 2010). Seu funcionamento pode ser agrupado em dois modos: WPA pessoal ou WPA-PSK, baseado na utilização de uma chave compartilhada, para uso doméstico e WPA empresarial, que faz uso de servidor de autenticação 802.1x, que permite melhor gestão e controle de segurança.

A topologia empregada no cenário 1 possui: um ponto de acesso (AP) e três estações de rede. O tráfego gerado na rede pela Estação Tipo 1 foi composto por HTTP e FTP (tráfego normal). A Estação Tipo 2 foi utilizada para gerar ataques de negação de serviço com o software AirPlay (AIRCRACK, 2013). Este software é capaz de quebrar senhas utilizadas nas implementações IEEE 802.11 WEP e WPA-PSK através da recuperação de chaves contidas nos pacotes capturados. Os ataques utilizados foram *ChopChop*, de autenticação, fragmentação e duração, conforme apresentado em (ARAÚJO *et al.*, 2012). Finalmente, a Estação Tipo 3 foi utilizada para executar a coleta dos dados transmitidos na rede, com o software Wireshark (WIRESHARK, 2013).



Os ataques do tipo *Denial of Service - DoS*, ou negação de serviços, exploram vulnerabilidades que afetam a disponibilidade dos recursos das redes IEEE 802.11 com criptografia pré-RSN. Os ataques de duração e de autenticação prejudicam a capacidade da estação base de gerenciar o acesso à infraestrutura da rede (BELLARDO & SAVAGE, 2003). Os ataques de *chopchop* e fragmentação exploram vulnerabilidades dos mecanismos de criptografia para tornar a rede indisponível (BITTAU *et al.*, 2006).

Para criar a base de dados, o tráfego da rede foi capturado e armazenado em arquivos. Foi necessário executar pré-processamento para extrair os dados de interesse, representados por alguns campos dos quadros MAC: *protocol version, type, subtype, to DS, from DS, more fragment, retry, power management, more data, WEP, order, duration, address1, address2, address3 e sequence control*, uma descrição dos campos que compõem os quadros MAC é apresentada em (QIAO *et al.*, 2002). Este pré-processamento é importante porque os ataques escolhidos para comporem os experimentos exploram vulnerabilidades dos quadros de gerenciamento.

Os dados capturados foram e organizados em amostras por três conjuntos: treinamento, validação e testes, com as quantidades apresentadas conforme a Tabela 1. A base foi formada por 24200 amostras, sendo parte reservada para treinamento, validação e testes, conforme trabalho desenvolvido por (EL-KHATIB, 2010). Esta divisão é importante para permitir que a base gerada possa ser utilizada também para avaliação de proposta de Sistemas de Detecção de Intrusão e nas aulas relacionadas à segurança da informação.

Tabela 1: Distribuição das amostras nos conjuntos de dados, cenário 1

Tipo	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

O *Intrusion Detection System* – IDS ou Sistemas de Detecção de Intrusão, monitora dinamicamente eventos em um sistema, e decide quando estes eventos são indícios de um ataque ou constitui uso legítimo de sistema, (WU & BANZHAF, 2010). Geralmente os IDS precisam de uma base de conhecimento utilizada para treinamento e testes, e este experimento também permite a utilização da base gerada para ser empregada na comparação ou estudos sobre os sistemas de detecção de intrusão e comparação entre as diversas abordagens propostas.

3.2 Cenário 2: Base de Dados com Criptografia WPA2 Habilitada

O cenário 2 foi projetado para ser um ambiente com maior nível de complexidade, quando comparado com o cenário 1. Foi habilitado o WPA2 (SAKIB et al., 2012), associação segura e mecanismo de autenticação baseado no padrão IEEE 802.1x (ALI et al., 2010). A topologia empregada, como mostrado na Figura 2, representa o ambiente que geralmente é encontrado nas organizações. O WPA2 é bastante utilizado, porém ainda possui vulnerabilidades que podem ser exploradas (TEWS & BECK, 2009).

