Utilização da segurança das redes Wireless existentes na rede Mesh.

Wesley Silva Viana[1] , Luís Augusto Mattos Mendes[1]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil
[1]13dejaneiro@gmail.com, [1]luisaugustomendes@yahoo.com.br

Resumo: *A mobilidade, a praticidade, e as novas tecnologias surgindo com bastante rapidez, e a necessidade de se adaptação são cada vez maiores. O grande foco será a segurança implementada nas redes sem fio Mesh. Os tipos de redes, serviços, a aspecto da segurança. Os dados que trafegam no ar, os tipos de cifragem usada nos dados que estão trafegando, e a necessidade de cifrá-los. O funcionamento das redes Mesh, sua segurança, e uma melhor forma de proteção. As principais questões em relação à segurança em redes sem fio. Sendo assim, este artigo discute as questões de senhas, criptografia WEP, WPA, WPA2, padronização das redes Mesh, exemplos de redes Mesh, e a melhor forma de utilização da segurança da mesma.*

Palavras Chaves: redes Mesh, criptografia; autenticação; segurança em redes sem fio.

Introdução

As conexões sem fio, as tecnologias Wireless, prometem elevar a patamares nunca imaginados conceitos como conectividade e mobilidade, criando novos hábitos, relações e formas de trabalho, além de trazerem excelentes possibilidades tanto para o ambiente residencial quanto corporativo. Sempre estão surgindo novas tecnologias, sem falar nos novos equipamentos, e as novas chances de crescimento profissional. As redes sem fio transmitem dados utilizando sinais de rádio. Enquanto em redes com fio você precisa ter um acesso físico a algum ponto da rede para se conectar. Em uma rede sem fio, basta estar próximo a um ponto que tenha acesso a rede sem fio, para poder ter algum tipo de ataque ou fazer algum tipo de ação na rede. A tecnologia de redes sem fio está crescendo notavelmente nos últimos anos, conquistando ambientes corporativos e domésticos. Sua característica de mobilidade torna flexíveis as alterações necessárias para suprir melhor as necessidades dos usuários. Além da mobilidade necessária, a segurança das informações que circulam na rede também é um ponto de elevada importância para usuários domésticos, e empresas, necessitando assim de soluções mais adequadas.

As redes sem fio consistem em redes de comunicações por enlaces sem fio como rádio freqüência e infravermelho que permitem mobilidade contínua através de sua área de abrangência. [1].

Já para uma determinada WLAN (*Wireless Local Area Networks*), a segurança é um elemento necessário, assim como suas tecnologias, suas aplicações, bem como suas implantações e implementações. As propriedades de comunicação protegidas por redes sem fio são as seguintes: [2]

- Na autenticação antes de ser autorizada, acontece uma troca de dados em tráfego com a rede sem fio, o nó de rede sem fio tem que ser identificado e, dependendo

do método de autenticação, deve apresentar “credencias” para poder ser validado.

- Antes de enviar a integridade dos dados, um pacote de dado deve incluir as informações em pacotes, assim o receptor pode determinar que o conteúdo da embalagem não foi modificado na transmissão.

2 Mesh

A tecnologia Mesh, que será tratada na seção posterior, teve origem no DARPA (*Defense Advanced Research Projects Agency*), centro de desenvolvimento de tecnologia militar dos Estados Unidos. Com o objetivo de buscar uma rede que permitisse uma comunicação fim a fim, sem a necessidade de comunicação em um ponto central, ou seja, não depender de um único equipamento que tivesse pelo menos as seguintes características para realizar as certas atividades, como: Banda Larga; suporte IP fim a fim; suporte à transmissão de voz, dados e vídeo; suporte para posicionamento geográfico, sem a utilização de GPS. [3]

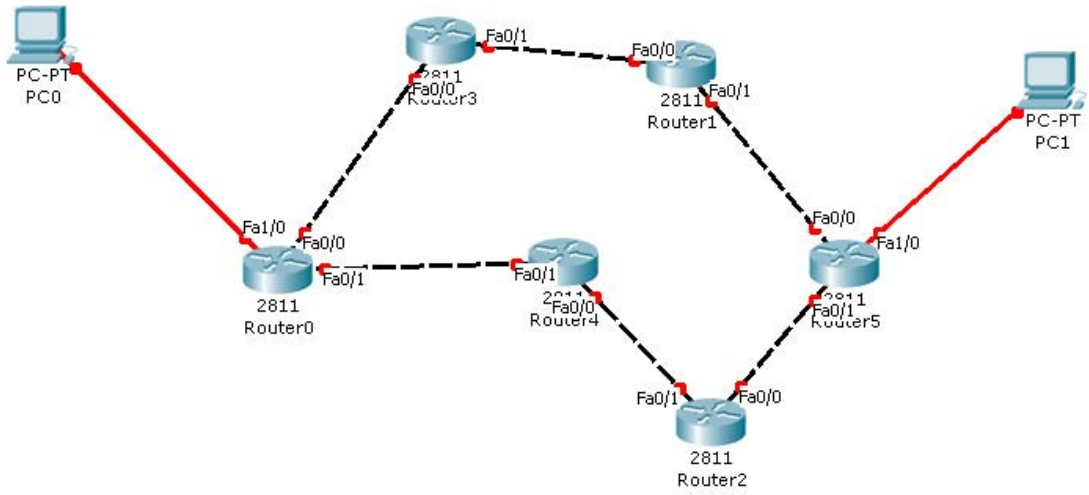

Figura 1 Mostra de uma rede sem um ponto central

A Figura 1 apresenta uma amostragem entre duas e mais redes, que são tipicamente uma rede Mesh. Uma comunicação entre dois computadores na rede internet poderá ocorrer, pacote a pacote, passando por diversos caminhos diferentes, absolutamente sem nenhuma hierarquia. Quando uma mensagem é enviada, ela não vai diretamente do emissor ao receptor. Ela é roteada de servidor a servidor, buscando o caminho mais eficiente.

