Um protocolo de roteamento resistente a ataques blackhole sem detecção de nós maliciosos

Joilson Alves Junior e Luiz Carlos Pessoa Albini

***Resumo*— Um ataque frequentemente realizado sob redes ad hoc é o *blackhole*. Este ataque consiste em um ou vários nós descartando indiscriminadamente todos os pacotes de dados que passam por eles. Tal ataque pode ter um efeito destrutivo na rede, interrompendo totalmente seu funcionamento. Este artigo apresenta um protocolo de roteamento que minimiza os efeitos de ataques *blackhole* sem a necessidade de detecção dos nós maliciosos. Ele combina um esquema de partilha de informações baseado no teorema chinês do resto com uma técnica de roteamento multi-caminhos. Resultados de simulações indicam que o protocolo proposto fornece equilíbrio entre segurança e desempenho no roteamento diante de ataques *blackhole*. Comparações com os protocolos tradicionais mostram que os efeitos de um ataque deste tipo sobre o protocolo proposto é mínimo. Por exemplo, em cenários nos quais mais de 40% dos nós da rede são atacantes, a taxa de entrega apresenta ganhos superiores a 50% e uma redução superior a 50% no número de pacotes de dados descartados por atacantes *blackhole*.**

***Palavras-Chave*— Redes ad hoc, ataque *blackhole*, teorema chinês do resto.**

I. Introdução

Redes ad hoc móveis, também conhecidas como MANETs, abreviação para *Mobile Ad Hoc Networks*, são redes sem fio que podem ser construídas em qualquer lugar, pois independem da existência de infraestrutura fixa ou centralizada [1]. As unidades de tais redes são, em sua maioria, pequenas, portáteis, alimentadas por baterias e se comunicam umas com as outras através de sinais de rádio em uma topologia altamente dinâmica.

Como o alcance dos sinais de rádio destas redes é limitado, cada nó só pode se comunicar diretamente com outros nós que estiverem dentro do raio de alcance de seus sinais. Contudo, pode existir a necessidade de um nó transmitir informações para outros nós que estão além do seu raio de alcance. Para isso, os nós devem cooperar entre si agindo como roteadores, repassando as informações do nó origem ao nó destino [2]. Neste contexto, o roteamento é um desafio, pois deve suportar a topologia dinâmica e a falta de operações centralizadas, garantindo a entrega das mensagens com pequena sobrecarga e atraso.

Um dos principais protocolos de roteamento para estas redes é o *Ad-hoc On-demand Distance Vector* (AODV) [3]. Ele é um protocolo que atua sob demanda, isto é, procura por rotas somente quando elas são realmente necessárias. O AODV constrói rotas através de mensagens de requisição de rotas *Route Request* e respostas de rota *Route Reply*. Quando um nó necessita enviar uma mensagem para outro do qual ele ainda não conhece a rota, uma mensagem de Route Request é enviada em broadcast. Cada nó que recebe esta mensagem pode enviar uma mensagem de Route Reply para a origem se ele é o destinatário, ou se ele conhece uma rota para o destino. Caso contrário, a mensagem é reencaminhada. Mensagens de *reply* são enviadas em unicast pelo caminho reverso criado pela mensagem de Route Request. A movimentação de um nó pode provocar a queda de um enlace que estava sendo utilizado. Nesta situação, o nó que detectou a quebra envia uma mensagem de Route Error até a origem, avisando sobre ela. Se a origem ainda deseja utilizar a rota, o processo de descoberta de rotas é reiniciado.

Uma forma mais rápida de recuperar as quebras de enlaces consiste em adaptar o AODV para utilizar multi-caminhos. Este é o objetivo do protocolo *Ad-hoc On-demand Multipath Distance Vector* (AOMDV)[4]. Em outras palavras, o objetivo do AOMDV é estender o AODV para encontrar múltiplas rotas disjuntas e livres de laços entre origens e destinos, ao invés de somente uma rota. Ao descobrir a primeira rota para o destino, a origem começa a usá-la. Todas as outras são deixadas como rotas de backup, que serão utilizadas caso a rota atual seja quebrada.

Outro desafio em redes ad hoc está relacionado à segurança dos nós. Além dos problemas tradicionais, a comunicação colaborativa possibilita novas ameaças de segurança e a ausência de infraestrutura dificulta a criação de mecanismos de defesa [5]. Dessa forma, ataques de nós maliciosos podem interromper o funcionamento da rede

Joilson Alves Junior e Luiz Carlos Pessoa Albini¸ NR2 - Departamento de Informática, UFPR, Curitiba, Brasil, E-mails: ¸ joilson@utfpr.edu.br, albini@inf.ufpr.br. Este trabalho foi parcialmente financiado pelo CNPq.

e causar impacto na disponibilidade dos recursos e das informações.