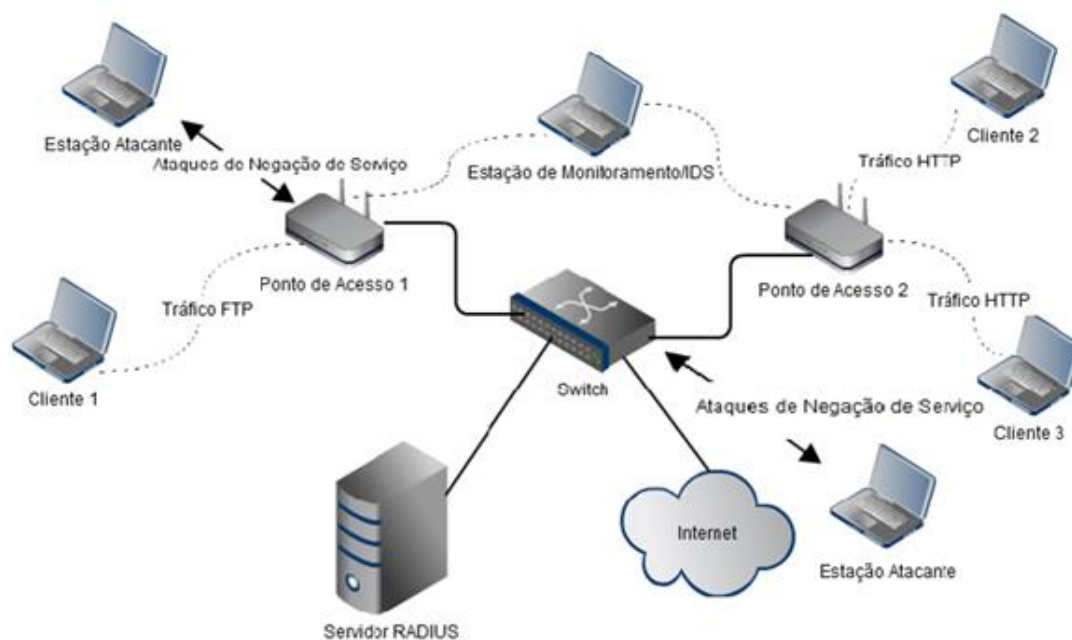


Figura 2: Topologia da rede, cenário 2

A rede utilizada possui cinco estações sem fio, dois pontos de acesso (AP) e um servidor RADIUS que é utilizado para autenticação de usuários. Três estações sem fio foram usadas para gerar tráfego normal na rede, com aplicações web (HTTP e FTP). Uma estação atacante foi configurada para gerar ataques baseados no Airplay, hping3 e Fake AP (AIRCRAK, 2013), para aplicar os ataques de autenticação falsa, synflooding, de autenticação e AP Falso. Finalmente, a outra estação foi utilizada para realizar a captura dos dados, com o software Wireshark (WIRESHARK, 2013).

Os dados capturados foram pré-processados para extrair os campos do cabeçalho MAC: *protocol version, type, subtype, to DS, from DS, more fragment, retry, power management, more data, WEP, order, duration, address1, address2, address3 e sequence control*. Durante o tempo de captura dos dados, a rede esteve em condições normais de funcionamento, sem ataques, e também em condições anômalas, sendo atacada.

A metodologia de organização dos dados coletados neste experimento segue a proposta de divisão de dados *holdout*, (SMITH, 1994), com a distribuição do espaço amostral dos registros numa proporção de 75% e 25%, respectivamente, nas bases de treinamento e testes. A quantidade de registros é apresentada na Tabela 2.



Tabela 2: Distribuição das amostras nos conjuntos de dados, cenário 2

Tipo	Treinamento	Teste
Normal	4500	1500
Deautenticação	750	250
Autenticação Falsa	750	250
AP Falso	750	250
Synflooding	750	250
Total de Amostras	7500	2500

O objetivo de gerar dois conjuntos de dados, com topologia e número de amostras diferentes foi de disponibilizar um ambiente heterogêneo para aplicação dos experimentos propostos neste artigo e também para os experimentos criados pelo professor da disciplina.

4. EXEMPLO DE USO DA PROPOSTA

O aluno de graduação, futuro engenheiro, deve visualizar o computador como uma ferramenta que será utilizada para desempenhar suas atividades, portanto é importante que tenha familiaridade com este recurso, logo é salutar o emprego da TI durante a sua formação, (FRANCHI, 2001).

As ferramentas disponibilizadas pela TI facilitam o entendimento da teoria pelos alunos. Aspectos importantes relativos às normas e funcionamento das redes de comunicação e de computadores podem ser observados na prática, tornando os conceitos familiares para os discentes. O professor poderá exibir, com o emprego de diversos softwares, os parâmetros configurados de uma rede. Como apresentado na Figura 3, os campos que compõem o cabeçalho dos quadros IEEE 802.11b podem ser observados: protocolo, tamanho do cabeçalho, flags, taxa de transmissão, canal utilizado, tipo de canal, entre outras informações. Todos estes dados podem ser explorados pelo professor durante as aulas expositivas.

