

Segurança em Sistema de Localização de Estações sem fio IEEE 802.11: Autenticação e Estações Maliciosas

Allan G. Henze¹, André Peres²

¹ Acadêmico do Curso de Sistemas de Informação da ULBRA Guaíba
< allan_henze@hotmail.com. >

² Professor Orientador do Curso de Sistemas de Informação da ULBRA Guaíba
< andre.peres@ulbra.br >

Resumo: Este artigo refere-se ao Seminário de Andamento de TCC do curso de Sistemas de Informação 2007/02. Nele está sendo apresentado um modelo de solução para questões de segurança que se aplicam à rede sem fio da Ulbra Campus Guaíba, abordando principalmente a questão de estações maliciosas e o processo de autenticação baseado na localização da estação. É mencionado, de forma sucinta, o sistema de localização já existente, bem como sua forma de funcionamento.

Abstract: This paper refers to the "Seminário de Andamento de TCC do curso de Sistemas de Informação 2007/02". It describes a solution to security issues that can be applied to Ulbra Guaíba wireless LAN, calling attention to identification of malicious stations and the location-based authentication process. It mentions the location system already in use, succinctly, as well as the way it works.

1 - INTRODUÇÃO

Atualmente existe um sistema de localização de estações sem fio padrão IEEE 802.11 em funcionamento na ULBRA campus Guaíba. Este software foi desenvolvido por Henrique Suris e utiliza, com técnica de localização, *fingerprint*. Este artigo apresenta uma proposta para o desenvolvimento de uma solução para identificar estações maliciosas que estejam tentando se associar a rede wireless da ULBRA campus Guaíba e ampliar o nível de segurança, adicionando mais um nível de autenticação (baseado na localização da estação) aos já existentes no padrão IEEE 802.11.

OBJETIVOS DO TRABALHO

O objetivo principal deste trabalho é poder implementar uma solução que até então não foi abordada, podendo, assim, adquirir novos conhecimentos e colocar em prática conceitos vistos ao longo da vida acadêmica.

2 - REFERENCIAL TEÓRICO

Atualmente, o conceito mais básico de wireless está extremamente difundido: comunicação sem fio. Com uma visão um pouco mais técnica, podemos dizer que wireless é, na realidade, toda e qualquer comunicação entre dois ou mais pontos distintos utilizando ondas eletromagnéticas onde o não são utilizados fios como meio físico. No entanto, tanto a utilização, a tecnologia e os estudos embarcados no ambiente wireless vai muito além desta mera explicação.

Segundo (PAHLAVAN, 2002), WLAN (wireless local area network) ou rede local sem fio é exatamente o que o nome se refere. Trata-se de aplicar a tecnologia Wireless como meio de comunicação em uma rede local de computadores, substituindo o cabeamento convencional. Desta forma, todas as funcionalidades das LAN também estão presentes na WLAN, incluindo compartilhamento de arquivos, compartilhamento de periféricos, acesso à internet entre outros recursos, como exemplificado na figura 1, disponível em (3COM, 2003).

