The Development and Evaluation of a Dataset for Testing of IDS for Wireless Networks

E. W. T. Ferreira and A. A. Shinoda

***Abstract*— This paper originates from research that investigated about the creation of the dataset representative of a wireless computer network. The proposal was intended to generate the dataset from network traffic of a real wireless network to be employed in the evaluation of Intrusion Detection Systems - IDS. Several attacks were granted against the network in order to obtain data from these anomalous behaviors. The methodological procedures performed involved the capture of the traffic on the wireless network and it's pre-processing to generate the dataset. To evaluate the dataset the following pattern classification algorithms were employed: Bayesian Networks, Decision Tables, IBK, J48, MLP and NaiveBayes, which are generally used in implementation of IDS. In addition, the Kappa coefficient was also used to assist in measure of the efficiency of algorithms employed. The good results obtained show that the data set can be used to compare different approaches of IDS for wireless networking.**

***Keywords*— Dataset, Intrusion Detection Systems IDS, Wireless Network, Information Security, Coefficient Kappa.**

I. INTRODUÇÃO

A SEGURANÇA da informação tornou-se fundamental para garantir o correto funcionamento das redes e sistemas computacionais. A segurança da informação está relacionada com a tríade: integridade, confidencialidade e disponibilidade. A integridade está pautada com a exatidão da informação, com a confiança de que a mesma não sofreu alterações. A confidencialidade é o processo que busca garantir acesso somente de usuários autorizados. A disponibilidade relaciona-se com a certeza de que os usuários autorizados terão acesso à informação quando necessitarem. As ações com objetivo de comprometer estes pilares da segurança podem ser classificadas como uma intrusão. Os procedimentos, com objetivo de identificar e isolar intrusos é chamado detecção de intrusão.

Um Sistema de Detecção de Intrusão – IDS é um software utilizado para detectar uso, ou tentativa de uso, sem autorização. Um IDS deve ser capaz de descobrir a existência de tráfego malicioso em uma rede de computadores. Isso inclui ataques, exploração de vulnerabilidade de serviços, tentativa de aumento de privilégios, acesso sem autorização além de tentativas de acesso a arquivos [1].

Com a grande disponibilidade das redes sem fio, houve também o crescimento de ataques e exploração de vulnerabilidade contra estas redes. Com a abrangência metropolitana, em alguns momentos pode-se encontrar pessoas que caminham pela cidade e realizam o mapeamento das redes, com objetivo de descobrir e explorar vulnerabilidades [2], portanto, torna-se evidente a necessidade de aprimorar a segurança das redes sem fio.

A avaliação de IDS em redes reais pode interferir na disponibilidade ou aplicações dos usuários. Além disso, a comparação entre abordagens distintas seria prejudicada, pois é difícil implantar o mesmo cenário, utilizado em testes de diferentes autores. Neste caso, a exemplo da base KDD 99 para redes cabeadas [3], utilizar uma base de dados específica de rede sem fio torna-se muito importante para permitir a avaliação de diversas propostas de IDS utilizando o mesmo cenário.

As bases de dados desempenham um importante papel na validação de um Sistema de Detecção de Intrusão. A qualidade dos dados permite não só avaliar a habilidade método proposto na detecção de comportamento intrusivo, mas também mostra a potencial eficácia do IDS no ambiente operacional. No geral, devido a falta de melhores conjuntos de dados, a maioria das pesquisas no campo de IDS baseiam-se em conjuntos com dados oriundos de simulação [4].

As redes sem fio possuem características próprias que diferem de redes com fio [5]–[8]. Estas propriedades, concebidas no conjunto de dados sobre a rede sem fio, criado a partir dos dados que trafegam em uma rede real, representa um ambiente isento de simulação.

Portanto, a captura, processamento e armazenamento dos dados obtidos da rede sem fio, permitiu a organização do banco de conhecimento, importante feito para realização de avaliação de diversas abordagens para detecção de intrusão, afinal são poucos conjuntos de dados de redes sem fio disponibilizados atualmente [9].

O conjunto de dados espelhou o comportamento dos usuários de uma rede sem fio em funcionamento. Estes dados contribuem também com pesquisas que utilizam simulação, pois podem ser utilizados como mecanismo de comparação entre dados simulados e dados obtidos de uma rede real.

O objetivo geral neste artigo é o de apresentar o resultado acerca da criação e avaliação de um conjunto de dados representativos do funcionamento de uma rede sem fio, com finalidade de ser utilizada em avaliações de IDS.

As próximas seções deste artigo estão organizadas da seguinte maneira: na seção 2 são apresentados os trabalhos relacionados. A seção 3 contém a metodologia empregada na construção do conjunto de dados, enquanto que na Seção 4 são apresentados os resultados das avaliações dos conjuntos de dados. Finalmente, na sequencia são apresentadas as considerações finais e sugestões de trabalhos futuros.