Como mostrado na Figura 4, a partir dos dados capturados, o professor poderá explorar o conteúdo relacionado à comunicação na rede e mostrar para os alunos como ocorre a troca de dados entre as estações, através das colunas *Address A* e *Address B*, além da duração e quantidade de dados transportados. Pode-se observar também o tráfego em *broadcast*, que é direcionado par toda a rede.

```

Frame 2: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Interface id: 0
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
Arrival Time: Nov 8, 2012 16:59:52.287382000 Horário de Verão Brasil Central
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1352404792.287382000 seconds
[Time delta from previous captured frame: 0.102447000 seconds]
[Time delta from previous displayed frame: 0.102447000 seconds]
[Time since reference or first frame: 0.102447000 seconds]
Frame Number: 2
Frame Length: 150 bytes (1200 bits)
Capture Length: 150 bytes (1200 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan]
Radiotap Header v0, Length 18
Header revision: 0
Header pad: 0
Header length: 18
Present flags
Flags: 0x00
Data Rate: 1,0 Mb/s
Channel frequency: 2412 [BG 1]
Channel type: 802.11b (0x00a0)
SSI signal: -65 dBm
Antenna: 1
RX flags: 0x0000
IEEE 802.11 Beacon frame, Flags: .....
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (96 bytes)
    
```

Figura 3: Campos que compõem o cabeçalho dos quadros de uma rede sem fio

Os dados capturados, que representam os ataques também podem ser observados, conforme mostrado na Figura 5. Neste cenário, o quadro de gerenciamento, com o comando de deautenticação, não foi gerado pelo sistema, mas por um atacante. As estações que receberam este quadro não possuem condições, normalmente, para realizar esta identificação, então o usuário perceberá o problema através da indisponibilidade do acesso, gerado pelo ataque.

WLAN Conversations											
Address A	Address B	Packets	Bytes	Packets A-B	Bytes A-B	Packets A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
SenaInt_75:cf:1e	Broadcast	61	9 150	0	0	0	0	0,000000000	6,1457	11910,79	N/A
IntelCor_a5:eb:94	LiteonTe_3f:ad:1b	633	399 443	346	357 629	287	41 814	0,138421000	6,0736	471060,71	55076,44
SenaInt_75:cf:1e	HonHaiPr_64:5a:58	16	1 656	7	1 008	9	648	0,272958000	5,0019	1612,18	1036,40
IntelCor_41:de:f0	Broadcast	79	10 066	79	10 066	0	0	0,292494000	5,7324	14047,93	N/A
IPv6mcast_ff:2e:18:61	HonHaiPr_13:ca:ad	6	820	0	0	6	820	0,348805000	0,9922	N/A	6611,71
Compalln_b6:44:5e	Broadcast	6	664	6	664	0	0	0,481274000	0,0082	650900,62	N/A
3comEuro_75:20:41	Broadcast	18	1 992	18	1 992	0	0	0,500612000	4,9730	3204,49	N/A
3comEuro_74:b4:81	Broadcast	20	2 208	20	2 208	0	0	0,652805000	5,0005	3532,48	N/A
SenaInt_75:cf:18	Routerbo_77:93:00	4	504	0	0	4	504	0,791252000	4,9963	N/A	806,99
3comEuro_a5:55:9b	Broadcast	3	344	3	344	0	0	1,579088000	0,0021	1293841,09	N/A
SenaInt_75:cf:1e	IntelCor_41:de:f0	8	1 152	8	1 152	0	0	2,315028000	0,1512	60960,04	N/A
IPv6mcast_00:00:00:0c	HonHaiPr_13:ca:ad	7	1 808	0	0	7	1 808	2,476251000	2,9273	N/A	4941,02
Dell_b3:5c:0b	Broadcast	9	2 337	9	2 337	0	0	2,753648000	1,9999	9348,43	N/A
Hewlett-_24:d5:7b	Broadcast	14	4 496	14	4 496	0	0	3,168330000	1,3692	26270,24	N/A

Figura 4: Estatística de comunicação entre os nós da rede

Finalmente, na Figura 6, pode-se observar a transmissão dos quadros de gerenciamento e a identificação de parâmetros importantes da comunicação, como beacom e número de sequencia (SN).