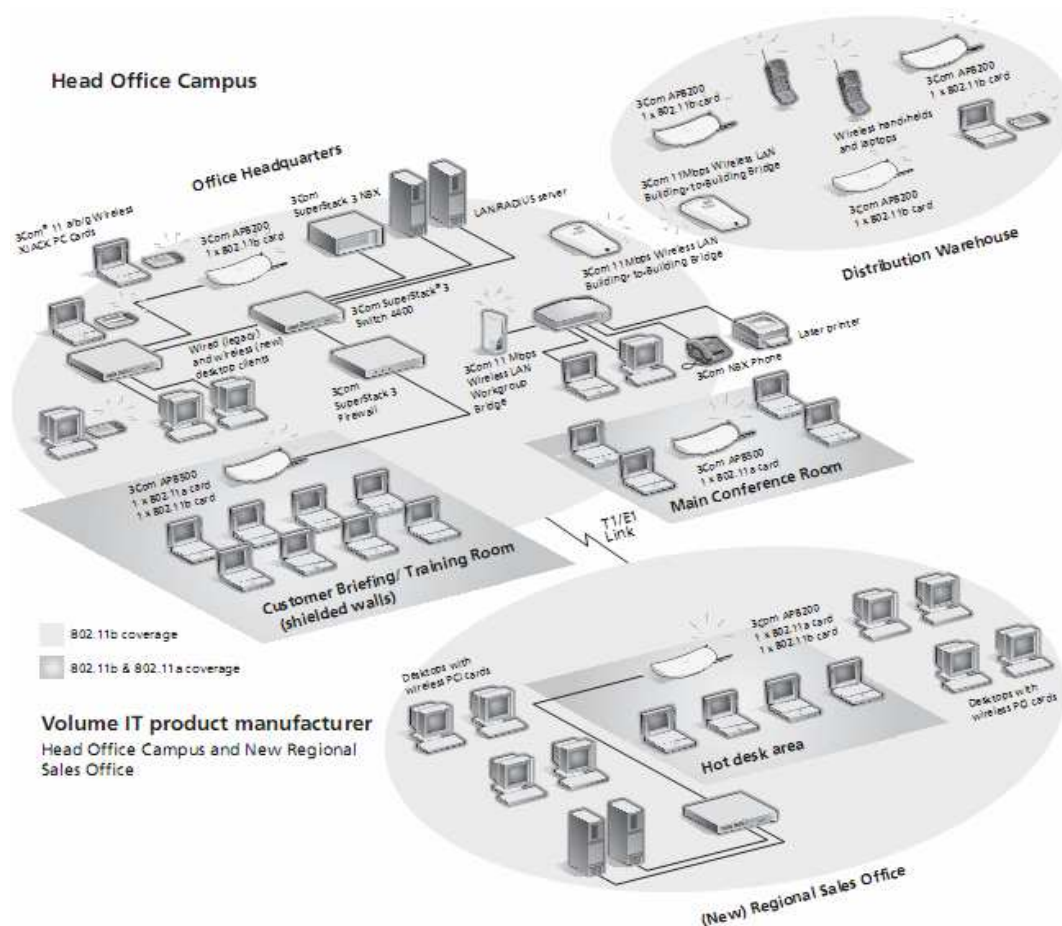


Figura 1 – Exemplo de aplicabilidade de WLAN

Visto o amplo crescimento das tecnologias e a proliferação das WLANs (por sua simplicidade de configuração básica e não exigir muitos recursos) foram determinados padrões para que sua utilização fosse eficaz e coerente. Assim sendo, através da IEEE (Institute of Electrical and Electronics Engineers) foi desenvolvido o padrão 802.11 para rede wireless.

PADRÕES

O padrão 802.11 é um membro da família IEEE 802, que trata de especificações para as tecnologias de redes locais (LAN). De acordo com as informações encontradas em (3COM, 2003), o padrão IEEE 802.11 original, estabelecido em junho de 1997, definia um sistema cuja banda fosse 2,4GHz com um *data rate* máximo de 2Mbps. Esta tecnologia ainda existe, mas não deve ser considerada para novas implantações. Hoje em dia, existem duas categorias básicas no padrão IEEE 802.11. A primeira são aquelas que especificam os protocolos fundamentais para um sistema wireless completo: 802.11a, 802.11b e 802.11g. Já a segunda categoria, é composta por extensões endereçadas às fragilidades ou para adicionar novos atributos aos padrões da primeira categoria. São eles: 802.11d, 802.11e, 802.11f, 802.11h, 802.11i, 802.11j. A tabela 1, também disponível em (3COM, 2003), mostra maiores detalhes a respeito da primeira categoria:

	Standard	Radio Band	Modulation	Max. Link Coverage	Max. Data Rate	Max. # Non-overlapping channels	Other Issues
More established standard ↑ ↓ Newer standard	802.11b	2.4 GHz	DSSS	100m/328ft	11 Mbps	3	- 802.11b networks have the largest installed base.
	802.11a	5 GHz	OFDM	50m/164ft	54 Mbps	12 (fewer in some regions)	- Needs 802.11 extensions to be used in some regions (e.g., EMEA)
	802.11g	2.4 GHz	OFDM	100m/328ft	54 Mbps	3	- Backward-compatible with 802.11b - Fully ratified

Tabela 1 – Padrões 802.11a, 802.11b e 802.11g.

