Regras *Fuzzy* para Análise de Segurança em Redes Wi-Fi

Eduardo Araujo, Nelson Tenório Jr.
CESUMAR – Centro de Ensino Superior de Maringá
overctba@gmail.com, nelson.tenorio@cesumar.br

***Resumo*—Com a popularização das redes sem fio, emerge o problema de segurança de acessos e tentativas de invasões nesse tipo de redes. Todavia a mão-de-obra para este tipo de serviço não é tão acessível a todos, principalmente em se tratando de usuários domésticos ou empresas de pequeno porte, que, muitas vezes, acabam simplesmente adquirindo o equipamento e realizando suas configurações por tutoriais. Deixando assim o investimento na segurança da rede Wi-Fi em segundo plano e, ainda, com grandes chances de cair no esquecimento. Assim, esta pesquisa apresenta e discute regras fuzzy para a análise da segurança de enlaces sem fio em busca de prováveis problemas de vulnerabilidades nas redes Wi-Fi residenciais e empresariais.**

I. Introdução

Há alguns anos apenas um grupo seleto de pessoas possuía acesso a computadores, os quais gozavam de grandes proporções e processavam as informações de forma centralizada. Acabaram substituídos com o surgimento de um conceito inovador de processamento, o qual consistia na possibilidade de que diversos equipamentos computacionais de processamento operando separadamente porém interconectados por um mesmo tipo de tecnologia a realizar a mesma atividade; modelo este que gerou um acréscimo significativo na demanda por computadores em todas as áreas de negócio e por sua vez agregou interesse e a necessidade das redes de computadores [1].

Quase na época do surgimento dos primeiros computadores portáteis, seus usuários gostariam de poder chegar em seus recintos de trabalho e poder operar com a rede sem utilizar a conexão por cabos, sonhavam com a mobilidade, surgiu quase que prontamente a comercialização de transmissores e receptores de radiofrequência de ondas curtas com o intuito de suprir esta necessidade, porém em seu primórdio a falta de compatibilidade entre os equipamentos de marcas distintas era elevado, gerando certo transtorno, neste momento, em meados da década de noventa, a indústria solicitou ao IEEE (Institute of Electrical and Electronics Engineers) para criar uma padronização para este segmento, cujo projeto recebeu o nome de 118802.11 e que se popularizou como Wi-Fi, mas sua nomenclatura correta é 802.11 [1].

Ao se montar uma rede Wi-Fi tanto residencial quanto empresarial, deve-se ter em mente o planejamento da sua segurança. Se desconsiderado esta última, os impactos na infraestrutura da rede Wi-Fi podem ser desastrosos, pois os dados, o desempenho e até o acesso, ficarão vulneráveis o suficiente para que pessoas não autorizadas possam usufruir dos serviços bem como acessarem e se apossarem dos dados dos usuários.

Na tentativa de aprimorar a segurança das redes Wi-Fi, profissionais da área e especialistas necessitam de ferramentas que viabilizem o reconhecimento ágil da vulnerabilidade para tratá-la com maior eficiência, de modo que os custos para esta implantação e manutenção sejam relativamente elevados, principalmente para as empresas que não possuem a TI como atividade fim. Desta forma, esta pesquisa pretende apresentar um modelo tomando por base a lógica *fuzzy* com o intuito de auxiliar futuramente o profissional de TI possam aprimorar na identificação do problema de segurança, de modo a contribuir para a redução de esforço já que o software torna-se um elemento auxiliar nesta tarefa.

Este artigo está organizado como se segue: na seção II é apresentado o conceito de segurança de redes; a seção III discute os conceitos dos protocolos e algoritmos de criptografia na segurança de redes Wi-Fi; na seção IV são apresentados os conceitos de lógica fuzzy; a seção V apresenta os trabalhos correlatos e um comparativo com esta proposta; a seção VI apresenta a proposta de regras fuzzy para identificar a segurança em redes Wi-Fi; e, por fim, a seção VI apresenta as considerações finais e uma discussão sobre os próximos passos da pesquisa seguida das referências bibliográficas utilizadas.