E. W. T. Ferreira, Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), Ilha Solteira, São Paulo, Brasil, Instituto Federal de Mato Grosso (IFMT), Cuiabá, Mato Grosso, Brasil, edwilson.ferreira@ifmt.edu.br

A. A. Shinoda, Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), Ilha Solteira, São Paulo, Brasil, shinoda@dee.feis.unesp.br

II. TRABALHOS RELACIONADOS

Existem diferentes propostas para construção de IDS: aprendizagem de maquina [10], consumo de energia dos hosts em redes ad hoc sem fio, mineração de dados [11]. Para avaliar as diversas propostas de IDS, pesquisadores costumam utilizar o conjunto de dados de auditoria disponibilizado pelo laboratório Lincoln do MIT denominado KDD 99 [12]–[14]. Esta base foi construída em 1999 através da captura do tráfego da rede e também com a inclusão de dados que simulam certos tipos de ataques. Após o processamento, estes dados passaram a ser utilizados como referência para análise de desempenho em uma competição de IDS em 1999.

A base KDD 99 é muito antiga, mesmo sendo considerada referência para avaliação de IDS. As técnicas de invasão evoluíram e diversos ataques foram criados ao longo desta década. Além disso, o KDD 99 foi baseado em uma rede cabeada de computadores, assim não contempla certas características que são particulares de redes sem fio.

Na pesquisa desenvolvida por [15] foi empregado um conjunto de dados para realizar o treinamento e teste de classificadores. O conjunto foi gerado através da captura do tráfego de uma rede sem fio composta por apenas 3 estações e 1 ponto de acesso. Foi gerado uma base com 24200 amostras da rede.

Muitos conjuntos de dados, utilizados para avaliação de IDS, são internos e não podem ser compartilhados, por questões de privacidade, outros sofreram um processo de para tornar anônimos os usuários ou ainda foram processados e certos dados foram removidos, alterando característica importantes do conjunto e assim não refletem o verdadeiro comportamento na rede [9].

Portanto, a criação de um conjunto de dados, para ser empregado em avaliação de IDS torna-se importante, e este foi o objetivo desta pesquisa.

III. ESTRATÉGIA DE CONSTRUÇÃO DO CONJUNTO DE DADOS

Para construir o conjunto de dados, que deve representar o funcionamento real de uma rede sem fio, optou-se em capturar dados de uma rede existente. A rede atende usuários de um campus de uma instituição de ensino, com isso, foi possível a obtenção de dados fidedignos do comportamento dos usuários. O panorama de tráfego, monitorado durante uma semana, é apresentado na Fig. 1. Percebe-se que a utilização é mais intensa no início da noite. Provavelmente isso ocorre devido à chegada dos alunos dos cursos noturnos. De forma semelhante, o cenário se repete no início da manhã.

Uma rede sem fio apresenta facilidades para realizar a captura de dados. Com a transmissão dos dados é realizada pelo ar, torna-se desnecessário a ligação física cabeada entre o equipamento que realiza a captura e os outros equipamentos da rede. É necessário apenas um computador com interface de rede sem fio configurado em modo promíscuo, que permite o recebimento de dados em todos os canais disponíveis.

Os dados capturados contém atributos que são específicos das redes sem fio. Tais atributos são encontrados na camada física e de enlace, visto que as camadas superiores são semelhantes nas redes cabeadas e sem fio. Portanto, o processo de captura foi executado com objetivo de obter os quadros que são transportados na camada de enlace da rede. O conjunto de dados contém informações obtidas dos campos *protocol version, type, subtype, to DS, from DS, more fragment, retry, power management, more data, WEP, order, duration, address1, address2, address3 e sequence control*.

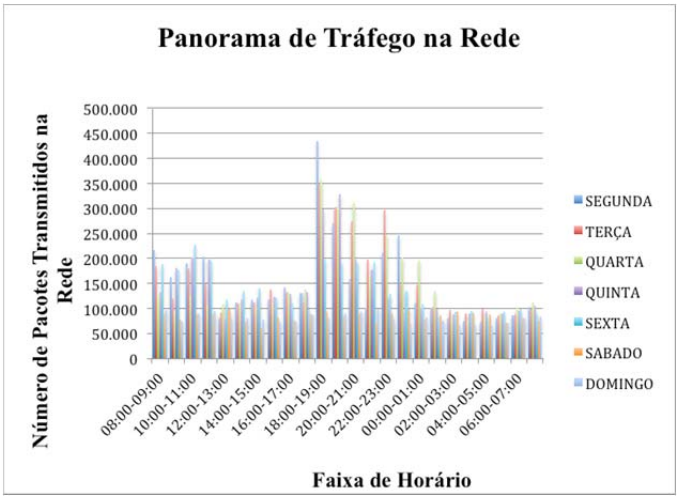

Figura 1. Panorama de Tráfego na Rede.

