Antecipação do *Handover* em Redes IEEE 802.16 Seguras

Tássio Carvalho[1], Valber Souza[2], José Jailton[3], Kelvin Dias[1,2,3]

[1]Programa de Pós Graduação em Engenharia Elétrica, [2]Faculdade de Engenharia da Computação, [3]Programa de Pós Graduação em Ciência da Computação – Universidade Federal do Pará – Belém, PA – Brasil
tassioccarvalho@yahoo.com.br, {valbersouza, jjj, kld} @ufpa.br

Abstract. This paper presents simulation results showing that the performance of applications are degraded during handovers as the subscriber station has to re-authenticate with the new base station, damaging the QoS of applications for these processes. Furthermore, in order to reduce the impacts on the performance of SS applications in the aforementioned scenarios results, we proposed and evaluated a technique that anticipates horizontal handover in a transparent way in WiMAX networks.

Keywords: handover, re-authenticate, QoS, WiMAX.

1 Introdução

Redes metropolitanas sem fio (WMANs) de alta velocidade tem sido alvo de inúmeras pesquisas como alternativa de conectividade à Internet em relação às tecnologias de conexão via cabo. Dentre os padrões de redes metropolitanas, destaca-se o IEEE 802.16 (WiMAX), um padrão de rede de alta velocidade e com controle distribuído para serviços múltiplos. Esse tipo de WMAN permite mobilidade a seus usuários, de acordo com a emenda 802.16e.

Desde a sua concepção, o WiMAX já tem implícito técnicas de segurança e criptografia através de um processo de autenticação de uma estação cliente que entra na rede e de um processo de gerência de chaves de criptografia e autenticação de dados PKM (Privacy Key Management).

Este artigo mostra que o processo de autenticação pode degradar o processo de *handover* (ou *handoff*). O *overhead* pode prejudicar os requisitos da qualidade de serviço das aplicações envolvidas no processo porque, sempre que o mesmo ocorrer, é necessário que a estação assinante (SS) se re-autentique a nova estação base (BS).

Para isso, apresentamos uma estratégia para amenizar esse problema através da utilização de uma técnica de predição de *handover*. Através de dados probabilísticos e das condições espaciais atuais do cliente, é possível supor de antemão a troca de estações rádio-base e antecipar o processo de conexão com a estação alvo.

Nesta seção, abordamos uma introdução as propostas do artigo. Na seção II abordaremos o padrão IEEE 802.16 e sua organização. Na seção III dissertamos sobre a autenticação no padrão deixando para a seção IV a explanação da proposta. A seção V trata dos cenários e dos resultados das simulações. Na última seção, as conclusões.

2 Padrão IEEE 802.16

O WiMAX (Worldwide Interoperability for Microwave Access) possui faixas de freqüência entre 2 e 70 GHz, taxas de transmissão que podem chegar a 70 Mbps em condições ideais e atingem uma área de cobertura que pode chegar a 50 Km, atingindo dessa forma a "última milha" [1].

A propagação de seus sinais pode acontecer com ou sem visada direta: Em LOS (*Line-of-Sight*) o sinal precisa ser propagado em espaço consideravelmente desobstruído (zona de *Fresnel*) e com freqüência acima dos 10 GHz e no NLOS (*Non-Line-of-Sight*) o sinal precisa ser propagado sobre reflexão, difração, dispersão temporal e interferência e com freqüência inferior a 10 GHz. A segunda é a situação mais comum em redes sem fio [2].

A arquitetura do padrão IEEE 802.16 é estruturada em duas camadas principais: a camada MAC (Medium *Access Control*) e a camada física. A camada MAC é subdividida em três subcamadas: a MAC Convergence, que prepara os protocolos das camadas mais altas para a transmissão; a MAC Common Part, que aborda o estabelecimento de conexão dos clientes e a MAC Privacy (subcamada de segurança). A última é encontrada logo acima da camada física e é responsável pela autenticação, pela criptografia dos dados e pela garantia da autenticidade do usuário.

2.1 Segurança e Handover

As falhas de segurança surgem com a quebra de um ou mais aspectos de comunicação entre dois ou mais nós e ao contrário de outros sistemas sem fio, o WiMAX usa autenticação de chave pública e criptografia para validar as credenciais da estação assinante [3].

