UM ESTUDO DA APLICAÇÃO DA FERRAMENTA ORINOCO EM REDES WIRELESS

Diogo Lisboa Lopes

Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Barbacena – MG – Brasil.

RESUMO: Este artigo tem como objetivo apresentar um estudo sobre a aplicação ferramenta Orinoco em redes *Wireless*. Abordando de uma maneira geral o funcionamento de redes sem fio, suas características, utilização e possíveis problemas encontrados com o uso desta tecnologia. Visa também apresentar uma melhor maneira de se implantar uma WLAN (rede *wireles*), possibilitando a instalação, manutenção e gerência da rede através do uso da ferramenta Orinoco.

Palavras chave: *Wireless*, Orinoco, rede sem fio, WLAN.

1 - INTRODUÇÃO

Conhecidas como *Wireless* ou redes sem fio, a tecnologia que possibilita mobilidade ao usuário sem perder conexão com a rede tem sido muito utilizada atualmente, pois junto com a evolução das redes de computadores, começaram a aumentar a necessidade de interligação não somente dos dispositivos fixos, mas também os móveis. Visto que está cada vez mais comum o uso de dispositivos móveis portáteis que utilizam infra-estrutura de rede sem fio, como os *notebooks* e *hand-helds*[1].

Redes que não utilizam cabeamento são conhecidas como *Wireless*, pois possuem seu funcionamento baseado na transmissão de dados através do ar, utilizando

[1] Computadores portáteis, exemplo: *Palm Top.*

sinais de RF (rádio freqüência) ou infravermelho e minimizando a utilização de cabos de conexão para que seus usuários se conectem a rede. As WLAN`s fornecem comunicação entre dispositivos com mobilidade dos seus usuários dentro da área de cobertura da rede, que poderá atingir até algumas centenas de metros, de acordo com os equipamentos utilizados.

A utilização das redes *Wireless* vem se tornando atraente por diversos motivos, tais como: mobilidade, facilidade de instalação, praticidade, instalação em locais que possuem inviabilidade técnica de uma rede cabeada ou, ainda, dificuldade para passagem de cabos. Podem também ser implementadas como uma alternativa ou extensão para as redes convencionais cabeadas. Além das redes locais esta tecnologia também vem sendo utilizada para redes de acesso a *Internet* em locais como cafés, restaurantes, aeroportos e outros que possuem acesso a *Internet* utilizando tecnologia sem fio. Encontramos atualmente este serviço em muitas cidades brasileiras como São Paulo e Rio de Janeiro que tem adotado a tecnologia *Wireless*.

Este artigo visa orientar quanto ao uso da ferramenta Orinoco em redes *Wireless*. O mesmo foi organizado em capítulos onde o primeiro visa familiarizar e entender melhor o funcionamento da comunicação sem fio; o segundo aborda seus tipos de operação; no terceiro é apresentado padrões do IEEE (Institute *of Electrical and Eletronics Engineers*); o quarto trata sobre possíveis interferências; o quinto aborda os problemas com a segurança apresentando também algumas soluções que possam se tornar de uso fundamental para integridade da informação; o sexto trata as vantagens obtidas com o uso da ferramenta Orinoco que possibilita a gerência e manutenção de uma rede *Wireless* e, através dela ou da análise de seus resultados permitir um melhor funcionamento das WLAN's. O sétimo capítulo apresenta as considerações finais sobre o artigo.

2 - TIPOS DE OPERAÇÃO

WLAN`s utilizam tipos de operação em rede conhecidos como infra-estrutura ou *peer to peer*, sendo que a primeira deve possuir o papel do A*cess Point*

(AP) fazendo a cobertura de determinada área geográfica. Essas áreas quando divididas são chamadas de células. Já na operação *peer to peer* trabalha com um tipo de topologia *ad-hoc*, onde os clientes remotos comunicam-se sem necessidade de um AP e os dois clientes envolvidos nestas comunicações ficam com a responsabilidade de envio das informações até o outro dispositivo.

3 - PADRÕES

Diante da grande quantidade de aparelhos que utilizam tecnologia sem fio, tornou-se necessário à criação de padrões de mercado de forma a se tornar mais amigável e transparente a utilização da comunicação móvel.

O IEEE padronizou a utilização de redes sem fio, determinando freqüências de modo a minimizar o problema da interferência e determinar características que tornam mais confiável e ágil o uso de LAN's sem fio.

Surgiu então o padrão IEEE 802.11, que se subdivide em alguns outros padrões que são mais utilizados como os IEEE 802.11a, b, e, g, i. Esses padrões seguem a mesma filosofia do IEEE 802.11, porém, possuem algumas características particulares o que os tornam diferentes no que se refere à freqüência e velocidade de comunicação. Atualmente dentre estes o mais utilizado é o 802.11b.