É importante salientar que existem algumas considerações a serem feitas quando trabalhando com estes padrões. Como por exemplo:

- 802.11b: não indicado para aplicações que utilizem muita banda, porém se a intenção é uma maior cobertura, deve ser considerada, além do custo dos equipamentos que utilizem este padrão ser inferior aos dos demais. Como principal

desvantagem, pode-se citar que o *data rate* deste padrão é muito baixo e, por utilizar a frequência 2,4GHz (mesma utilizada por alguns equipamentos de telefone sem fio e Bluetooth), pode ter sua capacidade reduzida e sofrer interferências.

- 802.11a: indicado nos casos de aplicações como voz (telefones IP) e vídeo, em função do alto *data rate*. O grande número de *non-overlapping channels* permite que vários Access Points sejam colocados uns mais próximos dos outros sem que haja interferência. Como desvantagem, pode-se citar que não é compatível com o padrão 802.11b e seu custo é mais elevado para se proporcionar semelhante cobertura do sinal.

- 802.11g: indicado quando se necessita rodar aplicação que consomem muita banda (áudio e vídeo) e uma área de cobertura mais abrangente. Além disto, ainda oferece compatibilidade com equipamentos padrão 802.11b. Como desvantagens têm-se alta possibilidade de interferência (por utilizar frequência semelhante ao padrão 802.11b) e, quando se operam ambos os padrões em conjunto, sua capacidade fica reduzida ao do 802.11b.

Os demais padrões seguem abaixo:

- 802.11d: garante a interoperabilidade em WLANs cujos países ainda não possuem o padrão 802.11 aplicado.

- 802.11e: define níveis de QoS (Quality of Service) para aplicações como áudio e vídeo.

- 802.11f: trata-se do IAAP (Inter Access Point Protocol). Melhora o *handover* entre APs e segmentos com switches como os usuários efetuam *roaming* entre eles.

-802.11h: adiciona um melhor controle entre potência de transmissão e seleção de canais no 802.11a.

-802.11i: prover melhoria de segurança, incluindo a utilização do protocolo de segurança 802.1x (que será abordado ao decorrer deste artigo).

-802.11j: adição dos endereços canal de 4.9GHz para 5GHz para o padrão 802.11 apenas no Japão.

802.11 E AS CAMADAS OSI

A figura 2, disponível em (3COM, 2000) demonstra o em que ponto os padrões da família 802.11 e operam nas camadas OSI.