Os ataques podem ser categorizados em duas classes: ataques passivos e ataques ativos [6]. Os ataques passivos não afetam o funcionamento da rede, sendo caracterizados apenas pela espionagem dos dados. Por outro lado, os ataques ativos são aqueles em que o atacante altera, descarta ou inviabiliza o uso dos dados que estão sendo transmitidos. Um ataque ativo comumente realizado em redes ad hoc é o *blackhole* [5], [7], [8]. O *blackhole* é um tipo de ataque de negação de serviço cujo objetivo é interromper o funcionamento da rede, descartando os pacotes que passam por eles. Um nó *blackhole* pode aproveitar-se da vulnerabilidade dos algoritmos de roteamento cooperativos e, através do envio de pacotes de roteamento falsos, rotear para si mesmo todos os pacotes de dados e descartá-los [5].

Este artigo apresenta um protocolo de roteamento que minimiza o impacto do descarte de pacotes por ataques do tipo *blackhole*, sem a necessidade de detecção dos nós maliciosos. Este protocolo combina um esquema de partilha de informações baseado no teorema chinês do resto [12] com uma versão modificada do protocolo de roteamento multi-caminhos AOMDV [4].

Resultados de simulações indicam que o protocolo proposto fornece equilíbrio entre segurança e desempenho no roteamento diante de ataques de nós *blackhole*. Comparações com protocolos tradicionais mostram que em cenários nos quais mais de 40% dos nós da rede são atacantes, a taxa de entrega apresenta ganhos superiores a 50%, com uma redução superior a 50% no número de pacotes de dados descartados por atacantes. É possível atingir quase quatro vezes a taxa de entrega dos protocolos tradicionais na presença de 60% de atacantes na rede.

O restante deste artigo está organizado desta forma: a seção 2 apresenta o novo protocolo de roteamento; a seção 3 contém a avaliação de desempenho e a seção 4, as conclusões.

II. Protocolo de roteamento resistente a ataques blackhole sem detecção de nós maliciosos

O funcionamento do novo protocolo é extremamente simples. Ele consiste em dividir as mensagens de dados em partes sobrepostas e enviar cada parte por uma rota diferente até o destino. Para remontar a informação original é necessário um número mínimo de partes. Qualquer tentativa de remontá-la com menos partes é impossível. Isso pode tornar o protocolo resistente a outros ataques. Entretanto, esta análise está fora do escopo deste artigo, fazendo parte dos trabalhos futuros.

O funcionamento do protocolo pode ser dividido em três etapas: (i) a divisão da informação original com base no teorema chinês do resto; (ii) a transmissão das partes usando rotas disjuntas através de roteamento multi-caminhos; (iii) a remontagem da informação original no destino. Em outras palavras, dada uma informação d, deve-se dividir d em n partes e enviar cada parte por um caminho diferente até o destino. Para reconstruir a d no destino, deve-se receber no mínimo k das n partes, onde $k \leq n$. Além disso, $k-1$ ou menos partes não podem reconstruir a informação original. Usando esta técnica, atacantes *blackhole* podem descartar até $n - k$ partes e mesmo assim a informação pode ser reconstruída no destino.

A. Divisão e remontagem das informações

Na origem, cada mensagem é dividida em n partes de mesmo tamanho, as quais são enviadas por n caminhos diferentes e disjuntos. O tamanho de cada parte deve ser d/k, em que d é o tamanho da informação original e k é o número de partes necessárias para reconstruir a informação original[10][11], sendo $n \geq 2$. A descrição matemática completa da divisão e remontagem da informação, bem como sua prova de corretude podem ser encontradas em [12].

Entretanto, esta divisão cria uma sobrecarga extra. A mensagem original deve ser dividida em n partes, cada uma com tamanho d/k. Como $n > k$, tem-se uma sobrecarga de $(n-k)$ mensagens, cada uma com tamanho d/k mais cabeçalhos. Por exemplo, se a mensagem original tiver 1030 bytes ($d = 1030$), com divisão em três partes ($n = 3$) e sendo necessárias duas partes para reconstruir a informação ($k = 2$), o custo para se mandar esta mensagem no novo protocolo é de três mensagens de tamanho $d/k = 1030/2 = 512$, ou seja, $3 * (512 + c)$, em que c representa o custo dos cabeçalhos dos diversos protocolos utilizados. Em protocolos tradicionais o custo é de $1030 + c$. Porém como será demonstrado, este custo extra compensa pela maior taxa de entrega e, consequentemente, menor retransmissão de dados.