Equipamentos que são compatíveis com o IEEE 802.11 foram também batizados de WI-FI (*Wireless Fidelity*) e normalmente possuem a mesma sigla impressa nas caixas dos fabricantes para que sejam identificadas como compatíveis com o padrão 802.11.

Segundo Martins, o padrão IEEE 802.11b é um padrão projetado pelo IEEE e um dos principais focos de estudo atualmente por ser o padrão utilizado na maioria das redes *Wireless*. Pode basear-se na tecnologia *Direct Sequence Spread Spectrum* (DSSS) que usa transmissão aberta (*broadcast*) de rádio e opera na freqüência de 2.4000 a 2.4835 GHz com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as

ondas estão se propagando (paredes, interferências, etc). Por ser uma transmissão aberta, qualquer pessoa com um receptor operando na mesma freqüência pode captar as ondas. Porém, conforme se afasta da estação de rádio transmissora o sinal começa a ficar cada vez mais fraco até que não possamos mais captá-lo. O padrão IEEE 802.11b possui características como: conexão *peer to peer* ou com a presença de *Acess Point* para acesso a rede, funciona com dois modos de espalhamento de freqüência o FHSS (*Frequency hopping spread spectrum*) e o DSSS (*Direct Sequence Spread Spectrum).* Funciona com infravermelho, utiliza CSMA-CA[2] (*Carrier Sense Multiple Access with Collision Avoidance)* que trata colisão de pacotes; utiliza ainda o protocolo WEP (*Wired Equivalent Privacy*) para criptografia.

O espalhamento de freqüência FHSS funciona com troca de freqüência de tempo em tempo. É mais utilizado em aplicações *outdoor*[3], em ambientes abertos, áreas urbanas, locais onde possuem muito ruído causando interferência. Pois, caso ocorra ruído, ele só afetará a rede no curto intervalo de tempo em que o espalhamento permaneceu com a freqüência que gerou interferência. Possui taxa de transferência mais baixa que o DSSS devido a mudar de freqüência em determinado intervalo de tempo.

O espalhamento de freqüência DSSS funciona com uma faixa de freqüência fixa, distribuída por igual e o sinal tem a mesma intensidade em toda a faixa de freqüência. Quando há interferência em uma freqüência da faixa, a transmissão continua pelas outras, afetando a velocidade de transmissão dos dados. É mais utilizada em aplicações *indoor*[4] por ter taxa de transferência de dados um pouco maior que o FHSS.

Existe também o padrão IEEE 802.11g que funciona com equipamentos que operam a 54 Mbps e permite compartilhar a mesma rede com equipamentos que usam o IEEE 802.11b, garantindo assim, a migração do padrão IEEE 802.11b para o IEEE 802.11g sem impacto na rede.

[2] Método de reenvio dos pacotes que sofrem colisão.
[3] Comunicação aberta (mais de uma estação recebe o sinal transmitido). Ex: Comunicação entre Torre c e Estações na Figura 1 do Anexo.
[4] Comunicação entre dois únicos dispositivos, sinal só é captado por um único equipamento. Comunicação fechada entre os dispositivos. Ex: Comunicação entre Torre A e Torre B da Figura 1 no Anexo.

4 - INTERFERÊNCIA

Um dos maiores problemas na utilização de redes *Wireless* é a interferência, pois, dependendo do tipo e grau de intensidade da mesma pode fazer com que uma rede sem fio deixe de ter seu funcionamento ideal e estabilizado. A interferência pode ocorrer em locais que possuam equipamentos que utilizam a mesma freqüência ou freqüências próximas especificações do padrão utilizado.

Devido à comunicação das WLAN's basear-se em infravermelho ou por rádio freqüência, a rede pode sofrer uma indesejável interferência com outros dispositivos que utilizam recursos semelhantes.

Ao se utilizar infravermelho, torna-se necessário que no caminho entre o transmissor e o receptor não se deve ter nenhuma barreira física, além de ser necessário um bom alinhamento entre os dois equipamentos para que a comunicação seja de feita da forma devida.

No caso de RF deve-se observar à freqüência que está sendo utilizada e garantir local adequado de forma que não haja aparelhos que possam gerar interferência. É importante também considerar locais onde não haja barreiras ou obstáculos a fim de impossibilitar uma boa propagação do sinal eletromagnético. Estas características são imprescindíveis para que não ocorra a queda na qualidade do sinal da rede. Situações como interferência ou barreiras físicas podem ocasionar o surgimento de áreas de sombras, que são locais que não possuem cobertura da rede. Para minimizar este problema faz-se necessário o deslocamento do usuário para uma área coberta pelo sinal. Situação desfavorável para usuários que necessitam se deslocarem sem perder a conexão com a rede.