Um fragmento do Conjunto de Dados é mostrado na Fig. 2. Os dados são separados por vírgula e cada linha representa e descreve um quadro que foi capturado. Deve-se observar que a última coluna indica o tipo de tráfego, portanto, trata-se de uma base rotulada. O rótulo é utilizado para verificar a eficiência do algoritmo de detecção utilizado pelo IDS avaliado.

```
0,2,0,1,1,0,0,0,0,0,0,1,4,15,2,117,2,Normal
0,1,13,0,0,0,0,0,0,0,0,0,2,0,0,2,Normal
0,1,13,0,0,0,0,0,0,0,0,7,0,0,2,Normal
0,0,8,0,0,0,0,0,0,0,0,1,9,0,0,0,0,FakeAP
0,2,0,1,0,0,0,0,0,1,0,6,7,0,0,218,2,Normal
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,2,Deauth
0,0,8,0,0,0,0,0,0,0,0,1,9,0,0,0,0,FakeAP
0,2,0,1,0,0,0,0,0,0,1,0,18,9,0,0,117,2,SynFlooding
0,1,13,0,0,0,0,0,0,0,0,0,0,7,0,0,2,Normal
0,0,12,0,0,0,0,0,0,0,0,1,2,0,0,0,2,Deauth
```

Figura 2. Fragmento do Conjunto de Dados.

Depois de avaliar o tráfego na rede foi percebido que não existiu, durante o período de observação, ataques ou comportamentos anômalos que pudessem comprometer a segurança. Portanto, apenas a captura do tráfego normal não teria contribuição no desenvolvimento da pesquisa. Assim, tornou-se necessário realizar diversos ataques contra a rede e seus usuários. Foram escolhidos ataques que geralmente são empregados contra este tipo de rede. Evidentemente que toda esta atividade foi autorizada pelo administrador da rede.

Com finalidade de ampliar as possibilidades de avaliação de IDS, foram configurados cenários distintos de redes, com topologias e configurações diferentes. A partir de cada cenário, foi gerado um conjunto de dados. Estes cenários são descritos nas seções seguintes.

A. Cenário 1 – Criação do Conjunto de Dados com Criptografia WEP/WPA

É conhecido que WEP é um protocolo antigo e possui diversas falhas de segurança, porém ainda existem muitas redes que o utilizam. Assim, optou-se em executar um experimento o uso do WEP e permitir avaliar propostas de IDS empregadas nestas redes.

A topologia empregada no cenário 1 para a construção deste conjunto de dados é apresentada na Figura 3. Trata-se de uma simples topologia, porém seu uso é bastante comum em ambiente doméstico e em pequenas empresas.

Figura 3. Topologia de Rede Utilizada na Geração do Conjunto de Dados do Cenário 1.

Foi utilizado o software Aircrack [16] para geração de ataques ChopChop, deautenticação, fragmentação e duração, pela Estação Tipo 1. Enquanto que a Estação Tipo 2 foi utilizada para realizar a captura dos dados, com o uso do software Wireshark [17]. A Estação Tipo 3 foi utilizada para representar um usuário normal na rede, com aplicações que fazem uso dos protocolos HTTP e HTTPS.

O ataque ChopChop foi empregado inicialmente através de programas escrito em Linguagem C no ano de 2004. Este ataque pode descriptografar um quadro WEP, mesmo sem conhecer as chaves criptográficas, explorando propriedades das operações de "ou exclusivo" utilizadas pelo protocolo Rivest Cipher - RC4 e pelo algoritmo do Cyclic Redundancy Check - CRC32, utilizados para computar o Valor de Verificador de Integridade – ICV [18].

Os ataques de deautenticação ocorrem quando o atacante gera quadros falsos em broadcast, endereço "FF:FF:FF:FF:FF:FF", na rede. A estação que recebe este quadro automaticamente se desconectará da rede. Este processo é então repetido continuamente [18].

Os ataques de fragmentação utilizam técnicas de montagem e desmontagem de quadros na tentativa de descriptografar chaves utilizadas nos quadros transmitidos pela camada de enlace [15]. Finalmente, ataques de duração exploram vulnerabilidades do protocolo de acesso ao meio, o CSMA/CA, no momento em que a estação reserva um canal para comunicação por um período de tempo. Neste caso, o atacante injeta quadros na rede com valores de tempo elevado, para reserva do canal, assim, outras estações não podem utilizar a rede durante este período, até que o temporizador expire. O ataque é contínuo, com o envio de novos quadros de reserva do canal, antes que o anterior tenha expirado [18].

Neste cenário optou-se pelo emprego da captura baseada em espaço amostral, para permitir o uso do conjunto de dados mesmo em ambientes com pouco poder computacional, porém, ainda que o conjunto seja reduzido, existe representatividade com amostras de todos os tipos de tráfego [15]. A distribuição das amostras geradas neste cenário são apresentados na Tabela 1.

TABELA I. DISTRIBUIÇÃO DAS AMOSTRAS GERADAS NO 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**

Fonte: Adaptado de [15]

B. Cenário 2 – Criação do Conjunto de Dados com Criptografia WPA2

A configuração do Cenário 2 é baseada na criptografia com Wifi Protected Access Version 2- WPA2 [19]. O mecanismo de autenticação IEEE 802.1x [20], que permite a associação segura de clientes na rede, também foi empregado. Este é o cenário comumente utilizado em ambientes corporativos, e a topologia é apresentada na Figura 4. Este cenário apresenta maior nível de complexidade, quando comparado ao anterior.