II. Segurança de Redes

O que entende-se por uma rede segura é tratado na literatura este é um conceito estimula seus utilizadores, mas o mesmo é pouco trivial, uma vez que não há um modo de se classificar uma rede simplesmente como muito ou pouco segura, considerando que a terminologia não é absoluta, onde cada organização provida de seus gestores juntamente com seus administradores de redes detém poderes suficientes para elaborar e definir os níveis de acessos que serão ou não concedidos a seus usuários. Analisando por este viés pode-se afirmar que para alguns a abstração de uma rede segura seria um ambiente em que não ocorra a captura ou leitura de dados por pessoas ou equipamentos desautorizados, já para outros, algo mais complexo como não permitir acesso, modificação destes e ou serviços sensíveis do negócio por meio de acessos restritos, com isso determinando de certo modo a segurança em suas estruturas [2].

O primeiro passo para se obter um ambiente seguro seria definir uma política de segurança de forma clara e inequívoca para os itens sensíveis do negócio e que devam ser deste modo objetos com necessidade de proteção. Mas concretizar tal tarefa é algo relativamente complexo, uma vez que envolve um universo muito mais amplo do que simplesmente contemplar projetos de segurança física e lógica para os equipamentos, pois envolve um fator extremamente difícil de se obter controle, neste caso o comportamento humano e outras facilidades que a rede pode prover, tomando um simples

exemplo, uma rede sem fio que pode ser detectada fora do prédio do escritório; de tal forma a ter de pesar no binômio segurança, complexidade, para que esta não seja tão rígida que dificulte a fluidez do cotidiano da empresa, nem seja branda demais a ponto de qualquer colaborador tenha acesso privilegiado sem permissão, com isso a tarefa da definição da política de segurança não só será ineficaz, como pouco provável se os indivíduos comprometidos com esta atividade desconheçam ou tampouco sejam capazes de valorar o que se pretende proteger. Assim, uma política de segurança de rede pode ser complexo, pois exige a relação da segurança de redes de computadores ao comportamento humano, avaliando o valor das informações [3].

Assim, existem alguns requisitos da segurança de redes, como prezar pela integridade dos dados contemplando proteção contra mudança nestes, a disponibilidade das informações objetivando a proteção contra a interrupção de serviços, a confidencialidade visando proteção contra acesso não autorizado dos dados que são transmitidos por esta e a privacidade para que os remetentes consigam manter-se anônimos.

III. Protocolos e Criptografias para redes Wi-Fi

Para abordar segurança em redes sem fio, deve-se tratar seus protocolos e algoritmos de criptografia, deste modo o protocolo WEP (*Wired Equivalent Privacy*) que foi o primeiro desenvolvido para esta tecnologia, uma vez que esta era recente no mercado, por membros do IEEE (*Institute of Electrical and Electronics Engineers*) com o intuito de prover uma segurança equivalente à das redes cabeadas aos enlaces Wi-Fi, de modo a conferir a esta confiabilidade, acrescentando um método de autenticação de um membro autorizado, mantendo também a integridade das informações trafegadas, para implementar este protocolo foi empregado um algoritmo de criptografia simétrica de fluxo e um verificador de integridade de, onde o primeiro é denominado RC4 e o segundo por CRC32, sendo que o RC4 é considerado de alta performance pois opera sobre demanda.

Este algoritmo mencionado anteriormente utiliza uma chave fixa de 40 bits com uma sequência variável de 24 bits cujo o padrão trata por vetor de inicialização ou IV, onde este cria esta sequência aleatória e anexa os dados cifrados por um método conhecido por XOR, conforme apresenta [4]. Após esta etapa os dados criptografados são enviados juntamente com o IV, onde uma vez que o receptor já possui esta chave o mesmo realiza o processo inverso para decriptar a mensagem recebida.