Apesar de ainda pouco difundida, a tecnologia Mesh tem um grande potencial de se tornar uma das mais promissoras redes sem fio nas telecomunicações deste início de século XXI [3].

O segredo do sistema Mesh, está no protocolo de roteamento, que faz a varredura das diversas possibilidades de rotas de fluxo de dados, baseada numa tabela dinâmica, onde o equipamento seleciona qual a rota mais eficiente a seguir para chegar ao seu objetivo, levando em conta a métrica a ser utilizada, com menos perda de pacotes, ou acesso mais rápido à internet, além de outros. Esta varredura é feita centenas de vezes por segundo, sendo intransparente ao usuário.

2.1 Tecnologias Mesh

Uma rede Mesh apresenta diversos benefícios se comparada com uma rede Wireless tradicional. Dentre estes benefícios podemos citar: Aumento da distância entre a origem e o destino, sem prejudicar a taxa de transmissão. À medida que aumenta a distância entre dois pontos, à velocidade de transmissão diminui, de forma que não prejudique a garantia da qualidade de entrega dos dados transmitidos (mantendo-se as mesmas características de potência na saída das antenas). Com a rede Mesh esta limitação deixa de existir, pois sempre se pode utilizar de saltos através de nós intermediários, tornando assim a distância de cada salto compatível com a velocidade que se deseja transmitir; redução do custo da rede: Como uma rede Mesh utiliza também dos equipamentos dos próprios usuários como roteadores/ repetidores, a necessidade de equipamentos da própria rede diminui sensivelmente. [3]

A tecnologia Mesh é um tipo de infra-estrutura de internet descentralizada e de alta confiabilidade e disponibilidade, já que cada nó da rede precisa transmitir somente para o próximo nó. Estes nós trabalham como estações repetidoras, que transmitem dados entre si até chegar aos pontos mais difíceis de alcançar. A alta confiabilidade da rede está no fato de cada nó na rede, estar conectado a vários outros nós, possibilitando que, se um dele desconectar-se por qualquer motivo, os demais encontre outra rota.

2.2 Padronizações da rede Mesh

Atualmente a tecnologia Wireless Mesh está sendo desenvolvida por diversas empresas. Estes desenvolvimentos, apesar de serem, em muitos aspectos, aderentes a algumas especificações atualmente utilizadas, como a 802.11 e 802.16, apresentam diversos aspectos particulares e patenteados pelas empresas desenvolvedoras. [3]

Baseada em protocolos 802.11, ela suporta usuários finais padrão Wi-Fi, o 802.11 a/b/g/i.

2.3 Aplicações

São inúmeras as aplicações atualmente identificadas para uma rede wireless Mesh, dentre as quais citamos: [3]

- Criação de Hot-Zones de Wi-Fi como pode ser observada na Figura 2.[3]

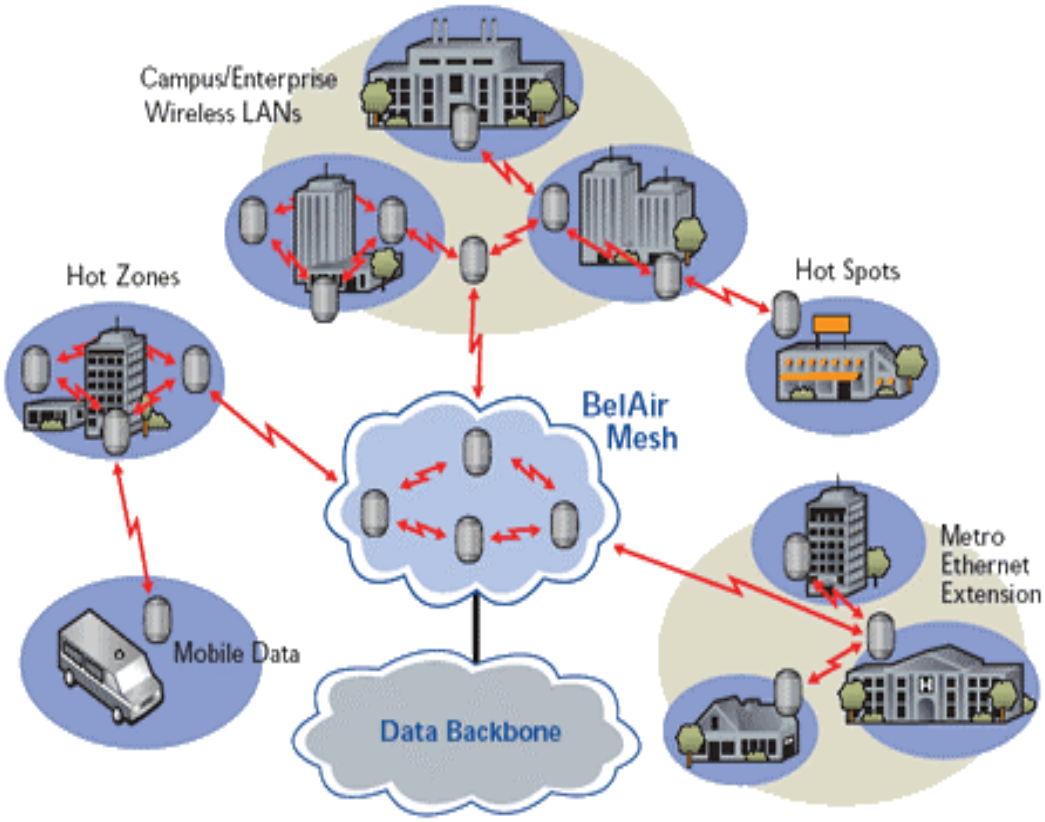

Figura 2 BelAir Networks Hot-Spot

Cada Hot-Spot necessita de um link para a Internet, o que dificulta a implementação econômica em pontos de baixa utilização.