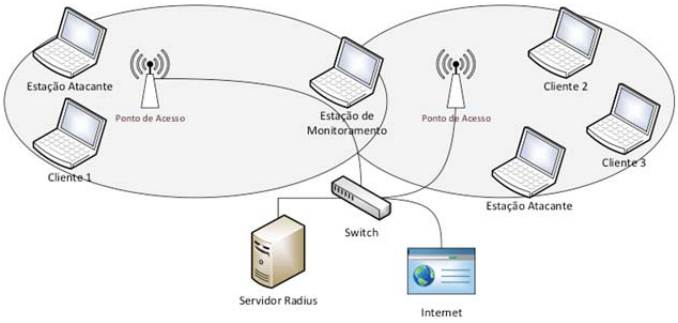

Figura 4. Topologia de Rede Utilizada na Geração do Conjunto de Dados do Cenário 2.

A rede possui várias estações sem fio, dois pontos de acesso (AP) e um servidor RADIUS que é utilizado para autenticação de usuários. Três estações (Cliente 1, Cliente 2 e Cliente 3) sem fio foram usadas para representar usuários da rede que geram tráfego normal, com aplicações web (HTTP e FTP). Uma estação atacante foi configurada para gerar ataques utilizando o software Aircrak [16], com vários tipos de ataques. Enquanto que uma estação de monitoramento foi configurada para realizar a captura de todo o tráfego na rede, através do software Wireshark [17].

Os ataques empregados neste cenários são comuns em redes sem fio: desautenticação, autenticação falsa, AP falso e inundação (*synflooding*). O primeiro ataque é exatamente o método empregado no cenário anterior. A autenticação falsa injeta quadros na rede, com o objetivo de incluir uma estação

que não é um cliente legítimo da rede, para capturar quadros que possuem Vetores de Inicialização. O ataque de AP Falso cria um ponto de acesso que não é legítimo na rede, enquanto que o ataque de inundação tem objetivo de gerar quadros em quantidade suficiente para paralisar equipamentos que não estão preparados para este tipo de carga.

A metodologia de organização dos dados coletados neste experimento segue a proposta de divisão de dados *holdout* [21], com a distribuição do espaço amostral dos registros numa proporção de 75% e 25%, nas bases de treinamento e testes respectivamente. A distribuição das amostras conforme sua classificação é apresentada na Tabela 2.

TABELA II. DISTRIBUIÇÃO DE AMOSTRAS NO CENÁRIO 2.

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

C. Cenário 3 – Criação do Conjunto de Dados com IEEE 802.11w

No cenário 3 foi empregado topologia semelhante ao cenário 2, com o uso de servidor de autenticação RADIUS e quadro APs. A interligação entre os pontos de acesso da rede sem fio foi realizada através de Sistema de Distribuição Sem Fio – WDS. A comunicação entre os equipamentos da rede foi realizada com o emprego do protocolo IEEE 802.11w. Durante uma semana foi capturado todo o tráfego da rede e organizado em um único conjunto de dados. A distribuição das amostras é apresentada na Tabela 3.

TABELA III. DISTRIBUIÇÃO DAS AMOSTRAS NO CENÁRIO 3.

Tipo	Número de Amostras
Normal	10.886.308
Desautenticação	323.975
Beacon Flood	545.480
RTS-Flood	3.198
EAPOL-Start	561.987
Total de Amostras	**12.320.948**

No passado, os quadros de gerenciamento não continham informações sensíveis e sua proteção não era essencial, o cenário tecnológico e de segurança era muito diferente da atualidade. Porém, com as novas implementações como fast handoff, mecanismos de descoberta na rede e esquemas de gerenciamento (IEEE 802.11r, 802.11k e 802.11v), novas e mais informações sensíveis sobre a rede começaram a ser transferidas nos quadros de gerenciamento. Assim, o IEEE apresentou a emenda 802.11w com objetivo de propiciar proteção a estes quadros. Deste modo, foi introduzido o conceito de quadros de Gerenciamento Robusto – RM. Estes quadros incluem mensagens de gerenciamento: *disassociation*, *deauthentication*, ou *action*. Foi ratificado padrões para atribuição de propriedades de chaves criptográficas com a Proteção de Quadro de Gerenciamento – MFP [22].

Então, no Cenário 3, foram empregados quatro tipos de ataques: Desautenticação, *Beacon Flood*, *RTS-Flood* e *EAPOL-Start*. Os dois primeiros tem alvos os quadros de gerenciamento, enquanto que o terceiro, além dos quadros de gerenciamento também ataca quadros de dados, e o último tipo de ataque visa os quadros de controle.

Os ataques de Desautenticação foram utilizados empregando o mesmo método do cenário anterior. Porém, neste caso, foram gerados sequência com 100 quadros falsos, em seguida, foram enviados mil quadros falsos, e no terceiro momento, uma sequência ininterrupta de quadros falsos de Desautenticação.

Os *beacons* são quadros enviados periodicamente pelos APs com informações sobre a rede. O seu emprego também possui a função de auxiliar sincronização na rede, geralmente são transmitidos a cada 100ms. Porém, no ataque de *Beacon Flood*, foi produzido número demasiado de quadros com objetivo de impossibilitar clientes de se associarem ao ponto de acesso verdadeiro da rede.