Destination	Protocol	Length	Info
f:1e Broadcast	802.11	44	Deauthentication, SN=774, FN=0, Flags=.....
f:1e Broadcast	802.11	44	Deauthentication, SN=775, FN=0, Flags=.....
f:1e Broadcast	802.11	44	Deauthentication, SN=776, FN=0, Flags=.....
f:1e Broadcast	802.11	44	Deauthentication, SN=777, FN=0, Flags=.....
f:1e Broadcast	802.11	44	Deauthentication, SN=778, FN=0, Flags=.....
f:1e Broadcast	802.11	44	Deauthentication, SN=779, FN=0, Flags=.....

Figura 5: Identificação do tráfego gerado pelo ataque Deautenticação

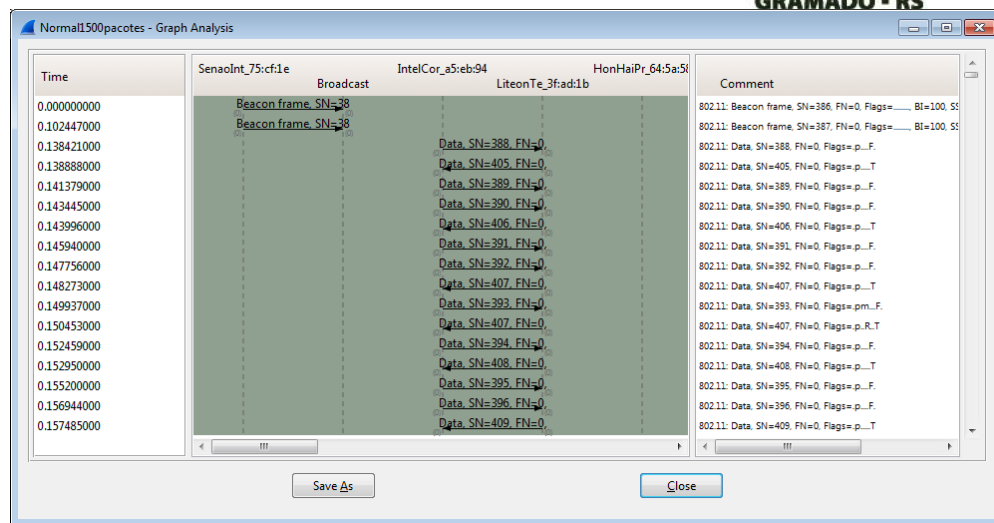


Figura 6: Identificação de quadros de gerenciamento

São inúmeras as opções para utilização da base de dados com objetivo de auxiliar o processo de ensino na computação e engenharia. O professor poderá explorar outras formas, através de listas de exercícios, identificação dos quadros de gerenciamento, pesquisas estatísticas sobre a distribuição de tráfego na rede, entre outras opções possíveis.

5. COMENTÁRIOS FINAIS

Neste artigo foi apresentada uma proposta que descreveu a geração de uma base de dados, com dois cenários distintos, que representam o funcionamento de duas redes sem fio de computadores, trabalhando em condições normais e também em situação de diversos ataques.

As atividades práticas, possibilitadas pelo uso da base desenvolvida nestes experimentos são inúmeras, o professor poderá utilizá-la tanto para demonstrar a teoria como também para solicitar atividades dos alunos. A base pode ser utilizada também nas disciplinas relacionadas à segurança, especialmente nos cursos que abordam os Sistemas de Detecção de Intrusão e Segurança em Redes sem Fio.

A base de dados obtida através dos experimentos descritos neste artigo foi obtida a partir de uma rede real, que permanece em funcionamento em uma instituição acadêmica. Portanto, os dados obtidos representam o comportamento natural dos usuários, além dos ataques disparados contra a rede, gerado pelos autores. É possível a instalação e configuração de uma rede sem fio, para uso em sala de aula, porém, o docente precisará repetir os procedimentos descritos nesta proposta e o tempo necessário para tal tarefa poderá comprometer o curso.

Por outro lado, pode-se fazer uso de bases distribuídas por algumas instituições de ensino e pesquisa. Contudo, a base de dados, gerado neste projeto, possui algumas características, a exemplo da topologia, que reflete o uso comum deste tipo de rede. Além disso, por ter sido instalada em uma instituição acadêmica, os dados trabalhados são de uma rede real, sem o emprego dados oriundos de simulação.