B. Modificação do AOMDV

Para criar as rotas disjuntas pelas quais as partes trafegam, foi realizada uma adaptação no protocolo AOMDV. O AOMDV original cria no máximo três rotas disjuntas e livres de laço entre dois nós quaisquer, em cada processo de descoberta de rotas. A modificação realizada na descoberta de rota foi a remoção da limitação de três rotas, o novo protocolo mantém todas as rotas disjuntas entre origens e destinos. Obviamente, esta modificação implica em tabelas de roteamento maiores.

Além disso, o AOMDV original utiliza somente a primeira rota encontrada, mandando todas as mensagens

pela mesma rota. As outras rotas somente são utilizadas quando a rota inicial torna-se inválida, ou seja, elas são rotas de reserva. A outra adaptação que o AOMDV sofreu foi para permitir que todas as rotas possam ser utilizadas ao mesmo tempo, enviando as diferentes partes da mensagem original. É importante mencionar que caso o protocolo não seja capaz de construir n rotas disjuntas entre a origem e o destino, as n partes da informação são transmitidas através das rotas disponíveis, seguindo uma distribuição cíclica.

III. Avaliação

O novo protocolo foi avaliado através de simulação usando o simulador NS (Network Simulator) versão 2.34 [13]. Seu desempenho foi comparado com dois protocolos de roteamento tradicionais (o AODV e o AOMDV), para demonstrar sua eficiência na presença de atacantes.

A. Ambiente de Simulação

A rede utilizada nas simulações é uma área retangular com 1500m x 300m com 75 e 100 nós distribuídos aleatoriamente. Os nós se movimentam livremente, seguindo o modelo de movimentação *random waypoint* [14], com velocidades de 1 m/s e 8 m/s e sem pausas. O padrão de tráfego é composto por conexões (UDP) com taxa de bits constante (CBR) entre 15 pares de nós escolhidos aleatoriamente. O modelo de propagação de rádio é o *twoRay ground*[14], enquanto a camada MAC segue as especificações IEEE 802.11[15]. O raio de transmissão dos nós é de 250 metros. As simulações são realizadas por 600 segundos e todos os resultados apresentados são médias de 35 simulações com intervalo de confiança de 95%.

O protocolo foi avaliado em dois cenários: o objetivo do **cenário 1** é examinar um ambiente de rede hostil, com alto percentual de nós atacantes, de 0% a 60% de atacantes, sobre uma rede com 100 nós. O **cenário 2** demonstra o funcionamento do protocolo perante o aumento do tráfego na rede, conexões CBR transmitindo 2, 8, 16, 32 e 64 mensagens por segundo, sobre uma rede com 75 nós e com um número fixo de 40% de atacantes.

Todas as simulações comparam o protocolo proposto, chamado de AOMDVM, o qual implementa o sistema de roteamento resistente a ataques de *blackhole*, com os protocolos AOMDV e AODV originais. São apresentados quatro diferentes resultados para o AOMDVM: AOMDVM 3R2P ($n = 3, k = 2$), AOMDVM 4R2P ($n = 4, k = 2$) , AOMDVM 6R2P ($n = 6, k = 2$) e AOMDVM 6R3P ($n = 6, k = 3$). Lembrando que n indica o número de partes em que a informação é dividida na origem e k indica o número mínimo de partes necessárias para que o destino remonte a informação original.

B. Métricas

O protocolo proposto foi avaliado com base nas seguintes métricas:

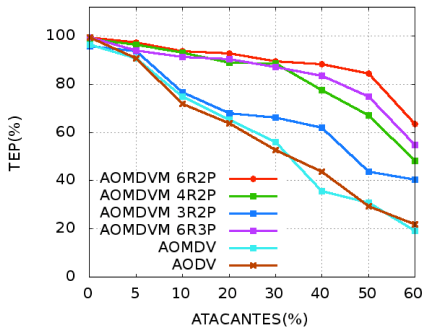
- **Taxa de entrega dos pacotes (TEP)**: é a proporção de pacotes de dados entregues ao destino em relação à quantidade de pacotes enviados. Um pacote é dado como recebido no protocolo proposto se o destino receber mais de k partes da mensagem original, i.e. se o destino conseguir remontar a informação original.
- **Sobrecarga de roteamento (SOR)**: é a quantidade total de pacotes de roteamento transmitidos. Em pacotes enviados através de múltiplos saltos, cada salto conta como uma transmissão.
- **Pacotes de dados descartados por nós maliciosos (PDM)**: é a porcentagem de pacotes de dados descartados pela ação de nós *blackhole* em relação à quantidade total de pacotes enviados. Ela indica a tolerância do sistema contra a ação de nós maliciosos.