5 - SEGURANÇA

As redes *Wireless* facilitam a disponibilidade da informação, visto que esta pode ser acessada a qualquer instante de qualquer lugar onde haja cobertura,

bastando, dessa forma, apenas se conectar sem a utilização de nenhum cabeamento. Desta forma a área de acesso à rede pode ultrapassar a área física e as limitações não são mais determinadas fisicamente, quebrando o paradigma de controle de acesso físico à rede. Essa característica de disponibilidade das informações pode tornar-se um problema no que diz respeito à segurança e obrigar as corporações que utilizam esse tipo de rede atualmente possuam um bom sistema de segurança, garantindo assim o sigilo, confidencialidade e integridade de seus dados, pois atualmente ataques a esses tipos de redes tem se tornado cada vez mais freqüentes.

Situações como a citada acima, tornou a segurança um dos principais requisitos de uma rede sem fio em que se necessita privacidade das informações. Pois a mesma informação que antes trafegava em cabos, agora são enviadas ao ar livre, levando a um novo cenário onde o controle de acesso e autenticidade dos usuários da rede devem ser garantidos mais do que nunca.

Muitos administradores de rede, instalam erroneamente equipamentos *Wireless* com configurações *default*[5] do fabricante, tornando sua rede muito atraente a ataques maliciosos de *hackers*[6] ou *crackers.*[7]

Manter a configuração *default* é um erro visto que existem pessoas que ficam rastreando redes vulneráveis. Uma das principais vulnerabilidades é manter a configuração *default* para o SSID (*Server Set ID*) ou até mesmo deixá-la com um nome muito claro, como por exemplo, o próprio nome da empresa. Visto que, o SSID é o nome único que diferencia e identifica uma rede sem fio da outra.

Através da ferramenta Orinoco do fabricante Lucent, é possível configurar o *Acess Point* ou *bridge* desabilitando a opção de *broadcast* do SSID para que não ocorra o perigo dessa informação ser capturada por algum invasor que utilize alguma ferramenta que captura o SSID quando o comutador estiver configurado para espalhar o mesmo através de *broadcast*. Entende-se por comutador os equipamentos de *Acess Point* e *bridge*. Outra opção fornecida pela ferramenta é a filtragem de endereços MAC *Adress*[8] pelo comutador, fazendo que ele aceite comunicação somente com

[5] Configuração padrão do fabricante.
[6] O uso do termo hacker é associado a especialistas em informática.
[7] Hacker que utiliza os seus conhecimentos para quebrar a segurança de sistemas de informação de forma ilícita.
[8] O MAC *Address* é o endereço físico de uma placa de rede ou de um Pcmcia.

dispositivos que são conhecidos pelo AP e previamente cadastrados em sua tabela de endereços MAC.

O correto monitoramento da rede é fundamental para se evitar situações indesejáveis, comportamentos anormais ou até mesmo a detecção de intrusos em seu ambiente de cobertura. Outras normas básicas e extremamente importantes referem-se a constante renovação de senhas, principalmente as senhas dos administradores da WLAN, juntamente com a não divulgação de endereçamento e outras configurações dos ativos da rede. É importante ainda desabilitar todo tipo de conexão remota, principalmente do roteador, além de desabilitar compartilhamentos existentes. O uso de *firewall*[9] também pode bloquear solicitações de *Internet* desconhecidas.

5.1 - WEP

Segundo Martins, é um protocolo muito utilizado atualmente, o *Wired Equivalent Privacy* foi desenvolvido para ser utilizado com o padrão IEEE 802.11, fornecendo uma melhor segurança às comunicações sem fio, pois usa criptografia e autenticação. Utiliza o algoritmo RC4[10] para criptografia dos pacotes que irão trafegar no ar além do CRC32[11], possibilitando ao receptor detectar se a mensagem está corrompida.

Após a detecção de fragilidades no algoritmo do RC4 como o reuso de chaves para criptografia, surgiram algumas propostas para melhora do WEP como a criação de chaves diferentes para cada pacote utilizando 128 bits para criptografia. Devido a esse tipo de falha, foram criadas novas versões do protocolo que tentam corrigir os erros apresentados anteriormente. Surgindo então, a nova versão do WEP que corrigiu o problema do reuso das chaves e foi chamado de “WEP2”. Juntamente com o WEP2 surgiu o protocolo TKIP (*Temporal Key Integrity protocol*), conhecido

[9] *Firewall* pode ser definidido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem *firewalls* baseados na combinação de hardware e software e *firewalls* baseados somente em software.
[10] Algoritmo utilizado para gerar chaves criptográficas no WEP.
[11] Função que permite ao receptor verificar se a mensagem foi corrompida.

também no mercado brasileiro como o protocolo de chaves temporárias, esse protocolo utiliza chaves assimétricas temporárias que se alternam periodicamente, corrigindo assim a fragilidade do algoritmo RC4. Esta solução é encontrada no mercado com o nome de WPA (acesso protegido WI-FI), pois o protocolo garante que mesmo se a chave for descoberta por alguém, esta provavelmente já terá mudado e o invasor não conseguirá descriptografar a mensagem.