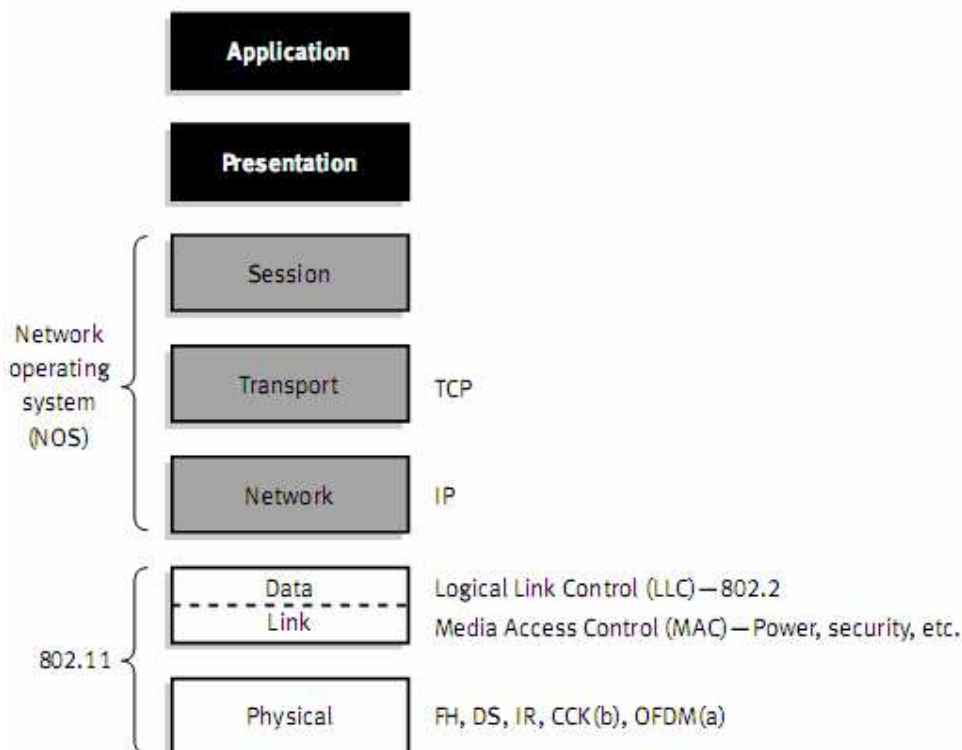


Figura 2 – Padrão 802.11 e as camadas OSI

Segundo (GAST, 2002), poder-se-ia dizer que o IEEE 802.11 é apenas mais uma camada de link que pode utilizar o 802.2/LLC (Logical Link Control), o que omitiria alguns detalhes. Entretanto, são estes detalhes que fazem com que este padrão funcione tão bem. A especificação original do 802.11 incluía o 802.11 MAC (Media Access Control) e duas camadas físicas: FHSS (Frequency-Hopping Spread-Spectrum) e DSSS (Direct-Sequence Spread-Spectrum). Revisões posteriores à 802.11 adicionaram outras camadas físicas, como, por exemplo, o 802.11b, que especifica o HR/DSSS (High-Rate Direct-Sequence), ou o 802.11^a, que descreve uma camada física baseada em OFDM (Orthogonal Frequency Division Multiplexing).

Ainda de acordo com (GAST,2002), 802.11 permite acesso à rede para dispositivos móveis e, para isso, uma série de melhorias foram implementadas no MAC. Como resultado, o MAC 802.11 é extremamente mais complexo que os MAC dos demais padrões da família IEEE 802.

A figura 3 [disponível em: < <http://www.javvin.com/protocolWLAN.html>> Acesso em: 09/2007] demonstra maiores detalhes destas camadas, inclusive com os níveis de autenticação, que será abordado superficialmente no próximo sub-ítem.

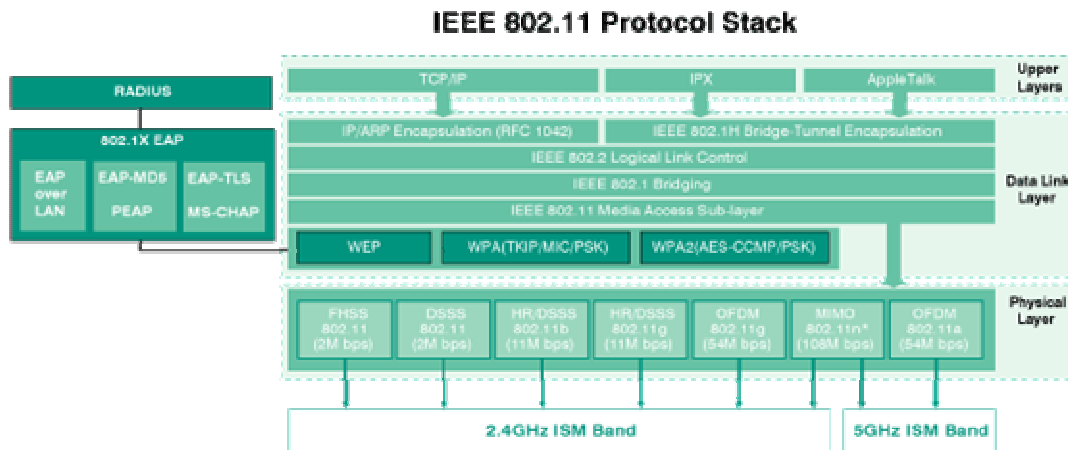


Figura 3 – Padrão 802.11, as camadas OSI e Autenticação

SEGURANÇA

O padrão IEEE 802.11 oferece dois métodos para disponibilizar a segurança dos dados: criptografia e autenticação. Nele existem dois métodos de autenticação: Open System e Shared Key.