Também a área de cobertura de um Hot Spot é limitada pela baixa potência dos Access Points. Utilizando-se da tecnologia Mesh, podem ser constituídas Hot-Zones (não simplesmente Hot-Spots), com a colocação de diversos AP(*Access Point*) em áreas adjacentes. A conexão com a Internet pode ser limitada, em função do tráfego, a um ou apenas a alguns dos Access Points. Com este conceito se expandido, permitirá se ter uma cobertura Broadband de grandes áreas, como o campus de uma universidade, ou mesmo pequenas e médias áreas urbanas. [3]

- Sistemas Inteligentes de Transporte como observado na Figura 3. [3]

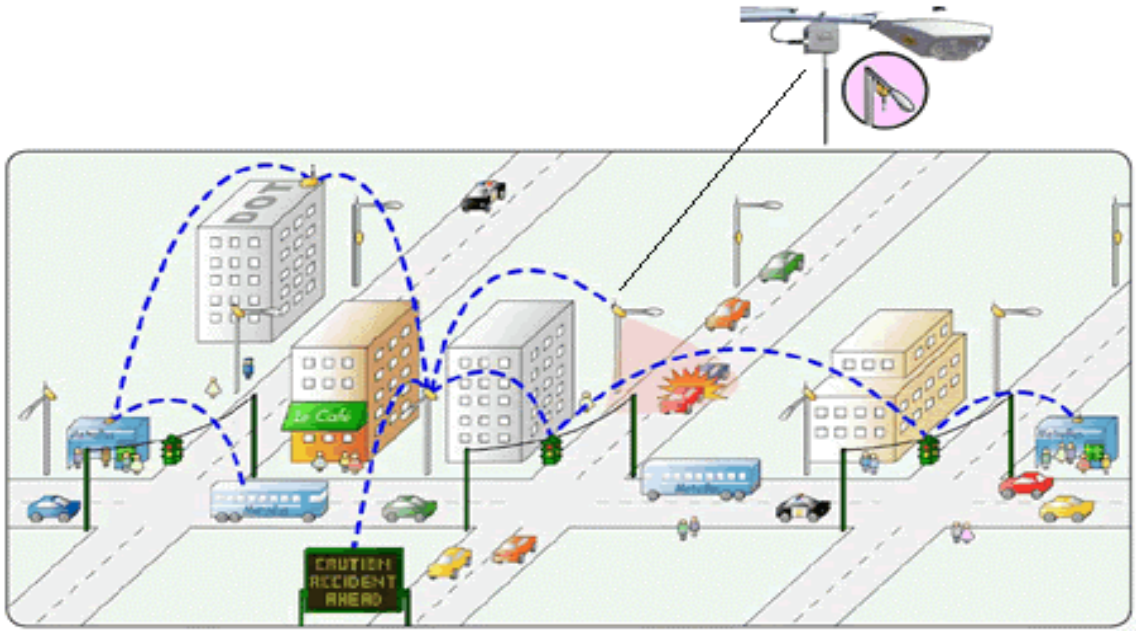

Figura 3 Sistemas Inteligentes de Transporte. [3]

Com uma rede Mesh instalada no curso das principais rotas de tráfego, diversas aplicações podem se tornar disponíveis, tais como: Controle da sinalização semafórica; controle de painéis luminosos de orientação de tráfego; informações aos usuários do transporte público sobre a situação dos coletivos de cada rota; gerência da frota de ônibus pelos concessionários; transmissão on-line das multas aplicadas pelos dispositivos automáticos de registro de infração; segurança Pública. [3]

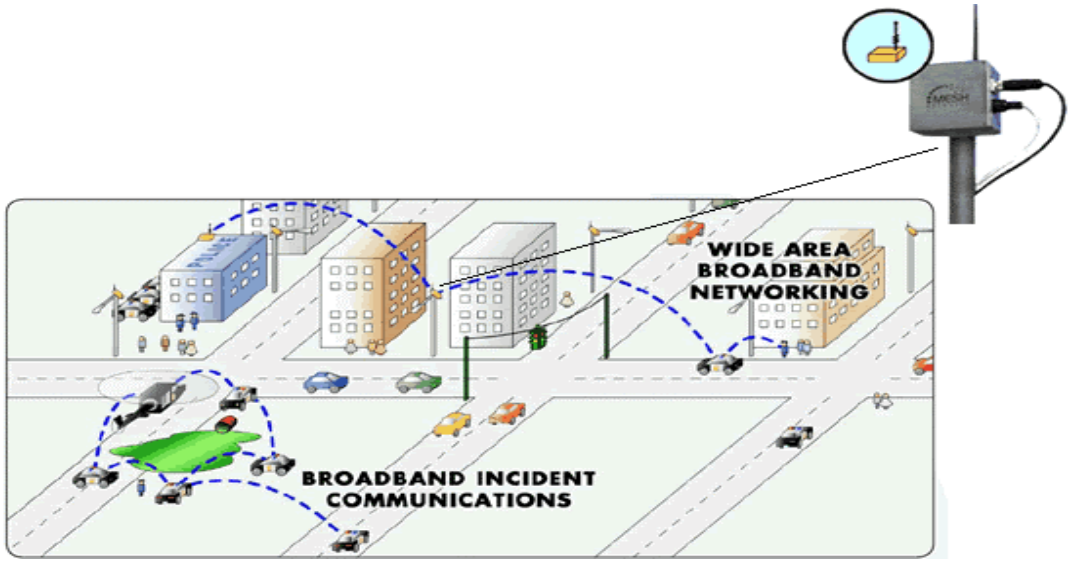

Figura 4 Segurança Pública. [3]