6 - FERRAMENTAS

A ferramenta Orinoco do fabricante Lucent, nos possibilita testar e avaliar o *link* entre os dispositivos sem fio de uma rede que utilize o Pc *card*[12] e o *card* para AP[13] compatível com o padrão IEEE 802.11 e com a solução Orinoco. No teste de link é possível verificar a qualidade do sinal e a quantidade de ruído que irá interferir na qualidade da comunicação sem fio e na boa propagação do sinal conforme pode ser visto nas Figura 2 e Figura 3 apresentadas no Anexo. Isso permite classificar a comunicação em excelente, bom, aceitável e ruim. Uma classificação excelente acontece normalmente em equipamentos que estão muito próximos, não possuem nenhuma interferência e a taxa de velocidade do tráfego da rede não sofre nenhuma perda. A classificação do sinal como bom ocorre em locais onde possuem pouca perda na velocidade do tráfego da WLAN, pode ocorrer interferência mínima e não possui nenhuma barreira que possa prejudicar a comunicação dentro da área de cobertura. A classificação aceitável ocorre quando a rede possui uma barreira que atrapalhe a propagação de RF ou quando há interferência de forma que não prejudique tanto a qualidade da comunicação, ocorrendo uma queda pouco perceptível na velocidade da rede. Já a classificação ruim, acontece quando há muita interferência ou barreiras que influem diretamente em uma má comunicação e pouca velocidade do tráfego, normalmente acontece quando a velocidade de transmissão fica próxima a 2Mbps.

A ferramenta permite também analisar a quantidade de pacotes enviados, recebidos e retransmitidos por cada cliente da rede, possibilitando um constante

[12] Faz o papel de placa de rede em rede sem fio.
[13] Faz o papel de placa de rede de um *Acess Point* em rede sem fio.

monitoramento no tráfego de uma WLAN e permitindo assim uma avaliação mais precisa do funcionamento da rede ou até mesmo detectar problemas como barreiras, congestionamentos e comprometimentos da rede em horários de maior utilização.

Foi dado um maior enfoque no Orinoco porque o mesmo apresenta todas as funcionalidades que são necessárias para administração, configuração e manutenção da rede, tornando a utilização de outras ferramentas como opcional. Além de possibilitar o gerenciamento de todas as funcionalidades necessárias de uma WLAN, existem outras ferramentas que podem ser utilizadas para auxílio ao gerenciamento de uma WLAN, como exemplo, Qcheck[14] que é uma ferramenta de medições de tempo de resposta da rede.

Com a utilização da ferramenta Orinoco o gerenciamento de uma rede sem fio se torna mais viável e seguro. Permitindo a configuração da senha de administrador para acesso e configuração das estações clientes, AP`s ou b*ridges*, determinando freqüência, protocolo, alinhamento entre antenas, melhor local para colocar um AP ou uma estação qualquer.

AP`s podem apresentar problemas de travamento, devido a diversos problemas como engarrafamento do tráfego na rede ou ultrapassagem do total de requisições de serviço para o AP. Neste caso, o administrador pode acessar remotamente o AP ou *bridge*[15] de qualquer estação cliente podendo dar *boot*[16] nos equipamentos ou alterar sua configuração após ter se autenticado através do seu usuário administrador configurado anteriormente.

O alinhamento das antenas utilizadas pode ser analisado pelo Orinoco e caso necessário efetua-se o alinhamento sem desligar o equipamento ponte e sem desconectar a antena. Podendo ainda determinar a melhor posição para alinhamento através da conexão com um *notebook*.

7 - CONSIDERAÇÕES FINAIS

[14] Ferramenta que mede tempo de resposta dos dispositivos de uma rede.
[15] Equipamento ponte que é utilizado como ponte entre dois tipos de rede diferentes.
[16] Iniciar o serviço de um dispositivo.

A idéia de que futuramente em qualquer local em que o homem esteja ele possa ter disponível o serviço de uma rede sem fio e poder se conectar a *Internet* e outros serviços, possibilita enxergar as redes *Wireless* como uma tecnologia que avança a cada dia nos provendo melhores recursos e tecnologias para utilização da rede e fornecendo as pessoas mais comodidade e facilidade para acesso as informações.

Porém, além de suas vantagens, as WLAN`s possuem fragilidades como segurança e interferência e apesar das diversas maneiras mais seguras para acesso a esse tipo de rede, a cada dia são descobertas novas fragilidades da rede como, por exemplo, a fragilidade de protocolos, o que nos leva a necessidade de constante renovação dos recursos que fornecem segurança nas redes de comunicação sem fio.