A tecnologia em si não é completa, trata-se de uma ferramenta que deverá ser utilizada pelo professor, como complemento nas atividades pedagógicas. Portanto, o professor continua

desempenhando um importante papel no processo de transmissão de conhecimento e da experiência adquirida ao longo do tempo, que envolve as atividades de ensino, pesquisa e extensão.

Como trabalhos futuros sugere-se a criação de roteiros de atividades para serem desenvolvidas pelos alunos. Os exercícios deverão contemplar aspectos teóricos, como a identificação de informações sobre as implementações dos padrões de rede, a partir da pesquisa na base de dados, bem como realizar avaliações de diversas abordagens de IDS.

Agradecimentos

Os autores agradecem a Fundação de Amparo a Pesquisa do Estado do Mato Grosso – FAPEMAT.

REFERÊNCIAS BIBLIOGRÁFICAS

AIRCRAK. **AirCrack-NG**. Disponível em: <<http://www.aircrack-ng.org/>> Acesso em: 14 jun. 2013.

ALI, Humayra Binte et al. Modeling and verification of Extensible Authentication Protocol for Transport layer Security in Wireless LAN environment. In: **Software Technology and Engineering (ICSTE), 2010 2nd International Conference on**. IEEE, 2010. p. V2-41-V2-45.

ANDRADE, Emmanuel Paiva; BRITO, Guilherme Silva Xavier de; OLIVEIRA, Martha Lucia Alcantara de. Aspectos cognitivos do ensino de engenharia face às exigências da competitividade e da inovação tecnológica. **ENCONTRO NACIONAL DE ENGENHARIA DE PRODUÇÃO**, 1997.

ARAÚJO, Nelcilenio et al. Performance Evaluation of the Fuzzy ARTMAP for Network Intrusion Detection. In: **Recent Trends in Computer Networks and Distributed Systems Security**. Springer Berlin Heidelberg, 2012. p. 23-34.

BALEN, Osvaldo; NETZ, Paulo Augusto. Aplicação da modelagem e simulação no ensino de modelos de sistemas gasosos. **Volume 7-Número 2-jul./dez. 2005**, v. 7, n. 2, p. 29, 2005.

BARBOSA, Ronaldo. Perspectivas de uso do computador no ensino. **Anuário da produção acadêmica docente**, v. 3, n. 5, p. 163-182, 2010.

BELHOT, Renato V. A didática no ensino de engenharia. In: **XXXIII CONGRESSO BRASILEIRO DE ENSINO DE ENGENHARIA**. 2005.

BELHOT, Renato V.; FIGUEIREDO, Reginaldo S.; MALAVÉ, Cesar O. O uso da simulação no ensino de engenharia. In: **Congresso Brasileiro de Ensino de Engenharia, XXIX COBENGE**. 2001. p. 445-451.

BELLARDO, John; SAVAGE, Stefan. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In: **Proceedings of the USENIX Security Symposium**. 2003. p. 15-28.

BITTAU, Andrea; HANDLEY, Mark; LACKEY, Joshua. The final nail in WEP's coffin. In: **Security and Privacy, 2006 IEEE Symposium on**. IEEE, 2006. p. 15 pp.-400.

DO CARMO, Breno Barros Telles; PONTES, Renata Lopes Jaguaribe. Utilização do Blog como ferramenta para incentivar a aprendizagem colaborativa na disciplina de arranjos produtivos organizacionais. **Revista de Ensino de Engenharia**, v. 31, n. 1, p. 40-52, 2012.

EL-KHATIB, Khalil. Impact of feature reduction on the efficiency of wireless intrusion detection systems. **Parallel and Distributed Systems, IEEE Transactions on**, v. 21, n. 8, p. 1143-1149, 2010.

FRANCHI, R. H. O. L Utilização de softwares nas aulas de matemática para engenharia: reflexão a partir de atividades desenvolvidas. In: **XXIX CONGRESSO BRASILEIRO DE ENSINO DE ENGENHARIA**, 2001.

KUMKAR, Vishal et al. Vulnerabilities of Wireless Security protocols (WEP and WPA2). **International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)**, v. 1, n. 2, p. pp: 34-38, 2012.

LASHKARI, ARASH Habibi; DANESH, Mir Mohammed Seyed; SAMADI, Behrang. A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). In: **Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on**. IEEE, 2009. p. 48-52.