Open System - é o sistema padrão de autenticação. Neste, qualquer estação que solicitar a associação à rede será aceita. Trata-se de um sistema nulo de autenticação.

Shared key – neste método, tanto a estação que solicita acesso quanto a autenticadora (seja um AP ou outra estação) necessitam que uma chave secreta seja compartilhada entre elas. Para este caso é utilizado o protocolo WEP (Wired Equivalency Privacy).

3 - SOLUÇÃO PROPOSTA

Com base nas informações já passadas, este artigo foca o desenvolvimento e implantação de features de segurança em um sistema de localização de estações sem fio padrão IEEE 802.11. Tal sistema, já foi desenvolvido e documentado por

Henrique Suris e se encontra em funcionamento na ULBRA campus Guaíba. O mesmo utiliza a técnica de *fingerprint* para localização das estações.

Atualmente, o módulo cliente do sistema apenas informa o servidor os pontos de acessos localizados pela estação, sua atenuação e SSID (Service Set Identifier – identificação da rede sem fio). Para que seja possível concretizar os objetivos, o módulo cliente deverá forçar a estação a se associar a todos os SSIDs identificados e solicitar, ao ponto de acesso correspondente, qual a atenuação do sinal. Vale lembrar que, para conseguir se associar ao AP correspondente, o módulo cliente deverá identificar o tipo de autenticação configurada, seja ela “Open System”, “Shared Key” ou “802.1x”, em cada um destes aparelhos e efetuar o processo de associação. Ou seja, a solução implementará mais uma camada de segurança, não substituindo nenhuma das já existentes.

Após realizar esta consulta em todos os pontos de acesso localizados, estas informações são passadas ao servidor que valida ou não a autenticação da estação.

Resumidamente, o sistema será responsável por garantir que as informações referentes à atenuação e SSID passadas para o mesmo são verídicas e que sua posição no espaço coberto pela rede wireless é, de fato, a que a estação esta informando ao sistema.

4 - CONCLUSÃO

Através deste primeiro contato mais aprofundado com a tecnologia wireless pode-se concluir que é um segmento em constante evolução e que certamente trará muitos avanços. Sem dúvida, este trabalho está sendo conduzido de forma a ser tanto instrutivo quanto funcional e certamente outras melhorias serão identificadas e implementadas no sistema já existente.

Acredita-se ainda, que, da mesma forma que ferramentas WIKI e comunidades relacionadas a softwares open-source, este TCC fará com que outros acadêmicos despertem interesse por este segmento e venham a dar continuidade a este sistema.

É importante ressaltar que, muitas referências ainda não foram citadas, mas que já fazem parte do TCC, que irá conter todas as informações necessárias para a

implementação da solução no decorrer do TCC-II. Sendo parte deste, as fase de modelagem, desenvolvimento e testes

5 - BIBLIOGRAFIA

3COM Corporation. **Technical Paper: IEEE 802.11b Wireless LANs**. USA: 3Com Corporation, 2000.

3COM Corporation. **White Paper: Deploying 802.11 Wireless LAN**. USA: 3Com Corporation, 2003.

DUBENDORF, Vern A. **Wireless Data Technologies – Reference Handbook**. England: John Willey & Sons Ltd, 2003.

GAST, Matthew S. **802.11 Wireless Networks: The Definitive Guide**. UK: O'Reilly & Associates, 2002.

PAHLAVAN, Kaveh; LI, Xinrong; YLIANTTILA, Mika; LATVA-AHO, Matti. **“Wireless Data Communication Systems”, Wireless Communication Technologies – New Multimedia Systems**, edited by MORINAGA, Norihiko; KOHNO, Ryuji; SAMPEI, Seiichi: KLUWER ACADEMIC PUBLISHERS, 2002. Page(s): 201-214

WLAN Wireless LAN by IEEE 802_11, 802_11a, 802_11b(Wi-Fi), 802_11g, 802_11n - <http://www.javvin.com/protocolWLAN.html>. Acessado em setembro de 2006.