É importante ressaltar ainda que uma rede sem fio deve antes de tudo, ser bem planejada antes de sua implantação e, dependendo de sua aplicação, este projeto deve ser muito bem elaborado e detalhado. Estes cuidados visam minimizar situações indesejáveis como uma má qualidade da comunicação sem fio ou até mesmo uma invasão. Além disso, após sua implantação torna-se necessário um bom gerenciamento e monitoramento utilizando-se de ferramentas e dos melhores recursos de segurança, visto que uma das grandes vulnerabilidades dessas redes está neste aspecto. Pois administrar uma rede *Wireless* torna-se mais fácil a cada dia devido à quantidade de ferramentas disponíveis no mercado.

Como proposta de trabalhos futuros sugere-se:

- Utilização da ferramenta Orinoco para análise da estrutura de uma rede *Wireless;*
- *Estudo comparativo entre Orinoco e outras ferramentas de gerência de redes Wireless.*

8 - REFERÊNCIAS BIBLIOGRÁFICAS

TANENBAUM, Andrew S. *Redes de Computadores*; Rio de Janeiro: Campus, 2003.

Orinoco Manager Suite: User's Guide, Disponível em: <http://www.mikrotik.com/Documentation/manual_2.3/Wavelan/ug_OM.pdf> Acesso em: 20 de agosto de 2004.

PEIXOTO, Roney de Castro. *Tecnologias Wireless demandam cuidados extras*. <http://www.csalaw.com.br/pdf/Art_dig11.pdf>, Acesso em 25 ago 2004.

PINHEIRO, José Maurício Santos. *A Trilogia Wireless*. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_trilogia_*wireless*.php> Acesso em 25 de agosto de 2004.

MARTINS, Marcelo. *Protegendo Redes wireless*. Disponível em <http:// www.modulo.com.br/index.jsp>Acesso em 10 de maio de 2005.

MACIEL, Paulo Ditarso; NUNES, Bruno Astuto Arouche; CAMPOS, Carlos Alberto; MORAES, Luiz Felipe. *Influência dos mecanismos de segurança no tráfego das redes sem fio 802.11b*. Disponível em: <http://www.lockabit.coppe.ufrj.br/rlab/rlab_textos.php?id=79> Acesso em 30 setembro de 2004.

ANEXO

Serão apresentadas no anexo algumas funções da ferramenta Orinoco aplicada a uma WLAN que utiliza o padrão 802.11b com o intuito de demonstrar o real funcionamento de uma das funções desta ferramenta, onde serão apresentados os testes de comunicação efetuados na referida rede *Wireless*. Vale ressaltar que por questões de segurança não serão divulgados alguns detalhes da rede como os *Adress* (endereços MAC) dos equipamentos analisados e seus *host names*[17] que foram alterados propositalmente.

A Figura 1 apresenta a infra-estrutura da rede na qual utilizou-se a ferramenta Orinoco para aplicação do *link* teste. É apresentado um fluxo de comunicação contínuo que segue a seguinte ordem: *Router* → *switch* → *Bridge* AP1000 conectada a um cabo particular → Torre A (Utliza antena Parabólica para comunicação *indoor* com a Torre B distanciadas de ~1,5KM.) → Torre B (Possui parabólica recebendo sinal da Torre A e parabólica comunicando com outro local não analisado na situação, possuindo também uma *bridge* com dois *cards e* parabólica setorial[18] encaminhando o sinal para Torre C) →Torre C (comunicação *indoor* com Torre B distanciadas de ~1KM, possuindo parabólica que recebe o sinal e uma semi-parabólica setorial encaminhando o sinal em modo *outdoor* para a Estação A). → Estação A (micro com uma antena de ganho de ~5db (cinco decibéis)).

[17] Nome identificador do equipamento na rede.
[18] Espalha o sinal em um ângulo de noventa graus.