Com uma rede Mesh com cobertura em uma área metropolitana, além de um sistema de câmeras de vídeo, distribuído em pontos relevantes, todas as viaturas podem

ser equipadas com dispositivos de acesso à base de dados do órgão de segurança pública permitindo uma atuação online, na identificação de criminosos, de prontuário de motoristas e as diversas outras aplicações. Além de conectar todos os computadores existentes, também todos os outros equipamentos elétricos preparados para este fim, tais como iluminação, aquecimento, cozinha, dispositivos de segurança, etc. também poderão fazer parte de rede. [3]

2.4 Casos de Sucesso

Alguns exemplos de implementação da rede Mesh. Belair Networks Figura 2**.** **(**Ottawa, Ontário Canadá) - Implantação de uma rede de Hot-Zones pela prefeitura municipal. Status: o projeto foi implantado no início de 2004. [3]
Na cidade de Tiradentes – MG Figura 3 a cobertura do centro histórico com 4 pontos de acesso. Gerenciamento policiamento de tráfego e da banda, autenticação e Firewall, um modelo de negócio alto-sustentável em desenvolvimento. Acesso a internet de banda larga, Telefonia IP (âmbito da prefeitura), câmeras (IP Wireless) de vigilância, aplicativos educacionais (Metasys), Programa UCA (Intel).

A questão da segurança da rede Mesh de Tiradentes, é constituída em multicamadas, incluindo o IEE 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA, Advanced Encryption Estandard (AES) para criptografia dos links entre os rádios. Autenticação dos pontos de acesso, tráfego seguro entre os pontos de acesso e controle da rede.

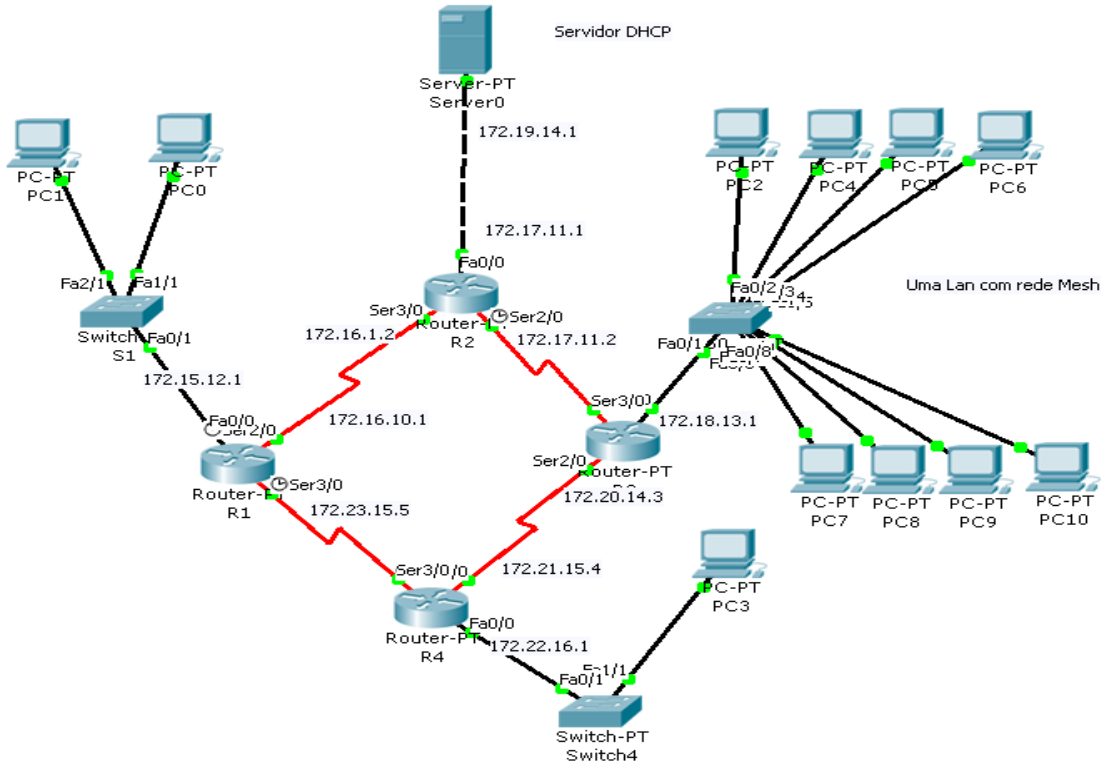

Figura 5 Exemplo de uma pequena rede Mesh – Simulação da Rede Mesh Tiradentes

Cidade Conservatória – RJ. Cobertura da cidade (Zona Urbana), 4 pontos de acesso gerenciamento, policiamento de tráfego e banda, autenticação e firewall. Projeto Remesh (Niterói)

2.5 Segurança

Discussões como, a autenticação, criptografia e integridade dos dados revelaram-se relativamente fraca e pesada para implantação em redes públicas e privadas. Posteriormente o presente documento descreve as normas complementares que fornecem métodos de autenticação mais forte e discutir melhorias para o inicialmente definido criptografia e integridade dos dados ou métodos substitutos para eles.

IEEE 802.11 define os seguintes tipos de autenticação: Sistema de autenticação Aberto; Shared Key Authentication.

- A Autenticação de Sistema Aberto

Sistema de autenticação Aberto, não fornece autenticação, apenas identificação, usando o endereço MAC (Media Access Control) do adaptador sem fio. O Sistema de autenticação utiliza os seguintes processos (mostrado na Figura 6):

Na autenticação sem fio, o cliente envia uma mensagem ao sistema aberto de Autenticação, que contém o endereço MAC como o endereço de origem.