Devido ao perecimento ocorrido pelas falhas apresentadas neste protocolo, surgiu a necessidade de um novo protocolo que resolvesse tais falhas. Então, a Wi-Fi *Alliance* com a missão de certificar os produtos baseados no padrão IEEE 802.11, quanto à interoperabilidade, juntamente com o IEEE desenvolveram o protocolo WPA (Wi-Fi *Protected Access*), um protocolo intermediário até a conclusão do projeto 802.11i [5]. Este protocolo trouxe consigo a essência do seu antecessor como: o bom desempenho; o consumo reduzido de recursos computacionais; e a compatibilidade com o hardware. Além disso, o protocolo tinha como uma novidade o TKIP (*Temporal Key Integrity Protocol*), que gera uma nova chave a cada 10KB de dados transmitidos e que opera simultaneamente com o RC4 fazendo um algoritmo de *hash* [6][7].

Mesmo com os aprimoramentos do WPA, algumas falhas persistiam, contudo foi elaborado um novo protocolo o WPA2 ou IEEE 802.11i que é a referência atual para redes sem fio, este agregou mais segurança com a adição do cifrador AES (*Advanced Encryption Standard*) que juntamente com o TKIP fornece chaves de 128 a 256 bits, ou seja, uma criptografia bem elaborada, mas para tal impactou no desempenho e acabou com a compatibilidade, pois fez-se necessário a aquisição de novo hardware para utilizar este padrão, o que dificultou sua aceitação em um primeiro momento [5].

IV. Lógica *Fuzzy*

O termo *fuzzy* na língua inglesa pode assumir diferentes sentidos, porém entre os mais aplicados são algo vago ou incerto. Na literatura brasileira é comum ver como lógica nebulosa e vem viabilizar a quantificação de situações reais com parâmetros imprecisos na proposição.

Com a lógica *fuzzy* a representação do conhecimento em detrimento da precisão em face da complexidade é fazendo uso de variáveis linguísticas [8][9].

Para tanto são utilizadas regras de produção *fuzzy*, variáveis linguísticas, funções de pertinência, operações e modelos de inferência *fuzzy*.

A teoria de conjuntos da lógica difusa pode ser vista como uma extensão da teoria clássica, que foi concebida para tratar graus de pertinência intermediários: a total representada por 1 e a não-pertinência representada por 0.

A formação das regras de produção *fuzzy*, em geral, é composta por duas partes principais, antecedente e consequente, quando são escritas no formato *if* (antecedente) *then* (consequente). O antecedente é composto por um conjunto de condições que, se satisfeitas, determinam o processamento do consequente termo da regra por um mecanismo denominado de inferência *fuzzy*.

O processo de elaboração das regras deve empregar variáveis linguísticas para representar a imprecisão dos fatos, em linguagem humana, na sua proposição.

Para efetuar operações na lógica *fuzzy* não podem ser empregadas as operações booleanas, pois não contemplariam as incertezas como: mais poderoso e menos poderoso. Assim, foram definidas operações distintas para estes cálculos fazendo uso dos conectivos *AND*, *OR* e *NOT* como demonstra a Tabela I.

Tabela I
OPERADORES FUZZY

Operador	Operação
AND	$\mu_{A \wedge B} = min\{\mu A, \mu B\}$
OR	$\mu_{A \vee B} = max\{\mu A, \mu B\}$
NOT	$\mu_{\sim A} = 1 - \mu_A$

Em um modelo de inferência, apresentado na Figura 1, faz-se necessária uma entrada com um valor escalar que

passa por uma máquina de inferência que, por sua vez, emprega um banco de regras para realizar a conversão deste valor em fuzzy. Esse processo é conhecido como fuzzyficação. Então seu resultado sofre o processo de defuzzyficação, quando há a conversão de fuzzy para escalar novamente.

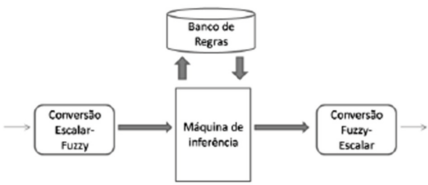

Figura 1. Modelo de inferência fuzzy.