Mecanismos de segurança precisam garantir que os dados do usuário não possam ser interceptados nem decodificados por ninguém além da rede e do usuário que "escutam" na interface aérea. A fim de proteger os dados transmitidos, a criptografia é usada com uma chave cifrada individual por usuário [3].

Devido ao forte processo de segurança e criptografia, e a obrigatoriedade da autenticação de uma SS junto à rede, esta sofre um grande impacto quando executa um procedimento de *handover* caracterizado pela mobilidade e conseqüentemente a migração de uma SS da área de cobertura de uma BS a outra (Fig. 1.).

Para um melhor desempenho deste procedimento e visando compensar o impacto e o atraso correspondente ao processo de criptografia e autenticação sempre que uma SS se transferir de uma BS a outra, se faz necessário antecipar o *handover*, de forma a compensar o tempo perdido pela SS para se re-autenticar a nova BS além de prover de forma transparente a continuação da conectividade do usuário durante a migração.

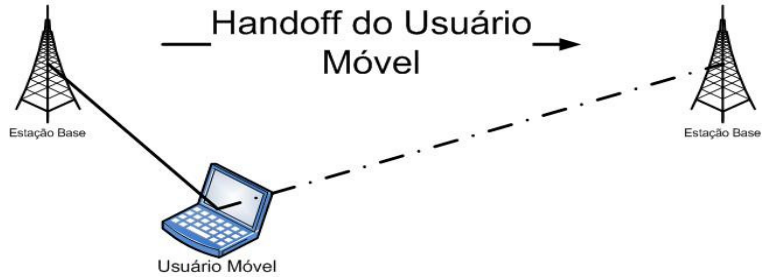

Fig. 1. *Handover* (ou *Handoff*) de uma estação assinante (SS) de uma BS a outra.

3. Autenticação no IEEE 802.16e

A autenticação é garantida durante o procedimento de entrada na rede e permanece em funcionamento protegendo os dados transmitidos através de criptografia.

A subcamada de segurança fornece operadores com forte proteção contra roubo de serviço e emprega um protocolo autenticado de gerenciamento de chave Cliente/Servidor em que a BS, controla a distribuição de chaves para a SS assim como provê a criptografia do fluxo de serviços associados através da rede.

A arquitetura dessa subcamada é dividida em dois protocolos: O protocolo de encapsulamento responsável pela criptografia dos pacotes de dados através de redes fixas BWA (broadband wireless access) e o protocolo de gerenciamento de chaves de privacidade (PKM) que permite uma distribuição segura de chaves de dados da BS para a SS [4].

3.1 Conexão com a Rede

À SS cabe a responsabilidade de detectar o sinal transmitido pela BS e se conectar a ele. Para estabelecer a conexão, a SS precisa passar por seis passos. No primeiro passo, de sincronização, a SS recebe em *broadcast* as mensagens DCD, UCD, DL-MAP e UL-MAP que contém a descrição dos canais de *downlink* e *uplink* tal como um mapeamento dos aparelhos aos quais os dados serão enviados.

Nos cinco demais passos, as respectivas mensagens serão trocadas com o objetivo de estabelecer o tamanho da área de contenção base (RNG-REQ e RNG-RSP); de

estabelecer a conexão inicial e as informações básicas de capacidade como a modulação, codificação e meios de transmissão (SBC-REQ e SBC-RSP); de estabelecer o processo de autenticação (PKM-REQ e PKM-RSP) através do certificado X.509 e do funcionamento de uma máquina de estados (FSM) verificando a identidade do cliente e criptografando seus dados; o processo de registro na rede (REG-REQ e REG-RSP) e a criação do fluxo de serviços iniciais da mesma (DSA-REQ, DSA-RSP e DSA-ACK) [3] (Fig. 2.).

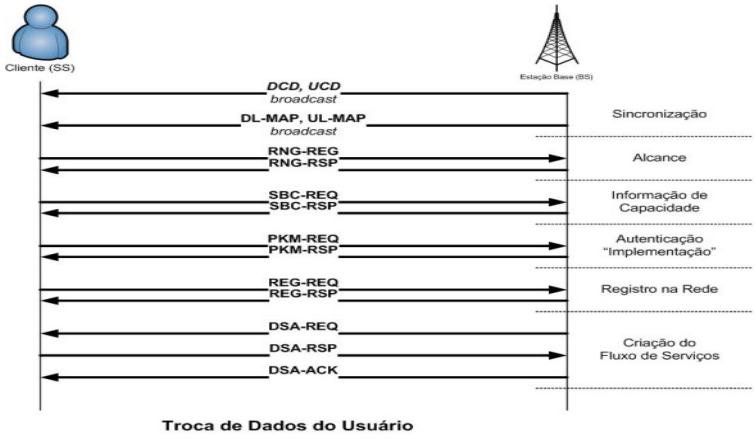

Fig. 2. Mensagens de entrada na rede.