LEITÃO, Mário et al. Avaliação de sobrecarga dos mecanismos de segurança WEP e WPA em redes 802.11 g. **Communication Technology**, v. 1, n. 1, 2010.

MOLINA, Carlos Eduardo Corrêa; MARINS, Fernando Augusto Silva; MONTEVECHI, José Arnaldo Barra. PROPOSTA DE UTILIZAÇÃO DA SIMULAÇÃO A EVENTOS DISCRETOS NO ENSINO DA ENGENHARIA DE PRODUÇÃO. **Revista P&D em Engenharia de Produção V**, v. 8, n. 01, p. 11-15, 2010.

PEDRO, Márcia Valpassos; SAMPAIO, Fábio Ferrentini. JLinkIt: Um ambiente de modelagem dinâmica computacional para o ensino-aprendizagem de Ciências. In: **Anais do Simpósio Brasileiro de Informática na Educação**. 2007. p. 61-70.

PEPPLOW, Luiz Amilton et al. Base de Conhecimento para Aplicação no Ensino de Modelagem e Simulação de Sistemas de Engenharia. In: **Anais do XXXVIII Congresso Brasileiro de Educação em Engenharia**. 2010.

QIAO, Daji; CHOI, Sunghyun; SHIN, Kang G.. . Goodput analysis and link adaptation for IEEE 802.11 a wireless LANs. **Mobile Computing, IEEE Transactions on**, v. 1, n. 4, p. 278-292, 2002.

REYNOLDS, A., de CAMPOS, D. A., & BERNARDES, J. (2011). Utilização das metodologias de simulação médica no ensino e aprendizagem nas escolas médicas Portuguesas. **Acta Médica Portuguesa**, 24(2), 223-30.

SAKIB, Nazmus et al. WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis and Improvement. **Global Journal of Computer Science and Technology**, v. 12, n. 6, 2012.

SMITH, P. A. Autocorrelation in logistic regression modelling of species' distributions. **Global ecology and biogeography letters**, p. 47-61, 1994.



SOUZA, M. M., RESENDE, R. F., PRADO, L. S., FONSECA, E. F., CARVALHO, F. A., & RODRIGUES, A. D. **SPARSE: Um Ambiente de Ensino e Aprendizado de Engenharia de Software Baseado em Jogos e Simulação.** 2010.

TEWS, Erik; BECK, Martin. Practical attacks against WEP and WPA. In: **Proceedings of the second ACM conference on Wireless network security.** ACM, 2009. p. 79-86.

VILELA, D. W. F. L. ; SHINODA, A. A. ; FERREIRA, E. T. ; Oliveira, Ruy ; NASCIMENTO, V. E. ; ARAÚJO, N. V. S. . 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. In: EnAComp, X Encontro Anual de Computação, 2013, Catalão. EnAComp, X Encontro Anual de Computação, 2013. p. 145-151.

WIRESHARK. **WIRESHARK.** Disponível em: <<http://www.wireshark.org/>> Acesso em: 14 jun. 2013.

WU, Shelly Xiaonan; BANZHAF, Wolfgang. The use of computational intelligence in intrusion detection systems: A review. **Applied Soft Computing**, v. 10, n. 1, p. 1-35, 2010.

CONSTRUCTION AND USE OF DATABASE ON THE OPERATION OF A WIRELESS NETWORK TO CONTRIBUTE IN EDUCATION COURSES IN THE COMPUTER SCIENCE AND ENGINEERING

***Abstract:** The use of technology as a tool to support and complement the teaching activities in undergraduate courses, has become frequent and various proposals have been presented in recent years. This paper presents the experience of building a database that represents the operation of a wireless computer, operating under normal conditions and in conditions well-known attacks. The aim of this work is the basis of computing and engineering courses, as support in the disciplines of data communications, computer networks and information security. The teacher can explore theoretical concepts related to the implementation of networks, as well as issues related to its operation. Was used as a physical network, students will have contact with data representing the real case of a domestic environment (scenario 1) and a corporate environment (scenario 2). An important advantage of this proposal is the ability of the student to perform tasks based on the database presented here, outside the university environment, requiring only a computer and the ease of working with data from real networks, without the need for physical installation of a computer network. It is expected that the proposed approach contributes to the improvement of the learning process and also encourage students to conduct research and studies of the theoretical aspects related to this field of knowledge.*

Key-words: engineering course, computers networks, information security, knowledge base.