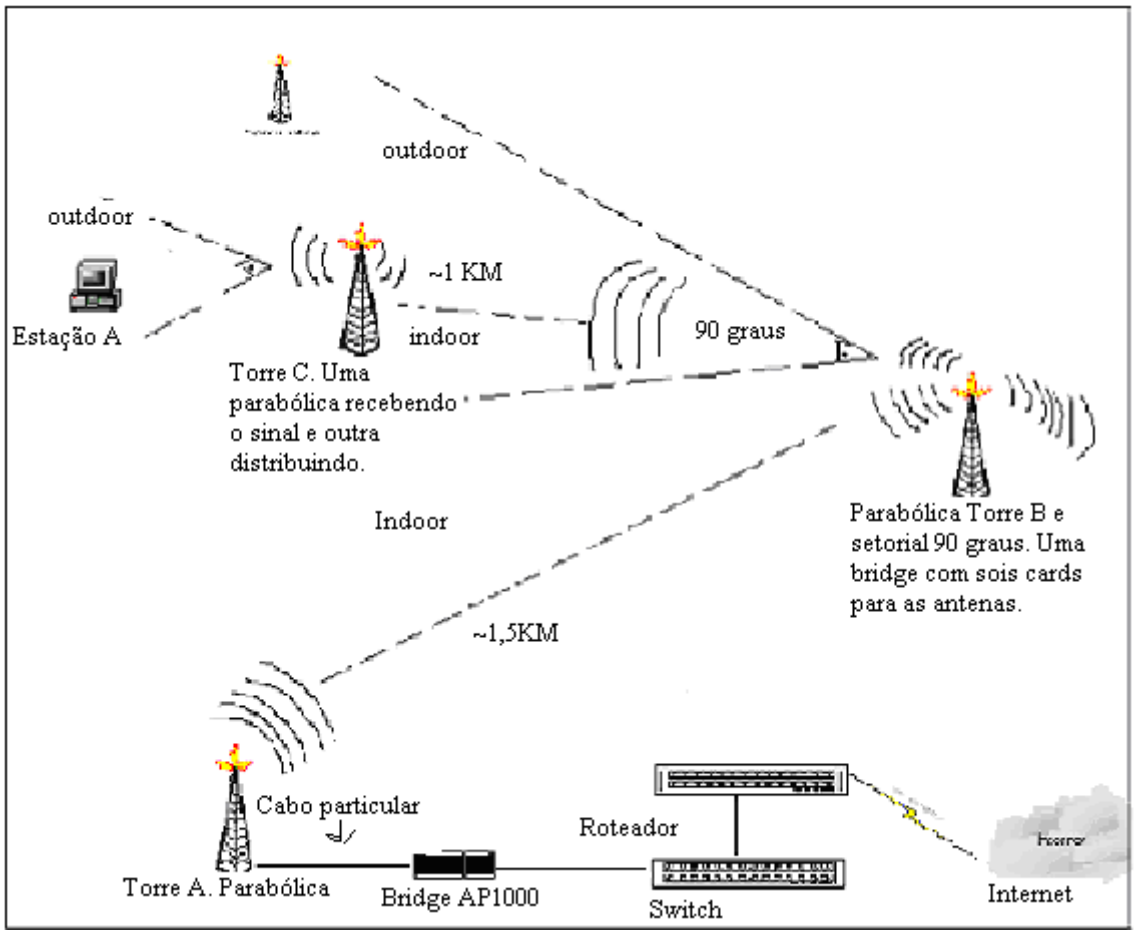

Figura 1. Infra-estrutura física da rede.

A Figura 2 apresenta a classificação de qualidade da comunicação entre a antena parabólica conectada a *bridge* da TORRE A e a parabólica conectada a *bridge* da TORRE B como boa, utilizando comunicação do tipo *indoor*. Foram alterados os *Adress* e o *host names* da figura propositalmente por questões de segurança conforme apresentado na Figura 2. É verificado em (*local levels* e *remote levels)* a qualidade do sinal na *bridge* local chamada de TORRE A e também na *bridge* remota chamada de TORRE B em função da análise que a ferramenta faz sobre SNR (sinal/ruído) destes locais. Possibilita ainda a análise da quantidade de pacotes que a *bridge* recebeu e quantos foram perdidos. A avaliação do estado do link permite ainda verificar a qualidade do sinal que é condicionada à quantidade de ruído existente na transmissão, logo, quanto maior o ruído, pior será a qualidade do sinal e, conseqüentemente, também a qualidade do *link* entre os clientes remotos.