3.2 Protocolo PKM e FSM

A autorização da SS é controlada por uma máquina de estados de autenticação e é um processo onde a BS garante a autenticidade de uma SS. A BS autentica uma SS através de uma chave de autenticação (AK, authorization key), da qual é derivada uma chave de criptografia de chaves (KEK, key encryption key), utilizadas para a transferência segura das chaves de criptografia de tráfego (TEK, traffic encryption key), sendo estas últimas as chaves que criptografam os dados dos fluxos de serviço.

A máquina de estados da autorização consiste de seis estados que representam os pontos onde a máquina de estados finitos (FSM, finite state machine) pode se encontrar: *Start, Authorize Wait (Auth Wait), Authorized, Reauthorize Wait (Reauth Wait), Authorize Reject Wait (Auth Reject Wait) e Silent*; e oito eventos distintos (incluindo o recebimento de mensagens) que podem acionar transição de estados: *Communication Estabilished, Auth Reject, Perm Auth Reject, Auth Reply, Timeout, Auth Grace Timeout, Auth Invalid e Reauth* (Fig. 3.).

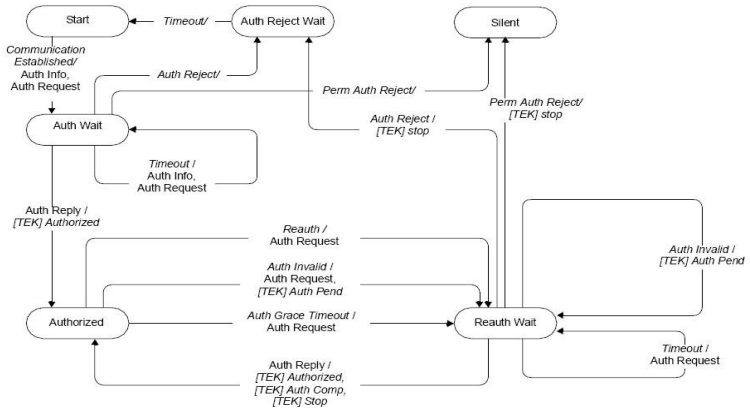

Fig. 3. Diagrama de Fluxos da FSM de Autorização [5]

3.3 Certificado X.509

O certificado X.509 é utilizado pela estação assinante durante o processo de autenticação com o objetivo de prover uma confidencialidade adicional à mesma através de um par de chaves públicas e privadas [6]. A criptografia do mesmo é feita através do algoritmo RSA, deixando os algoritmos AES ou DES para criptografarem as mensagens de autenticação e os demais dados trocados posteriormente pela rede.

Um certificado garante a estação assinante sua identidade tal como sua autenticidade. Esse certificado digital é composto por diversos campos que permitem a identificação do usuário certificado e da autoridade certificadora, além de parâmetros referentes a algoritmos e procedimentos usados no processo de certificação. Ele é assinado digitalmente e garantido por uma autoridade de certificação (CA). Esse método funciona seguindo os conceitos de chave pública e privada.

O certificado X.509 age dentro da troca de mensagens PKM, responsáveis por esse processo. Neste, o fabricante recebe um certificado da CA que contém um endereço MAC e uma chave pública. Assim, durante a autenticação, a SS envia o certificado para a rede (BS). A rede possui a chave pública da CA e pode assim verificar o certificado. A estação assinante é assim autenticada e a chave pública do cliente (SS) contida no certificado é usada para criptografar as demais mensagens do processo de autenticação.

Essa chave pública é utilizada para criptografar uma chave de autenticação (AK). Essa chave é enviada para a estação assinante que irá descriptografar a mesma através de sua chave privada. A estação assinante então gerará uma chave de criptografia de chaves (KEK) através da AK e requisitará junto à estação base (BS) uma chave de encriptação de tráfego (TEK) para dados de usuário. Para finalizar esse processo de

autenticação, a BS enviará a TEK criptografada com a KEK que será descriptografada pela estação assinante (Fig. 4.). Neste momento, o processo de troca de mensagens PKM está encerrado e todos os dados trafegados pelo cliente serão criptografados através da TEK, garantindo desta forma uma autenticidade da SS assim como uma proteção maior dos dados, passando maior confiança aos clientes WiMAX [7].