Foi empregado o software Metasploit [23] para desferir os ataques *RTS Flood* e *EAPOL-Start*. Os quadros Requisição para Enviar – RTS são enviados pelos equipamentos de rede sem fio quando existem dados para serem transmitidos, e assim fazer a reserva do canal para comunicação. Porém, com objetivo de causar danos na rede, os quadros RTS utilizados no ataques tiveram o campo duração alterado para um valor elevado, provocando a paralização da rede.

Os quadros EAPOL são empregados para transportar segmentos de rede oriundos do Protocolo Extensível de Autenticação – EAP sobre uma Rede Local – LAN, com objetivo de prover a comunicação entre um cliente (suplicante) e o ponto de acesso (autenticador) . Ataques de *EAPOL-Start* geram excessivas requisições de inicializações de sessões EAPOL a um ponto de acesso, caracterizando-se como um Ataque de Negação de Serviço – *DoS*, com objetivo de paralisar o equipamento.

IV. AVALIAÇÃO DO CONJUNTO DE DADOS

A avaliação dos conjuntos de dados foi realizada através do emprego de técnicas de classificação, habitualmente utilizadas em IDS. A comparação entre cada técnica foi efetivada através de medidas de erro, apuradas durante a fase de treinamento, e por meio da medida do percentual de classificação na avaliação, além da comparação destes indicadores com o coeficiente Kappa.

O coeficiente Kappa é uma métrica de concordância induzida, primeiramente usada entre observadores de psicologia [24]. Esta métrica mede o grau de aceitação ou de respostas concordantes entre diversos juízes. É empregado utilizando a proporção entre a concordância observada (Po) e a concordância devida ao acaso (Pa), e a forma de cálculo é apresentada na Equação 1.

$$k = \frac{Po - Pa}{1 - Pa} \tag{1}$$

O valor unitário indica que a classificação foi correta, enquanto que o valor do coeficiente nulo, indica que a classificação ocorreu ao mero acaso, portanto valores

próximos de um confirmam que foram empregados os melhores classificadores. Este coeficiente tem sido utilizado em propostas para implementação de IDS [25].

A avaliação dos conjuntos de dados foi executada com a implementação de Redes Bayesanas, Tabelas de Decisão, Algoritmos Baseados em Instâncias - IBk, J48, MLP e NaiveBayes. Estes classificadores foram escolhidos por serem comumente utilizados em IDS.

As Redes Bayesanas são gráficos direcionados acíclicos que permitem a representação de distribuição de probabilidades sobre um conjunto de variáveis aleatórias. Cada vértice representa uma variável aleatória e cada nó representa a correlação entre as variáveis [26]. Muitas propostas de IDS foram apresentadas com o emprego desta técnica [27].

A representação em formato de tabela para expressar um conjunto de condições necessárias para determinar a ocorrência de um conjunto de ações a serem executados define o funcionamento básico das Tabelas de Decisão [28]. Exemplos de IDS baseado em Tabelas de Decisão são encontrados em [29].

O algoritmo IBk é uma implementação do método de Agrupamento de Vizinhos - kNN, técnica utilizada para classificação e regressão, que consiste encontrar vizinhos mais próximos de uma data instância. No caso do IBk, utiliza-se os três vizinhos mais próximos do padrão de consulta. Esta é uma técnica relativamente simples, porém também tem sido utilizada em propostas de IDS [30].

O J48 é um simples algoritmo baseado em classificadores de árvores de decisão. Para classificar um novo item, primeiro é necessário criar uma árvore de decisão de acordo com valores de atributos obtidos a partir dos dados de treinamento. Esta técnica também é utilizada para calcular o ganho de informação de cada atributo e assim otimizar o mecanismo de classificação nos IDS [31].

O MLP é uma rede neural artificial que mapeia com conjunto de entradas para sua apropriada saída, consiste de várias camadas de nós em um gráfico direcionado. Seu emprego em IDS tem gerado diversas propostas de implementação [14].

Finalmente, NaiveBayes é um classificador probabilístico baseado na aplicação do teorema de Bayes com hipóteses de independência entre os preditores. Este algoritmo é relativamente fácil de ser implementado, sem parâmetros iterativos complexos, tornando-se útil para realizar o experimento proposto [32].

A avaliação dos classificadores, aplicados nos conjuntos de dados criados, foi realizada com o uso do software Weka [33]. Este software tem sido utilizado em testes e assim tornou-se bom candidato para exames de protótipos. Como um dos objetivos é aferir o conjunto de dados, não foi realizado nenhuma customização de parâmetros dos classificadores, e a execução do software foi efetuada com todos os valores *default*.

O conjunto de dados do Cenário 3 é muito volumoso, contém 12.320.948 amostras, assim as avaliações requerem alto poder computacional. Portanto foi utilizado 5% deste conjunto de dados, obtidos através do método de amostragem *Reservoir* [34], a distribuição do subconjunto do Cenário 3 foi atualizada conforme apresentação na Tabela 4.