O nó receptor, normalmente um ponto de acesso sem fio (AP), responde com mensagem a um sistema aberto que indica o sucesso (autenticação de iniciar o cliente sem fio está autorizado) ou fracasso.

.

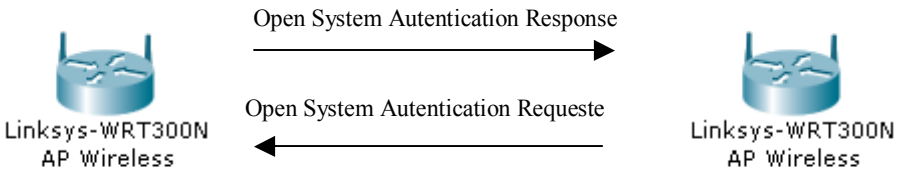

Figura 6 Sistema de autenticação aberto

Alguns APs permitem-lhe configurar uma lista de endereços MAC dos clientes sem fio que são autorizadas. No entanto, esta não protege uma rede sem fio, pois um invasor pode facilmente captar os pacotes de clientes ligados entre si e, em seguida, utiliza o endereço MAC válido como o seu próprio cliente sem fio. [3]

- Shared Key Authentication

Shared Key Authentication verifica que uma chave de autenticação tem conhecimento de um segredo compartilhado, às vezes conhecido como um código de acesso. O padrão IEEE 802.11 pressupõe que o segredo é compartilhado e entregue aos clientes participantes sem fio através de um canal seguro que é independente do IEEE 802.11.

Shared Key Authentication utiliza o seguinte processo mostrado na Figura 7. [3]

Utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. Um segredo é utilizado semente para o algoritmo de criptografia do WEP na cifragem dos

quadros. A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudo-randômicos.
3. A estação requisitante deve então mostrar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4. O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

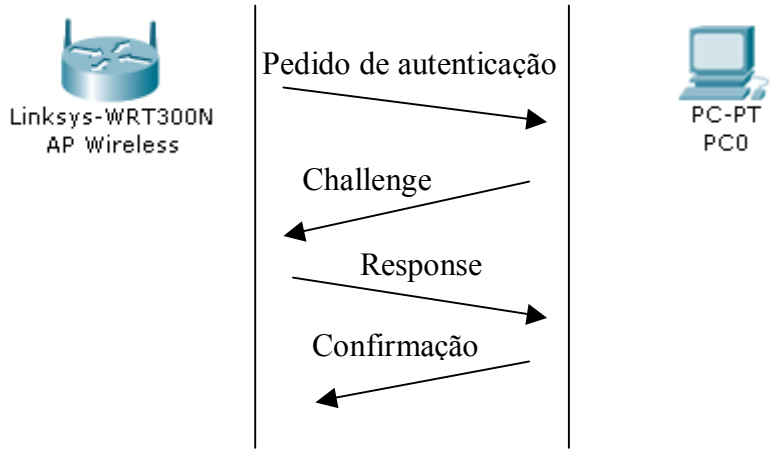

Figura 7 Shared Key Authentication [3]

- Criptografia e integridade dos dados

O propósito da criptografia é levar uma mensagem ou um arquivo chamado **texto plano,** e criptografa-lo em um **texto cifrado** de tal modo que somente a pessoa autorizada saiba convertê-lo novamente para um texto plano. Para todos os outros o texto cifrado é apenas um monte incompreensível de bits. Embora possa parecer estranhos aos iniciantes na área, os algoritmos (funções) criptográficos e de decriptação sempre devem ser públicos. Tentar manter em segredo nuca funciona e oferece às pessoas que estiverem tentando manter os segredos uma falsa sensação de segurança. [11].

A palavra Criptografia do grego "Kryptós" e "gráphein", que significam “ocultos” e "escrever", respectivamente. Trata-se de um conjunto de conceitos e técnicas que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. [3]

Na computação, as técnicas mais conhecidas envolvem o conceito de *chaves*, as chamadas "chaves criptográficas". Trata-se de um conjunto de bits baseado em um determinado algoritmo capaz de codificar e de decodificar informações. Se o receptor

da mensagem usar uma chave incompatível com a chave do emissor, não conseguirá extrair a informação. [3]

2.6 **WEP**

Surge então o WEP que traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP, também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID e a lista de endereço físico permitidos, também conhecido por endereço MAC (*Media Access Control*).

O *Wired Equivalency Privacy* (WEP), opera na camada de enlace de dados e fornece criptografia entre o cliente e o *Access Point*. O WEP é baseado no método criptográfico RC4 (*Route Coloniale* 4) da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (*secret shared key*) de 40 ou 104 bits. O IV é concatenado para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 (C*yclic Redundancy Check*) para calcular o *checksum* da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o *checksum* para garantir que a mensagem não foi alterada.

Wep começou a se tornar muito frágil, ao mesmo tempo em que foi se criando novos modelos de segurança para esse protocolo. A escalabilidade WEP, da maneira que foi concebida, tinha quer ser instalada manualmente em cada aparelho que fazia parte da rede, isso não escala muito quando se tem muitos aparelhos, isso gera um problema de gerencia muito grande. O protocolo vem sendo substituído pelo WPA.