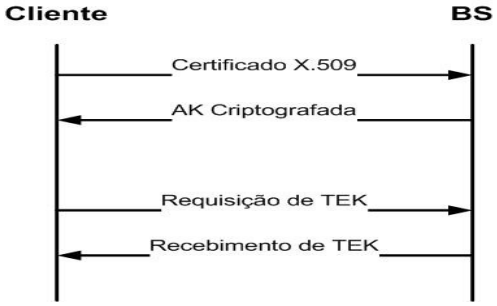

Fig. 4. Autenticação e Troca de Chaves

3.4 Política de Antecipação de Handover

Para prover qualidade de serviço (QoS) tratando de forma transparente a antecipação do *handover*, duas métricas de decisão de disparo de sinalização são utilizadas: a velocidade da estação assinante móvel e a probabilidade da conexão cair. A velocidade é obtida através de um GPS (Global Position System) instalado na SS móvel que a repassa para a atual BS. O GPS é de suma importância para a antecipação do *handover,* pois a idéia é determinar qual o melhor instante para disparar o processo de *handover* para que o mesmo seja transparente ao usuário. A probabilidade da conexão cair é obtida através das informações da camada física a respeito da intensidade do sinal.

Existe uma probabilidade do *link* cair em relação a proporção de sua mobilidade. Os processos são disparados de acordo com a mobilidade e com a probabilidade da conexão falhar, variando em 90%, 70% e 50% respectivamente quando as mobilidades forem baixas, moderadas e altas.

A predição do handover não compromete o mecanismo de segurança, ela só antecipa o processo (associação e autenticação) fazendo com que este ocorra antes, compensando desta forma o atraso do mecanismo.

4 Simulação

Para executar os testes deste artigo, nos utilizamos do *Network Simulator* (*ns*) [8], que se encontrava**,** no momento inicial de nossas simulações**,** em sua versão 2.30. Utilizou-se a extensão do WiMAX desenvolvida pelo NIST [12] para o *ns-2* para a execução de nossas simulações.

Para executar nossos testes, criamos uma extensão em C++ das trocas de mensagens PKM citadas anteriormente, assim como a máquina de estados FSM para prover esse processo de autenticação, as funcionalidades para antecipar o *handover* e a criptografia das mensagens do processo de autenticação e de sua certificação, sendo este último implementado através da biblioteca *Crypto++* [13]. Para a criptografia dos dados e das mensagens nos utilizamos do algoritmo AES com 256 *bits* e do RSA para o certificado X.509.

4.1 Cenários

Para avaliar o desempenho de uma rede WiMAX dentro de nossa proposta precisamos avaliar a vazão da mesma e verificar o funcionamento dela sem as nossas extensões e posteriormente com elas. Desta forma, podemos observar, mensurar e postergar resultados demonstrados graficamente que provam o atraso sofrido devido ao processo de autenticação e qualificam a estratégia de predição do *handover* que além de dar ao cliente maior QoS, inibe a necessidade do mesmo ter de se re-autenticar sempre que necessitar mudar de rede (BS).

Fez-se uso em todos os cenários de tráfego CBR (Constant Bit Rate), pacotes de tamanho de 100 bytes, atrasos máximo de 1*ms*, BS's com áreas de cobertura de 120 metros, áreas de sombra entre as mesmas com 18 metros e um nó fixo ligado à BS através de cabos para funcionar como receptor dos pacotes que serão trafegados através da estação base a partir da estação assinante WiMAX. Este nó será representado por um computador convencional nos dois cenários mostrados a seguir.

Em nosso primeiro cenário (Fig. 5.), temos uma estação assinante WiMAX fixa dentro da área de cobertura de uma estação base correspondente.