TABELA IV. DISTRIBUIÇÃO DAS AMOSTRAS DO SUBCONJUNTO DO CENÁRIO 3.

Tipo	Número de Amostras
Normal	544.186
Desautenticação	16.217
Beacon Flood	27.424
RTS-Flood	149
EAPOL-Start	28.071
Total de Amostras	**616.047**

O emprego dos classificadores, gerou resultados que são apresentados nas Tabelas 5, 6 e 7, para os conjunto de dados oriundos dos três cenários, respectivamente.

TABELA V. RESULTADO DA CLASSIFICAÇÃO PARA O CENÁRIO 1.

Algoritmo	Percentual de Instâncias Classificadas Corretamente	Percentual de Instâncias Classificadas Incorretamente	Coeficiente Kappa
Redes Bayesanas	82,0610	17,9390	0,6485
Tabelas de Decisão	76,3415	23,6585	0,4955
IBk	80,7317	19,2683	0,6390
J48	78,5610	21,4390	0,5906
MLP	81,6463	18,3537	0,6497
NaiveBayes	77,3780	22,6220	0,5860

Os resultados obtidos, com o emprego dos classificadores, apresentam valores com percentual aceitável de instâncias classificadas corretamente. Tais resultados são relativamente inferiores quando comparados com abordagens que empregam estes mesmos algoritmos. Este panorama é esperado, afinal não foi realizado nenhuma customização dos métodos de classificação ou melhoria, pois este procedimento não faz parte do escopo da pesquisa.

TABELA VI. RESULTADO DA CLASSIFICAÇÃO PARA O CENÁRIO 2.

Algoritmo	Percentual de Instâncias Classificadas Corretamente	Percentual de Instâncias Classificadas Incorretamente	Coeficiente Kappa
Redes Bayesanas	85,8133	14,1867	0,7819
Tabelas de Decisão	92,8533	7,1467	0,8778
IBk	92,9067	7,0933	0,8787
J48	92,8533	7,1467	0,8778
MLP	92,4267	7,5733	0,8710
NaiveBayes	66,3333	33,6667	0,5094

Um desafio relacionado à segurança em redes é a comparação apropriada das propostas apresentadas para Sistemas de Detecção de Intrusos [9]. Boa parte dos estudos fazem uso de conjuntos de dados gerados para competições de descobrimento de conhecimento e também de dados coletados a partir das redes utilizadas pelos pesquisadores [4]. Porém, a maioria dos conjuntos foi criado para redes cabeadas.

Com a lacuna existente em função da deficiência de conjuntos de dados que represente o funcionamento de uma rede sem fio, foi desenvolvido esta pesquisa. A criação de

cenários distintos, permite realizar a avaliação de IDS em todos os casos. Os três cenários foram produzidos utilizando técnicas diferentes, para ampliar o universo dos dados.

TABELA VII. RESULTADO DA CLASSIFICAÇÃO PARA O CENÁRIO 3.

Algoritmo	Percentual de Instâncias Classificadas Corretamente	Percentual de Instâncias Classificadas Incorretamente	Coeficiente Kappa
Redes Bayesanas	76,0888	23,9113	0,4227
Tabelas de Decisão	98,0445	1,9555	0,9082
IBk	98,0721	1,9279	0,9097
J48	98,0638	1,9362	0,9093
MLP	93,3481	6,6519	0,6922
NaiveBayes	71,2098	28,7902	0,3473

O emprego de técnicas comuns de classificação, demonstrou que bons resultados foram obtidos. Conforme é possível verificar através dos valores apresentados nas Tabelas 5, 6 e 7. Com o emprego do coeficiente Kappa, o melhor resultado foi conseguido através de Redes Neurais para o conjunto de dados do Cenário 1, algoritmo IBk nos Cenário 2 e no Cenário 3.

No Cenário 1, as Redes Bayesanas apresentaram o melhor percentual de Instâncias Classificadas Corretamente, sendo 82,0610% enquanto que as Redes Neurais detectaram 81,6463%, percebe-se que a diferença entre os dois algoritmos é insignificante, assim como ocorreu com o coeficiente Kappa.

Nos cenários 2 e 3 isso não ocorreu, o coeficiente o índice de instâncias classificadas corretamente estão de acordo com o coeficiente Kappa. É importante destacar que não houve nenhuma customização dos parâmetros utilizados na implementação destes classificadores, assim como também não houve nenhum procedimento de otimização

V. CONCLUSÕES E TRABALHOS FUTUROS

Foi criado o conjunto de dados a partir dos tráfego capturado de uma rede sem fio. Este conjunto de dados está organizado com três cenários distintos, com topologia simples, no caso do Cenário 1 e topologia complexa como apresentado no Cenário 2, por fim, o Cenário 3 criado com a implementação do protocolo IEEE 802.11w.

O coeficiente Kappa, como métrica de medição de eficiência, demonstrou bom resultado. Isto pode ser constatado quando os valores do coeficiente Kappa são comparados com os valores das instâncias classificadas corretamente.