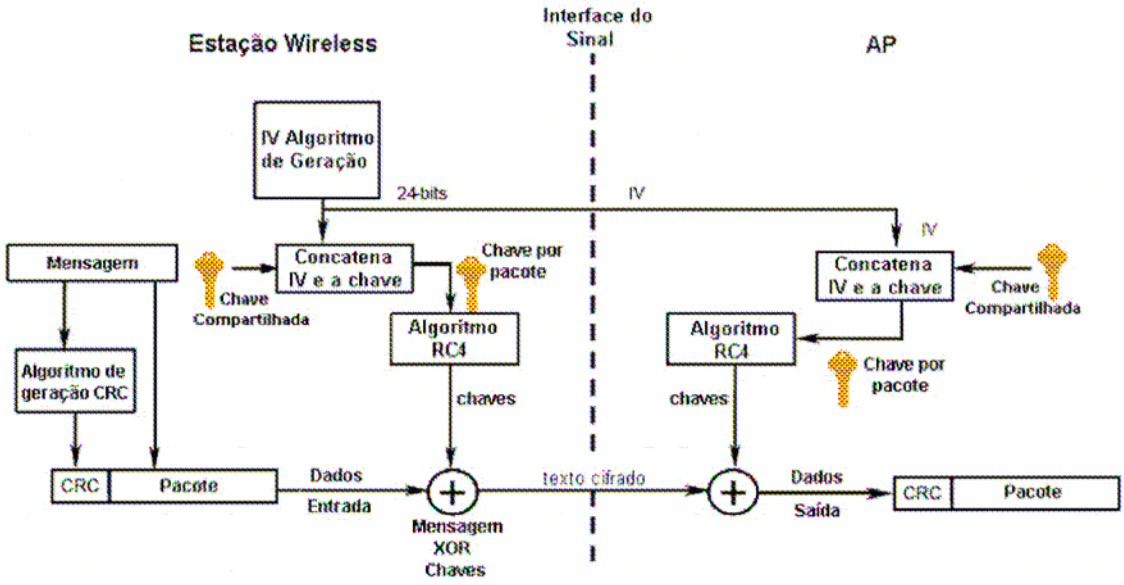

Figura 8 Exemplo de um processo de autenticação do protocolo WEP [4]

Alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação. Caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. O WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possuem falhas conhecidas e facilmente exploradas por softwares. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados. [5]

2.4.2 **WPA**

Com o passar do tempo, o mecanismo de segurança que se tinha pensado, que era o WEP, como sendo o mecanismo mais seguro, começou a se mostrar muito frágil, começaram-se a criar programas e paipers, discutindo sobre a fragilidade desse protocolo, então ao mesmo tempo em que foi se homologado os novos padrões, também foi se criando o novo modelo de segurança para esse padrão. O objetivo, a motivação, foi não só a segurança, mas a questão da escalabilidade, por que o WEP, da maneira que foi concebido, ele precisa ser manualmente ser instalado cada equipamento da rede, e isso não escala muito bem, pois quando se têm vários equipamentos em um ambiente corporativo, por exemplo, quando várias pessoas estão viajando, que placa da problema e tem que ser substituída, isso gera um problema de gerência muito grande.

Então o protocolo que veio substituir o WEP, que é chamada de WPA (Wi-Fi protected Accesses), ele foi pensando para resolver não só problema se segurança como o problema de escalabilidades, de novos usuários. Esse novo padrão ele foi concebido ao longo de 2 anos, mas foi homologado junto com IEEE 802.11, que é chamado de WPA, e é dividido basicamente em dois modelos: um que é chamado de WPA de chaves compartilhadas (Pré Shared Key), que trabalha de maneira similar ao WEP, que deve ser configurado manualmente em cada máquina que faz parte da rede, mas ele tem um novo padrão, que necessita que os usuários se autentiquem para poder usar a rede, e isso escala muito melhor, pois não necessita instalar em cada máquina uma chave WEP, você simplesmente cadastra um usuário na rede, como um servidor de autenticação da própria rede. [5]

2.4.2.1 **Mecanismos de Criptografia WPA**

O WPA (*Wi-Fi Protected Access*) possui diferentes modelos de segurança, adaptável ao tipo do uso em que ele será implementado. Uma para aplicações pequenas, como redes domésticas e pequenos escritórios, utilizando uma chave previamente compartilhada (Pré-shared key ou WPA-PSK), sendo responsável pelo reconhecimento do aparelho. Outro método é conhecido como infra-estrutura, adicionando um servidor RADIUS (*Remote Authentication Dial-In User Server – Serviço de Autenticação de Usuários Discados*) para autenticação, podendo ainda necessitar de uma infra - estrutura de chaves públicas (ICP), caso se utilize certificados digitais para autenticar usuários. [6]

O método de chave compartilhada é semelhante ao WEP, onde a troca de chaves é feita manualmente, fazendo com que seu uso se torne melhor adequado às redes pequenas onde os participantes estão acessíveis na maior parte do tempo. [6]

O protocolo TKIP (*Temporal Key Integrity Protocol*) é o responsável pelo gerenciamento da troca de chaves. No WEP as chaves eram estáticas e seu vetor de inicialização era de apenas 24bits, passando agora para 48bits. [6]

O TKIP pode ser programado para alterar o vetor de inicialização a cada pacote, por sessão ou por período, tornando mais difícil a obtenção do mesmo via captura de tráfego. [6]

Uma das vantagens em se utilizar equipamentos adicionais para a autenticação do usuário é de ter uma base centralizada, onde todos os métodos de acesso (não apenas *Wi-Fi*, mas cabeadas e/ou discadas também) utilizem a mesma forma, sem a necessidade de manter uma sincronização. No WPA também foi inserido em modelo para autenticação de usuários, conhecidos como EAP (*Extensible Authentication Protocol*), que utiliza o padrão 802.11x e permite vários métodos de autenticação, incluindo a possibilidade de certificação digital.

Uma das vantagens em se utilizar equipamentos adicionais para a autenticação de usuário é de ter uma base centralizada, onde todos os métodos de acesso (não apenas W*i-Fi*, mas cabeadas e/ou discadas também) utilizem a mesma forma, sem a necessidade de manter uma sincronização.