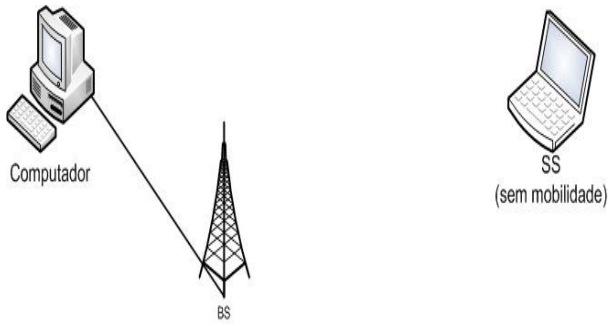

Fig. 5. Cenário 1, sem mobilidade

Em nosso segundo cenário (Fig. 6.), temos quatro estações base A, B, C e D e uma estação WiMAX móvel que executa um processo de *handover* entre as quatro (partindo da BS A rumo a BS D) com velocidade constante de 10 m/s. Ao chegar na última BS, a estação assinante móvel volta para a anterior onde estabiliza (BS C).

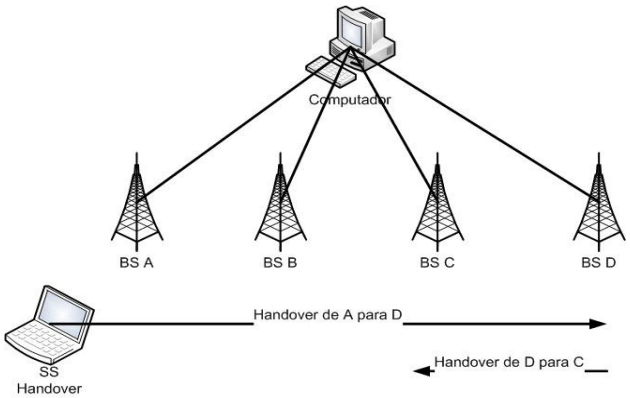

Fig. 6. Cenário 2, com mobilidade e *handover*

4.2 Resultados

Nos dois cenários aqui citados e em diversos testes realizados, verificamos que o tempo utilizado pelo processo de autenticação e criptografia das mensagens degrada a vazão e o desempenho das BS's sempre que esta necessita autenticar uma SS. Os tempos mensurados para criptografar e descriptografar o certificado, a AK e a TEK foram obtidos mediante a média de 500 simulações e costuma aumentar proporcionalmente ao aumento do número de usuários que necessitam adentrar e se autenticar junto à rede.

Como proposta, para suavizar um atraso superior decorrente de tais processos, vingaria a antecipação do *handover* não apenas como QoS, mas também como uma forma de minorar este atraso, decorrente do processo de autenticação e criptografia.

No entanto, o impacto causado por tais processos decorreram de problemas ainda maiores quando a quantidade de usuários é aumentada gradativamente, chegando assim a atrasos consideravelmente drásticos.

No primeiro cenário (Fig. 7.) desprezamos o atraso correspondente pelo processo de criptografia e autenticação na amostragem gráfica devido se tratar de apenas um usuário e este não ser grande em relação à amostragem intervalar de 0,5 segundos.

Verificamos uma vazão constante e máxima após o período inicial de autenticação e da troca de mensagens criptografadas, tal como a entrada por parte de uma SS estática à rede. Nota-se que a vazão permanece constante até o final do tempo de simulação.

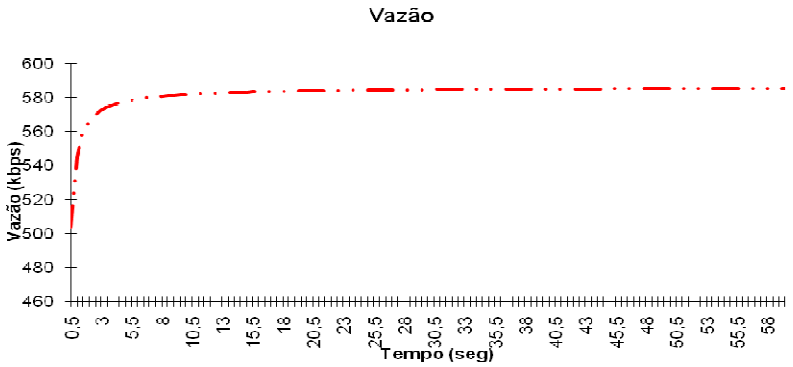

Fig. 7. Resultado da simulação do cenário 1

No segundo cenário (Fig. 8.), o nó móvel devido a sua alta mobilidade permanecerá pouco tempo dentro da área das BS´s e por isso realizará 4 *handovers*. As simulações comprovaram que sem o emprego da política de antecipação de *handover*, o nó móvel faz *hard handover*¸ ou seja, durante o processo de *handover* há a quebra de conexão e portanto o nó móvel não recebe pacotes nesse período de mudança de BS. Porém as simulações com o emprego da política de antecipação comprovaram que em nenhum instante há quebra de conexão ou período sem recebimento de pacotes, pois nesse caso o nó móvel realizou *seamleass handover*, permitindo que o cliente continue a usufruir de seus serviços normalmente independente da mudança de BS, provendo o máximo de QoS, desta forma caracterizando um cenário ideal. O gráfico abaixo demonstra a eficiência da política de antecipação de handover em relação ao cenário que não emprega a política.