Foram realizadas avaliações utilizando o conjunto de dados, em todos os cenários implementados. O objetivo das avaliações foi verificar qual seria o comportamento de alguns IDS, quando empregados no conjunto de dados. Para isso, foram selecionados algoritmos de reconhecimento de padrões, geralmente empregados em sistemas de detecção de intrusão.

Os resultados obtidos demonstraram a viabilidade do emprego do conjunto de dados. Com os uso de vários cenários, este conjunto de dados pode ser utilizado para avaliação de propostas de IDS. Tal avalição torna-se mais justa, pois geralmente os autores de propostas de IDS costumam fazer testes em suas redes, por conseguinte, o confronto com outras abordagens torna-se muito difícil. Além disso, outra importante contribuição desta pesquisa é a base rotulada, em que cada linha do arquivo possui uma etiqueta que indica o tipo de conexão que a linha representa.

O cenário 3 foi gerado a partir do monitoramento de 7 dias, assim, o conjunto de dados ficou enorme. É claro que o processamento deste conjunto requer mais poder computacional do que os outros cenários, porém, esta quantidade de dados concebe o comportamento de usuários durante todo um ciclo, além de conter todos os ataques que foram desferidos contra a rede. Outro diferencial deste cenário refere-se a camada extra de segurança disponibilizada pelo uso do IEEE 802.11w, que provê proteção a alguns quadros de controle na camada de enlace. Esta diversidade do cenário propicia um ótimo ambiente para avaliação das diferentes abordagens de IDS para redes sem fio.

Como continuação desta pesquisa sugere-se construir outros conjuntos de dados oriundos de outros tipos de redes sem fio, a exemplo das redes baseadas em IEEE 802.16 (redes metropolitanas), IEEE 802.15 (redes pessoais) especialmente as redes baseadas em IEEE 802.15.4 (redes de sensores). Além disso, deve-se continuar a pesquisa sobre a possibilidade do emprego de Autômato Celulares nas implementações de IDS, afinal, estes mecanismos requerem pouco poder computacional para serem executados, portanto, poderão representar grande avanço na área de segurança da informação.

REFERÊNCIAS

[1] A. Patcha and J.-M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends,” *Comput. Networks*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.

[2] S. Mousionis, A. Vakaloudis, and C. Hilas, “A Study on the Security, the Performance an the Penetration on Wi-Fi Networks in a Greek Urban Area,” in *5th IFIP WG 11.2 International Workshop WISTP*, 2011, vol. 6633, pp. 381–389.

[3] E. W. T. Ferreira, G. A. Carrijo, R. de Oliveira, and N. V. de S. Araujo, “Intrusion Detection System with Wavelet and Neural Artifical Network Approach for Networks Computers,” *IEEE Lat. Am. Trans.*, vol. 9, no. 5, pp. 832–837, Sep. 2011.

[4] M. Tavallaee, N. Stakhanova, and A. A. Ghorbani, “Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods,” *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 40, no. 5, pp. 516–524, Sep. 2010.

[5] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, “A comparison of mechanisms for improving TCP performance over wireless links,” *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 756–769, 1997.

[6] J. Baliga, R. Ayre, K. Hinton, and R. Tucker, “Energy consumption in wired and wireless access networks,” *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 70–77, Jun. 2011.

[7] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, “A performance comparison of multi-hop wireless ad hoc network routing protocols,” in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking - MobiCom ’98*, 1998, pp. 85–97.

[8] F. Hernandez-Campos and M. Papadopouli, “Assessing The Real Impact of 802.11 WLANs: A Large-Scale Comparison of Wired and Wireless Traffic,” in *14th IEEE Workshop on Local & Metropolitan Area Networks*, 2005, pp. 1–6.

[9] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, “Toward developing a systematic approach to generate benchmark datasets for intrusion detection,” *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, May 2012.

[10] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, "Intrusion detection by machine learning: A review," *Expert Syst. Appl.*, vol. 36, no. 10, pp. 11994–12000, Dec. 2009.

[11] G. Singh, F. Masseglia, C. Fiot, A. Marascu, P. Poncelet, T. Theeramunkong, B. Kijsirikul, N. Cercone, and T.-B. Ho, "Data Mining for Intrusion Detection: From Outliers to True Intrusions," in *13th Pacific-Asia Conference Advances in Knowledge Discovery and Data Mining*, 2009, vol. 5476, pp. 891–898.

[12] H. F. Eid, M. A. Salama, A. E. Hassanien, T. Kim, H. Adeli, W. Fang, J. G. Villalba, K. P. Arnett, and M. K. Khan, *Security Technology*, vol. 259. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 195–203.

[13] S. Kandeeban and R. Rajesh, "A Genetic Algorithm Based elucidation for improving Intrusion Detection through condensed feature set by KDD 99 data set," *Inf. Knowl. Manag.*, vol. 1, no. 1, pp. 1–9, 2001.

[14] S. H. Zhong, H. J. Huang, and A. Bin Chen, "An Effective Intrusion Detection Model Based on Random Forest and Neural Networks," *Adv. Mater. Res.*, vol. 267, pp. 308–313, Jun. 2011.