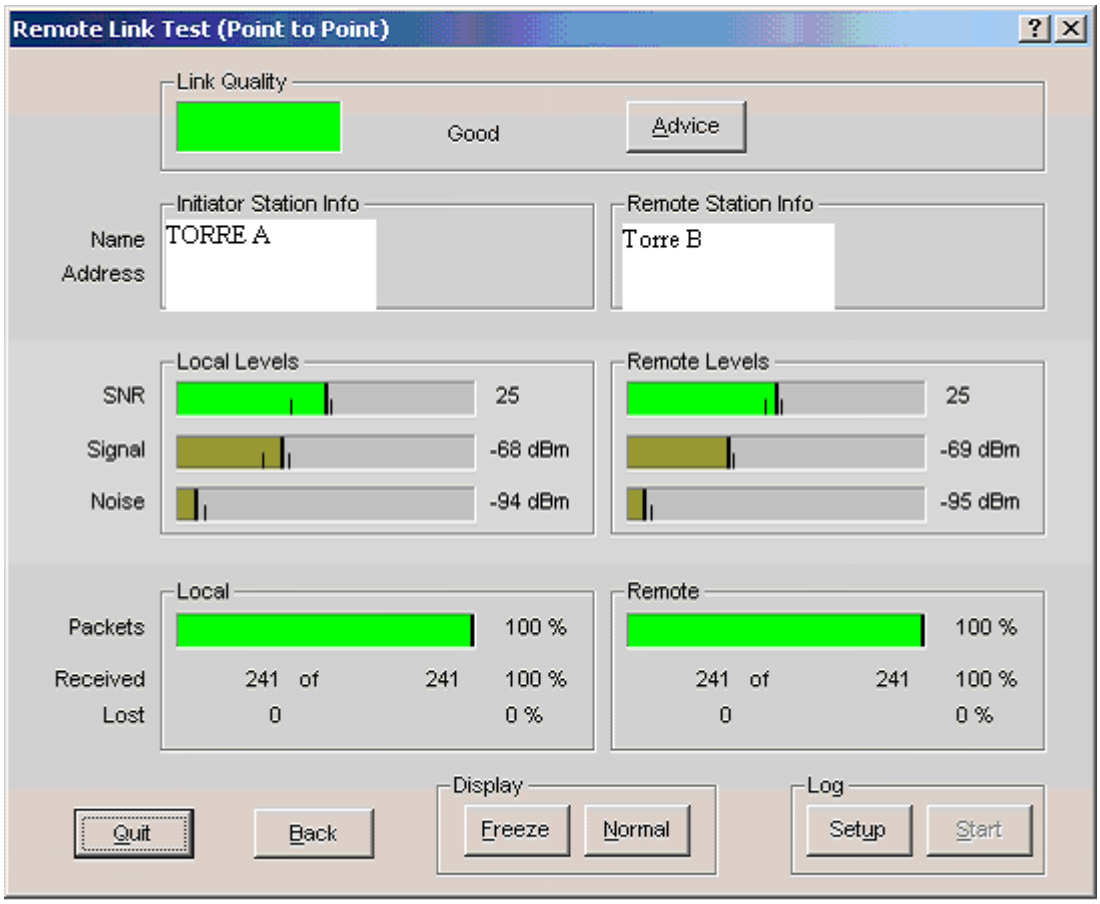

Figura 2. Teste do *link* entre as Torres A e B.

A Figura 3 apresenta o *link* teste entre a semi-parabólica conectada a *bridge* Torre C e antena de 5db conectada a Estação A. Foram alterados os *Adress* e o *host names* da figura propositalmente por questões de segurança conforme apresentado na Figura 3. A comunicação foi classificada como aceitável, pois, há um considerável ruído próximo a TORRE C que caso piorasse um pouco mais faria com que a

comunicação ficasse de má qualidade, mesmo assim, a *bridge* ainda consegue enviar todos os pacotes sem perda.