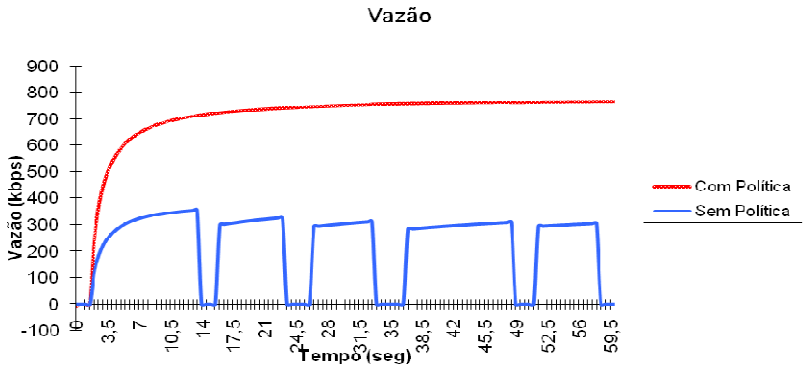

Fig. 8. Resultado da simulação do cenário 2

Além de prover o máximo de QoS, a antecipação do *handover* que otimiza o funcionamento da rede e fornece de forma transparente ao seu assinante móvel a

continuidade de seus serviços, diminui, também, o impacto causado pelo processo de autenticação e criptografia que atrasa no cenário acima o início do tráfego e da vazão na rede. No entanto, a técnica de predição compensa este tempo com o ganho sobre o tempo que seria perdido sempre que a SS precisasse se re-autenticar quando migrasse de uma BS à outra.

5 Conclusões

Este artigo propõe um esquema de autenticação para a tecnologia WiMAX, visando a segurança e a integridade dos dados recebidos pelo nó móvel com o intuito de inviabilizar a interceptação dos dados por um intruso na rede, além de evitar possíveis ataques de *hacker*. O sistema de autenticação não causa grandes impactos na rede salvo quando a quantidade de usuários é grande.

Visando também QoS e a diminuição do tempo gasto com essa segurança, foi implementado uma política de antecipação de *handover* com o intuito de que a mudança de ponto de acesso pelo cliente seja transparente evitando qualquer perda de conexão e consequentemente de pacotes de dados.

Para trabalhos futuros, propomos incluir novas métricas no algoritmo como a distância, balanceamento de carga e categorias de serviço do WiMAX a fim de avaliar a possibilidade da nova BS receber mais clientes.

6 Referências

1. Buvat, J. "WiMAX: The Last Mile Winner"**.** Telecom & Media Insights Issue. (2006).
2. Eklund, C. "IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for broadband Wireless Access"**.** IEEE Communication Magazine, June (2002).
3. Sauter, M. "Communication Systems for the Mobile Information Society"**.** John Wiley & Sons Ltd. Nortel Networks (2006).
4. Marks, R. Stanwood, K. Chang, D "IEEE Standard for Local and Metropolitan Area Networks"**.** October (2006).
5. IEEE 802.16. "IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems"**.** October (2005).
6. Bluetooth Special Interest Group – SIG "Personal Area Network Profile Version 1.0"**.** February. Disponível em: http://www.bluetooth.org (2003).
7. Telecommunication Standarlization Sector of ITU. "ITU-T-X.509" Information technology – Open Systems Interconnection – Authentication framework. August (1998).
8. Network Simulator (ns-2). "Ns Web Site"**.** Disponível em: http://www.isi.edu/nsnam/ns/ (2008).
9. National Institute of Standards and Technology – NIST. "NIST Web Site". Disponível em: http://www.antd.nist.gov (2007).
10. Crypto ++. "Crypto++ Web Site". Disponível em: http://www.cryptopp.com (2008).