[15] K. El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 8, pp. 1143–1149, Aug. 2010.

[16] Aircrack, "Aircrack-ng," 2014. [Online]. Available: http://www.aircrack-ng.org/. [Accessed: 19-Feb-2014].

[17] G. Combs, "Wireshark · Go Deep.," 1998. [Online]. Available: http://www.wireshark.org/. [Accessed: 19-Feb-2014].

[18] M. Guennoun, A. Lbekkouri, A. Benamrane, M. Ben-Tahir, and K. El-Khatib, "Wireless networks security: Proof of chopchop attack," in *International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2008, pp. 1–4.

[19] A. H. Lashkari, M. M. S. Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 48–52.

[20] K. Y. Park, Y. S. Kim, and J. Kim, "Security enhanced IEEE 802.1x authentication method for WLAN mobile router," in *14th International Conference on Advanced Communication Technology (ICACT)*, 2012, pp. 549–553.

[21] P. Smith, "Autocorrelation in logistic regression modelling of species' distributions," *Glob. Ecol. Biogeogr. Lett.*, vol. 4, no. 2, pp. 47–61, 1994.

[22] M. S. Ahmad and S. Tadakamadla, "Security Evaluation of IEEE 802.11w Specification," in *ACM conference on Wireless network security - WiSec '11*, 2011, pp. 53–58.

[23] Rapid7 LLC, "Metasploit: Penetration Testing Software," 2014. [Online]. Available: http://www.metasploit.com. [Accessed: 04-Oct-2014].

[24] J. Cohen, "A Coefficient of Agreement for Nominal Scales," *Educ. Psychol. Meas.*, vol. 20, no. 1, pp. 37–46, Apr. 1960.

[25] N. V. de S. Araújo, A. A. Shinoda, R. de Oliveira, E. W. T. Ferreira, and V. E. do Nascimento, "Kappa-ARTMAP Fuzzy: uma metodologia para detecção de intrusos com seleção de atributos em redes de computadores," in *31º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 2013, pp. 119–130.

[26] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," *Mach. Learn.*, vol. 29, no. 2–3, pp. 131–163, 1997.

[27] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1–2, pp. 18–28, Feb. 2009.

[28] J. Huysmans, K. Dejaeger, C. Mues, J. Vanthienen, and B. Baesens, "An empirical evaluation of the comprehensibility of decision table, tree and rule based predictive models," *Decis. Support Syst.*, vol. 51, no. 1, pp. 141–154, Apr. 2011.

[29] S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 129–141, Jan. 2012.

[30] H. Om and A. Kundu, "A hybrid system for reducing the false alarm rate of anomaly intrusion detection system," in *1st International Conference on Recent Advances in Information Technology (RAIT)*, 2012, pp. 131–136.

[31] M. K. Nagle and S. K. Chaturvedi, "Feature Extraction Based Classification Technique for Intrusion Detection System," *Int. J. Eng. Res. Dev.*, vol. 8, no. 2, pp. 23–38, 2013.

[32] Z.-G. Chen and S.-R. Kim, "Combining principal component analysis, decision tree and naïve Bayesian algorithm for adaptive intrusion detection," in *Proceedings of the 2013 Research in Adaptive and Convergent Systems on - RACS '13*, 2013, pp. 312–316.

[33] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software," *ACM SIGKDD Explor. Newsl.*, vol. 11, no. 1, p. 10, Nov. 2009.

[34] J. S. Vitter, "Random sampling with a reservoir," *ACM Trans. Math. Softw.*, vol. 11, no. 1, pp. 37–57, Mar. 1985.

Ed´ Wilson Tavares Ferreira é graduado em Ciência da Computação pela Universidade Federal de Mato Grosso (UFMT), Cuiabá, Mato Grosso, Brasil, em 1997. Obteve o título de mestre em Engenharia Elétrica pela Universidade Federal de Uberlândia (UFU), Uberlândia, Minas Gerias, Brasil, em 2002 e de Doutor, em Engenharia Elétrica pela Universidade Federal de Uberlândia (UFU), Uberlândia, Minas Gerias, Brasil, em 2009. Atualmente está realizando estágio de pós-doutorado na Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP) e é professor do Instituto Federal de Mato Grosso (IFMT) e suas pesquisas se concentram na área de Segurança da Informação e Redes Sem Fio, tópico no qual tem escrito e revisado artigos.

Ailton Akira Shinoda possui graduação em Engenharia Elétrica pela Universidade Estadual de Campinas UNICAMP (1986), mestrado em Engenharia Elétrica pela Universidade Estadual de Campinas UNICAMP (1993), doutorado em Engenharia Elétrica pela Universidade Estadual de Campinas UNICAMP (1996) e pós-doutorado pela Yokohama National University (1998) . Atualmente é Professor Adjunto da Universidade Estadual Paulista "Júlio de Mesquita Filho" UNESP. Tem experiência na área de Engenharia Elétrica, com ênfase em Telecomunicações. Atuando principalmente nos seguintes temas: Sistemas de Comunicação Móvel, rede sem fio, Compatibilidade Eletromagnética (EMC), FPGA, PCB.