Para se executar a defuzzyficação existem métodos que tomam por fundamento o cálculo de área para conversão, como o modo de Centro Máximo (CoM), Centro de Gravidade (CoG) e Média do Máximo (MoM), sendo que destes elencados o mais utilizado é o segundo, onde para empregar este "cortam-se as funções de agregação no grau do termo respectivo, e as áreas sob o resultado do corte são então sobrepostas e o cálculo do centro desta área aponta para o valor "defuzzyficado".[10]

V. Trabalhos Relacionados

O trabalho de [VIANA, CORREIA, PIRMEZ] apresenta uma arquitetura que visa uma solução para o problema de IDS convencional, empregando um identificador de dispositivos, que se baseia na assinatura de transmissão do dispositivo. Igualmente, utiliza um analisador de mobilidade buscando a integração com os processos de autenticação baseados em uma análise cinemática de mobilidade dos dispositivos e um componente dotado de inteligência computacional quando, neste caso a lógica *fuzzy* é a responsável por correlacionar os reportes dos outros dois, de modo que se comporte como elo de integração da solução, contudo de maneira a ampliar a segurança sem impactar na qualidade de serviço quanto na mobilidade.[11]

Um outro trabalho, de [LAGES, DELICATO, PIRMEZ], apresenta um sistema de reputação *fuzzy* para segurança orientada a serviços em redes de banda larga sem fio. Nele os autores propõem aumentar o nível de segurança das redes sem fio metropolitanas empregando um cálculo de reputação, que neste contexto é a confiabilidade da utilização da rede por parte dos usuários avaliando se o usuário oferece riscos aos serviços utilizados. A lógica *fuzzy* calcula a reputação recebida pelo usuário nos distintos e serviços utilizados nesta rede, agilizando o cálculo em um curto espaço de tempo [12].

A Tabela II apresenta um comparativo de propostas de outros autores que utilizam lógica *fuzzy* para determinar a segurança de uma rede sem fio. Os parâmetros utilizados para comparação foram determinados com estudos bibliográfico dos parâmetros preliminares utilizados por especialistas da área de segurança em redes sem fio. Assim, se destacaram os seguintes parâmetros de comparação: (C) Criptografia, (P) Protocolo, (A) Autenticação e (PR) Padrão da Rede.

Tabela II
COMPARAÇÃO TRABALHOS CORRELATOS

Propostas	**(C)**	**(P)**	**(A)**	**(PR)**
EWIDS [11]	Não	Não	Sim	802.16
Reputação [12]	Não	Não	Não	802.16
Fuzzy Wi-Fi	Sim	Sim	Sim	802.11

VI. Regras *Fuzzy* para a Segurança de Redes Wi-fi

Para definir o que vem a ser uma rede Wi-Fi segura, foram adotadas cinco variáveis linguísticas: ruim, regular, boa, ótima e excelente. Essas variáveis abstraem os níveis de uma rede Wi-Fi. Também foram escolhidos e definidos três os parâmetros para a aplicação das regras de produção *fuzzy*, sendo eles: o protocolo, a criptografia e a autenticação. As definições, tanto das variáveis linguísticas quanto das regras fuzzy, foram fundamentadas com base no entendimento de estudos bibliográficos preliminares dos parâmetros mais empregados por profissionais da área de segurança de redes e, ainda, com base na evolução dos padrões e algoritmos de criptografia destes enlaces.

Sendo assim, as regras *fuzzy* obtidas foram as seguintes:

If (P = WEP) *AND* (C = RC4) *AND* (A = NÃO), *then* segurança = **ruim**;

If (P = WPA) *AND* (C = TKIP) *AND* (A = NÃO), *then* segurança = **regular**;

If (P = WPA) *AND* (C = TKIP) *AND* (A = SIM), *then* segurança = boa;

If (P = WPA) *AND* (C = CMMP) *AND* (A = NÃO), *then* segurança = **regular**;

If (P = WPA) *AND* (C = CMMP) *AND* (A = SIM), *then* segurança = **boa**;

If (P = WPA2) *AND* (C = TKIP) *AND* (A = NÃO), *then* segurança = **regular**;

If (P = WPA2) *AND* (C = TKIP) *AND* (A = SIM), *then* segurança = **boa**;

If (P = WPA2) *AND* (C = CMMP) *AND* (A = NÃO), *then* segurança = **ótima**;

If (P = WPA2) *AND* (C = CMMP) *AND* (A = SIM), *then* segurança = **excelente**.