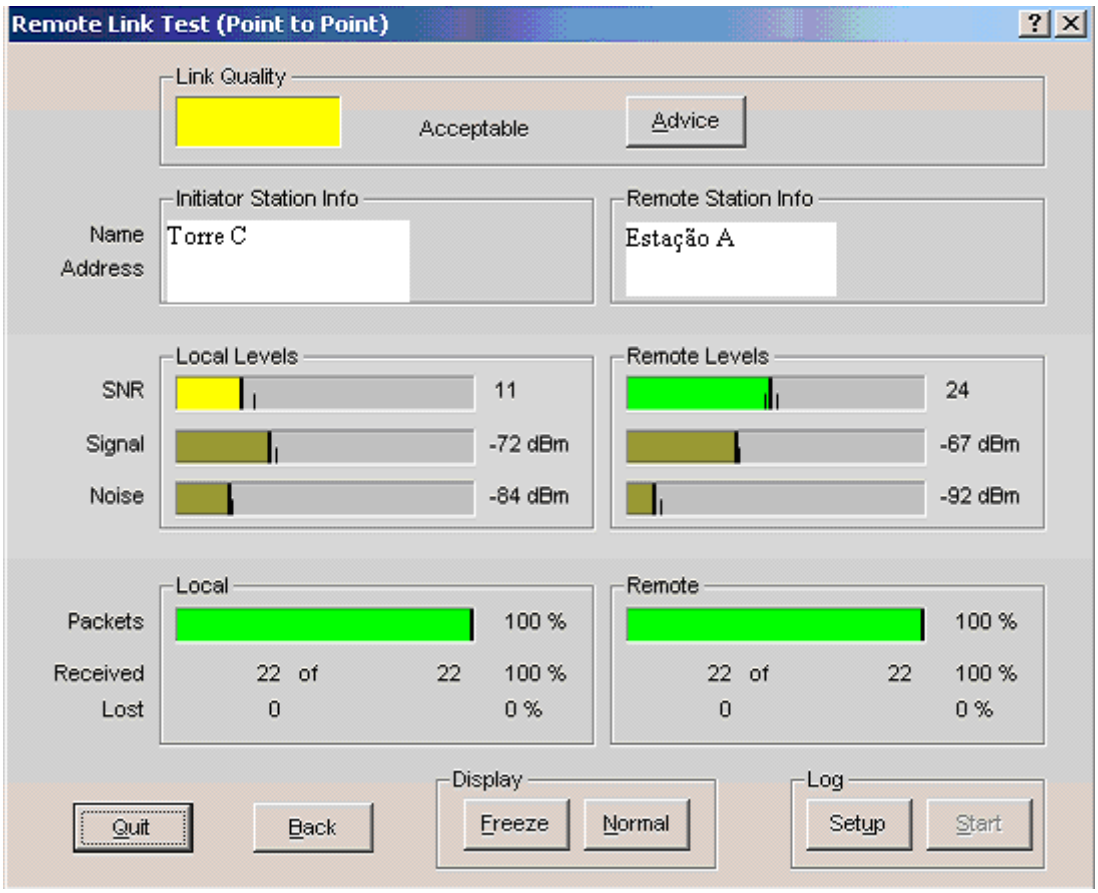

Figura 3. Teste do *link entre a Torres C e Estação A.*

A Figura 4 nos apresenta uma análise da variação de SNR em função do tempo que na ocasião foi escolhido um minuto. Foram alterados os *host names*

propositalmente por questões de segurança conforme apresentado na Figura 4. Percebemos que houve uma variação considerável em um pequeno intervalo de tempo. O gráfico representa o link teste da Figura 3 durante tempo de um minuto e pode-se confirmar que o SNR se manteve próximo de 11 para TORRE C onde havia um considerável ruído e próximo de 24 para Estação A, onde o sinal tinha uma melhor qualidade. Fica claro assim, que quanto maior o ruído pior será o sinal.

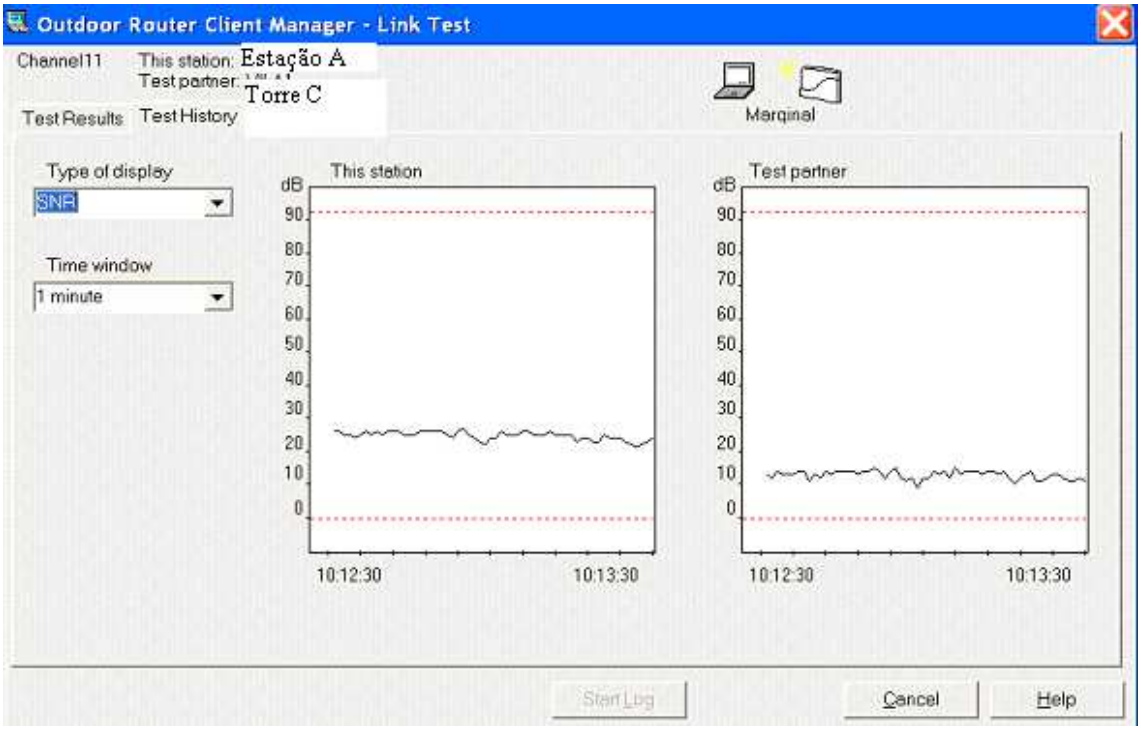

Figura 4. Gráfico de análise do SNR x Tempo entre *bridge* TORRE C e Estação A.

Como demonstrando anteriormente é possível gerenciar a qualidade do sinal de uma WLAN utilizando-se de ferramentas como o Orinoco. Esta análise é de suma importância para que se tenha uma maior segurança na rede no que se refere à banda disponível, tráfego de dados, qualidade do sinal, possibilitando assim inserções corretivas quando necessário.