- **Criptografia WPA2**

Segundo a MICROSOFT [13], o WPA2 é uma certificação de produto disponível por meio da Wi-Fi Alliance que certifica equipamentos sem fio como sendo compatíveis com o padrão 802.11i. O WPA2 oferece suporte aos recursos de segurança obrigatórios adicionais do padrão 802.11i que não estão incluídos em produtos que oferecem suporte ao WPA. Com o WPA2, a criptografia é realizada com o AES (Advanced Encryption Standart), que também substitui o WEP por um algoritmo de criptografia bem mais forte. Como o TKIP do WPA, o AES permite a descoberta de uma chave de criptografia de difusão ponto a ponto inicial exclusiva para cada autenticação, bem como a alteração sincronizada da chave de criptografia de difusão ponto a ponto para cada quadro. Como as chaves AES são descobertas automaticamente, não há necessidade de se configurar uma chave de criptografia para o WPA2. O WPA2 é a modalidade de segurança sem fio mais forte. [6]

Como talvez não seja possível agregar suporte AES por meio de uma atualização de *firmware* ao equipamento existente, o suporte a AES é opcional e depende do suporte ao *driver* do fornecedor. [6]

- **EAP**

A seleção do método de autenticação necessário para sua empresa pode ter um efeito significativo sobre a infra-estrutura que sua solução exige. O padrão 802.1X utiliza um esquema de autenticação conectável denominado EAP (*Extensible Authentication Protocol* - Protocolo de Autenticação Extensível). [6]

A autenticação 802.1X por senha é suficiente para empresas pequenas que não possuem atualmente uma infra-estrutura de certificado adequada e não precisam de certificados para outras finalidades.

Como alternativa, a autenticação 802.1X por senha pode ser vista como uma tecnologia provisória para a obtenção do controle de acesso 802.1X à WLAN durante o planejamento de uma infra-estrutura de certificado futura. No entanto, os custos

envolvidos na aquisição de um ou mais certificados de servidor de um terceiro confiável devem ser ponderados com cuidado em comparação com o valor que uma infra-estrutura de certificado poderá trazer para uma empresa. Estas orientações foram desenvolvidas para ajudá-lo a obter uma solução de autenticação de cliente por certificados que usa o EAP-TLS (*Encripted System Files - Transport Layer Security*) com custo e esforço mínimo.

Há um caso especial na implementação do IEEE 802.1X. Em ambientes pequenos, um servidor de autenticação pode não estar disponível, então uma chave pré-estabelecida é usada. A chave é de conhecimento do suplicante e do autenticador. Uma autenticação parecida com a que acontece no WEP então é feita entre esses dois participantes. [6]

- O suplicante - Um usuário ou um cliente que quer ser autenticado. Ele pode ser qualquer dispositivo sem fio.
- O servidor de autenticação - Um sistema de autenticação, tipo RADIUS, que faz a autenticação dos clientes autorizados.
- O autenticador - O dispositivo que age como um intermediário na transação, entre o suplicante e o servidor de autenticação. O ponto de acesso, na maioria dos casos.

2.7 Criptografia Quântica

A criptografia quântica tem como característica principal o fato da sua segurança estar baseada em características físicas intrínsecas da natureza. Devido a isso, hoje ela aparece como a principal alternativa à criptografia clássica atualmente utilizada, e cuja segurança esta baseada, em última análise, na falta de recursos computacionais. O estudo que está sendo realizado aborda inicialmente os tópicos em física quântica, necessários para o entendimento dos protocolos de criptografia; uma revisão dos principais algoritmos de criptografia clássica; estudo dos protocolos de criptografia quântica que envolvem fótons únicos e as propostas alternativas dessa área que são os protocolos que envolvem variáveis continuas (estados coerentes contendo muitos fótons). A segurança deste protocolo esta baseada na condição da chave em variáveis relacionadas ao campo eletromagnético que não podem ser medidas simultaneamente com precisão absoluta (quadraturas do campo). Nosso objetivo final é o desenvolvimento de uma simulação computacional de um protocolo de variáveis contínuas utilizando a luz laser (estados coerentes). Através desta simulação será possível investigar o funcionamento deste protocolo em diversas situações, assim como verificar a ação de um possível espião. [7]

3. Considerações Finais

A preocupação com os dados que trafegam em uma rede sem fio é uma questão muito discutida entre diversos profissionais da área. Apenas a restrição ao acesso à rede não é o suficiente, é necessário também manter seguro os dados que trafegam nessa rede.

A percepção que temos é que, cada vez mais as empresas estão trabalhando de forma remota, seja em viagens a trabalho, no hotel, em casa, etc. As tecnologias de infra-estruturais atuais tornam isso possível. Por outro lado, isso e influenciado cada vez mais por serviços oferecidos de forma interrupta.

A tecnologia Wireless não é menos ou mais segura que a tecnologia convencional cabeada. A tecnologia sem fio é mais simples de ser instalada e configurada, isso a torna mais fraca no aspecto que pessoas às colocam para funcionar, não colocam mecanismos confiáveis para que a rede se torne mais segura.

No caso de ambientes corporativos, a segurança esta ligada aos mecanismos de segurança. Contudo entra a questão de configuração e mecanismos de segurança apropriados para aquele ambiente, à medida que ela adota as medidas de segurança disponíveis para rede, e testam esses mecanismos, a empresa poderá se sentir segura da mesma forma que uma rede cabeada. A necessidade do uso de rede Wireless em um ambiente corporativo faz com que as pessoas com baixo nível de conhecimento, acabem prejudicando a segurança de uma determinada rede, pois a instalação e configuração de um AP (*Acesses Point*), por exemplo, não é algo complicado de se fazer, e isso faz com que possa a vir prejudicar todo um trabalho que foi desenvolvido por pessoas especializadas para fazer todo o mecanismo de segurança adequada para aquela rede. As empresas têm que se preocupar com as políticas de seguranças implantadas por elas, pois a definição de estratégia de implementação, normas, têm que se adequar a essa nova realidade que a empresa virá a se tornar.