As regras acima descritas estão em conformidade com o padrão de "*if* <antecedente> *then* <consequente>" utilizando o operador *fuzzy* AND, juntamente com a definição de seus parâmetros, onde o parâmetro do "Protocolo" é representado pela letra P, o parâmetro "Criptografia" é representado pela letra C e, por fim, o parâmetro "Autenticação" é representado pela letra A. Seus conjuntos universos são representados por P={WEP,WPA,WPA2}, C={RC4, TKIP, CMMP} e A={SIM,NÃO}, respectivamente. A Tabela II apresenta a atribuição pesos para cada item destes conjuntos com base na sua complexidade. Assim, no que diz respeito ao Protocolo, quanto maior é o valor do seu peso, maior será a complexidade necessária para quebrar sua chave. No que diz respeito à Criptografia, quanto maior o peso mais

eficiente é considerado o seu algoritmo de "cifragem". Enfim, no caso da autenticação se ela não existe o peso é 1 e se existe o peso é 2.

Tabela III
PESOS DOS PARÂMETROS

Pesos	Protocolo	Criptografia	Autenticação
1	WEP	RC4	NÃO
2	WPA	TKIP	SIM
3	WPA2	CMMP	-

VII. Considerações Finais

Para que uma rede Wi-Fi residencial ou empresarial tenha níveis aceitáveis de segurança faz-se necessária a contratação de serviços especializados. Muitas vezes estes serviços possuem um alto custo e envolvem um grande esforço visto a quantidade de variáveis envolvidas e o custo do profissional que executa a tarefa. A lógica *fuzzy* possui dezenas de aplicações diferentes em diversas áreas do conhecimento e utiliza uma linguística similar à linguagem humana, facilitando a compreensão do que vem a ser, por exemplo, algo bom ou ruim. Em redes Wi-Fi a simples mudança de uma criptografia ou de uma autenticação pode até deixá-la menos segura, mas não ao ponto de transformar o nível de segurança de ótimo para ruim. Para definir esse ponto de incerteza e auxiliar os profissionais da área a definirem o que vem a ser uma rede Wi-Fi segura e, ainda, tentar reduzir o custo e esforço de profissionais que lidam com a segurança de uma rede, essa pesquisa torna-se relevante.

Em um primeiro momento identificou-se as principais variáveis linguísticas na tentativa de definir os níveis de segurança de redes Wi-Fi possibilitando assim a montagem das regras *fuzzy*. Com tais regras definidas abrem-se as portas para a evolução da pesquisa. Sendo assim, o passo que está sendo executado é uma atividade a campo.

Nessa atividade está sendo realizada uma varredura no centro de uma cidade no interior do Paraná, para identificar as redes Wi-Fi utilizando um *smartphone* com sistema operacional *Android* em sua versão 2.2. Em nenhum momento pretende-se invadir ou causar qualquer tipo de dano nessas redes.

Com os dados da varredura em levantados, pretende-se alimentar um banco de dados livre para a estruturação e de uma base de experimentos. Os experimentos serão *in-vitro* e regidos por um protocolo previamente elaborado e devidamente documentado. Será utilizada a linguagem Java com classes próprias para trabalhar com lógica *fuzzy*. Quando se pretende implementar as regras apresentadas neste trabalho e criar o modelo de inferência para processamento desses dados e verificação dos níveis de segurança dessas redes. Em paralelo será feita uma revisão sistemática para levantar trabalhos correlatos na área. Até o momento foi realizado um levantamento bibliográfico e nenhum trabalho correlato foi encontrado.

A análise dos resultados dos experimentos será realizada pela comparação entre o conhecimento de um profissional da área com o nível de segurança sugerido pelo modelo de inferência, resultado esse da defuzzyficação. Para tal será utilizada uma planilha de cálculo com o pacote estatístico.

Ao final espera-se que esta pesquisa sirva de fonte para o andamento de outros trabalhos na área de segurança de redes Wi-Fi, aprimorando deste modo a eficácia na provável identificação falhas na segurança e apontando estas ao profissional de redes, resultando em uma resposta mais ágil ao problema.

Referências

[1] TANENBAUM, Andrew S. 2003. Redes de computadores. [trad.] Vanderberg D. de Souza. 4ª edição. Rio de Janeiro : Elsevier, 2003. 10ª Reimpressão. ISBN 85-352-1185-3.

[2] DIMARZIO, J. F.; SOUZA, Vandenberg D. de. . Projeto e arquitetura de redes. Rio de Janeiro: Elsevier, 2001. - cap. 4.

[3] COMER, Douglas E. 2007. Redes de computadores e internet. [trad.] Álvaro Strube de Lima. 4ª edição. Porto Alegre : Bookman, 2007. ISBN 85-60031-36-7. pp. 547-548.

[4] CORRÊA JR., Marcos A. C. Evolução da Segurança em Redes Sem Fio. UFPE – Universidade Federal de Pernambuco. Disponível em: <http://www.cin.ufpe.br/~tg/2008-1/maccj.pdf> . Acesso em: 17/08/2011.

[5] . Belo Horizonte, Minas Gerais, Brasil. Acessado em: 10 de Agosto de 2002. AGUIAR, Paulo A. Freire. Segurança em Redes Wi-Fi, Montes Claros, 2005 In: Unimontes. Disponível em : < http://www.ccet.unimontes.br/arquivos/monografias/73.pdf>. p. 56 Acesso em 02/07/2011.

[6] SUZIN, Camila. FILHO, Walter P. CAMARGO, Maria E. Análise de desempenho de protocolos de criptografia em redes sem fio. Vacaria, 2007 In: IADIS. Disponível em < http://www.iadis.net/dl/final_uploads/200713L027.pdf>. Acesso em 27/06/2011.

[7] MULLER, Nathan J. 2003**.** *Wi-Fi for Enterprise.* s.l. : McGraw-Hill, 2003. p. 174.

[8] ZADEH, Lotfi A.; FU, King-sun;TANAKA, Kokichi, SHIMURA, Masamichi. Fuzzy sets and their applications to cognitive and decision processes. Academic Press, Inc. New York San Francisco London ,1975. p. 3.

[9] COX, Earl. 1994. The fuzzy systems handbook: a practitioner's guide to building, using, and maintaining fuzzy systems. Library of Congress Cataloging-in-Publication Data ISBN 0-12-194270-8

[10] BERARDI, Rita Cristina Galarraga. Avaliação de Qualidade de Dados de Métricas de Esforço Baseado em Data Provenance e Fuzzy Logic, Porto Alegre, 2009 In: Domínio Público. Disponível em:<http://www.dominiopublico.gov.br/download/texto/cp096468.pdf>. Acesso em 10/06/2011.

[11] SBRC – 2006. 24º SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 2006, Curitiba. VIANA, Nilson Rocha; CORREIA, Reinaldo de B.; PIRMEZ, Luci. EWIDS Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas. Disponível em < http://www.sbrc2007.ufpa.br/anais/2006/ST/ST20_1.pdf>. Acessado em 12/09/2011.

[12] SBRC – 2006. 24º SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 2006, Curitiba. LAGES, Alexandre Gomes; DELICATO, Flávia C.; PIRMEZ, Luci. Um Sistema de Reputação Fuzzy para Segurança Orientada a Serviços em Redes de Banda Larga sem Fio. Disponível em <http://www.sbrc2007.ufpa.br/anais/2006/ST/SC1_2.pdf>. Acessado em 12/09/2011.