Para empresas médias, o ideal seria primeiro estabelecer uma política para se defender contra possível ma utilização dessa tecnologia. Os procedimentos normais de homologação de Hardware e Software dentro da empresa, e em paralelo, já ir estudando a tecnologia para ver o que tem de novo, quais são as novas funcionalidade disponíveis para manter a segurança de uma rede sem fio e quais diz respeito à empresa, qual o método que ela irá usar para ficar mais próximo do que já se usa hoje.

O uso correto de medidas de segurança, protocolos adequados para os devidos serviços de rede sem fio, é o grande segredo para um bom sistema. Dentre todos os protocolos, métodos de criptografia apresentado por cada um, as diferenças são evidentes, pois cada um com sua característica e forma de ação para um determinado serviço, pois dependendo do tipo de serviço adotado por certa empresa, trará mais benefícios que prejuízos.

A rede Mesh, esta com um potencial muito grande de evolução. Para alguns, como sendo a tecnologia Wireless mais bem aceita, levando-se em conta todas as suas características de implantação e custo/benefício. A segurança a ser implanta nesse tipo de serviço não foge dos padrões atuais, pois o mecanismo de criptografia implementado serão os mesmos. O grande diferencial da Mesh em relação às outras rede Wireless, esta na sua forma de trabalho. O fato de não ter um nó central para fazer todo o roteamento da rota, faz da Mesh, seu grande diferencial em relação às outras redes Wireless.

Na cidade de Tiradentes-MG, ponto onde se trabalha com a rede Mesh, é utilizado equipamentos da empresa CISCO, equipamentos esses que trabalham de forma

que não fogem das características de uma rede Mesh. Com baixo custo, fácil manutenção, e que usam protocolos, tanto de criptografia quanto de roteamento, para determinar a melhor forma de implementação da mesma.

Um bom administrador de rede, e/ou uma empresa que preze por uma boa segurança, sempre estará atenta(o), às melhores formas de proteção para sua rede. Formas de proteção que vão, deste uma simples configuração de Firewall e/ou Antivírus, até os mais elevados patamares de protocolos de criptografia. Estar sempre atento as novas tendências do mercado é um fator primordial quando se fala nos melhores mecanismos de proteção de dados.

4 **Bibliografia**

[1] BEZERRA, Fábio Fernandes. Monografia apresentada como conclusão do curso De Engenheiro de Telecomunicações, assunto: Ferramenta de Análise Modal De Protocolos de Segurança para Redes Sem Fio. Universidade Regional de Blumenau, 2004.

[2] MICROSOFT. IEEE 802.11 Wireless LAN Securities with Microsoft Windows. Disponível em:<http://www.microsoft.com/downloads/details.aspx?FamilyID=67fdeb48-74ec-4ee8- 650-334bb8ec38a9&displaylang=en>. Acessado em 20 de Maio de 2008.

[3] RODRIGUES, Edson Duffles Teixeira. Tutoriais Banda Larga e VOIP. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialwmn/pagina_1.asp >>. acessado em: 03 de Junho de 2008.

[4] MAIA, Roberto. Segurança em Redes Wireless. Disponível em: < http://www.gta.ufrj.br/seminarios/semin2003_1/rmaia/802_11i.html>. Acessado em 20 de Novembro 2008.

[5] RUFINO. Nelson Murilo. Consultor de Segurança, e Consultor de Rede Sem Fio: Criptografia. Disponível em:<http://firewall.powerminas.com/seguranca-em-redes-wireless-parte-05-criptografia/> acessado em 10 de Junho de 2008

[6] MICROSOFT. Decisão sobre Uma Estratégia de Rede Sem Fio Protegida. 2004. Disponível em:<http://www.microsoft.com/brasil/security/guidance/topics/wireless/secmod168.mspx >. Acessado em 20 de Novembro 2008.

[7] INTERNO DE INICIALIZAÇÃO CIÊNTIFICA DA UNICAMP. XIII, 2005, Campinas-SP. Simulação de Um Protocolo de Criptografia Quântica

[8] WIKIPÉDIA, a Enciclopédia Livre. Redes Mesh. Disponível em: http://pt.wikipedia.org/wiki/Redes_Mesh. Acessado em 05 de Junho 2008.

[9] TANENBAUM, Andrew S. Sistemas Operacionais Modernos. 2ª Ed. 2005.695.

[10] REDES WIRELESS, Segurança em rede Wireless. Mauá Disponível em: <http://www.scribd.com/doc/4750980/Redes-WIRELESS>. Acessado em: 19 de Novembro 2008.

[11] MICROSOFT. Visão Geral da atualização de segurança WPA sem fio no Windows XP. 2005. Disponível em:<http://support.microsoft.com/kb/815485/pt-br>. Acessado em 16 de Outubro de 2008.

[12] COELHO, Jorge. CONIP: *Cidades Conectadas.* Disponível em: < http://www.conip.com.br/conip2007/palestras/Sala_3/JorgeCoelho.pdf >Acessado em 3 de junho de 2008.
[13] TANENBAUM, Andrew S. Redes de Computadores. 4ª Ed. 2003. 955.
[14] BOWMAN, Barb. Segurança Sem Fio WPA: Rede Domestica. Disponível em: <http://www.microsoft.com/brasil/windowsxp/using/networking/expert/bowman_03july28.mspx> Acessado 12 de Abril de 2008.