C. Resultados de simulação

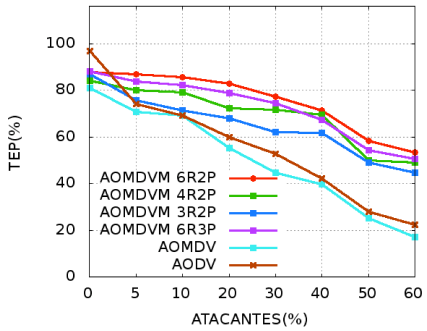
É possível observar na figura 1, que a taxa de entrega de todos os protocolos diminui com o aumento do número de atacantes. Contudo, o protocolo proposto obteve melhores resultados para todos os percentuais nós atacantes. Com 60% de atacantes na rede, a taxa de entrega do protocolo proposto utilizando ($n = 4, k = 2$), ($n = 6, k = 2$) e ($n = 6, k = 3$) é superior a 50%, enquanto os protocolos AODV e AOMDV originais entregam apenas 20% de seus pacotes. Com a velocidade dos nós em 1m/s e 50% de atacantes, o novo protocolo com ($n = 6, k = 2$) apresenta ganhos ainda superiores, atingindo 84,87%, enquanto o AOMDV e o AODV entregam apenas 30,6% e 29.10%, respectivamente.

A figura 2 mostra que o aumento do percentual de atacantes aumenta também a quantidade de pacotes descartados. Este resultado é esperado porque conforme aumenta-se o número de nós atacantes, também cresce o número de rotas comprometidas pela presença dos mesmos. Contudo, nota-se que o protocolo proposto reduz o número de pacotes descartados em relação ao AODV e AOMDV, independentemente do percentual de atacantes, oferecendo ganhos superiores a 50%.

A figura 3 ilustra a sobrecarga dos protocolos. Pode-se notar que o novo protocolo mantém uma sobrecarga semelhante ao do AOMDV original. Isso ocorre porque o processo de descoberta de rotas dos dois protocolos são iguais. Considerando o aumento do tráfego na rede (figura 4), é possível observar que a taxa de entrega de todos os protocolos é inversamente proporcional ao tráfego. Contudo, o novo protocolo apresenta sempre uma taxa de entrega superior aos outros protocolos independentemente do tráfego. Entretanto, o aumento do tráfego não

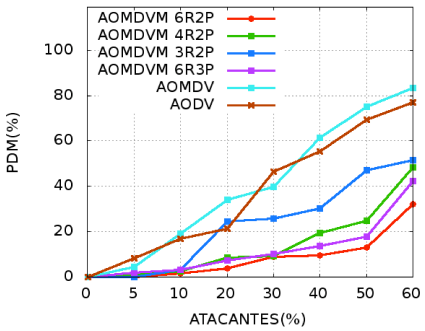


(a) Cenário 1 - Velocidade 1

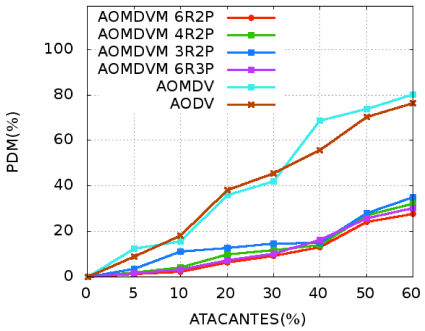


(b) Cenário 1 - Velocidade 8

Fig. 1: Taxa de entrega versus percentual de atacantes *blackhole* - rede com 1.500m X 3000m e 100 nós



(a) Cenário 1 - Velocidade 1



(b) Cenário 1 - Velocidade 8

Fig. 2: Pacotes de dados descartados por nós *blackhole* - rede com 1.500m X 300m e 100 nós

ocasiona um aumento no número de pacotes descartados por atacantes (figura 5). Isso ocorre porque existe um aumento dos descartes de pacotes por outras naturezas, como congestionamento e *buffer overflow*.

IV. Conclusões

Este artigo apresentou um protocolo para reduzir o impacto do descarte de pacotes em rede ad hoc causados por ataques do tipo *blackhole*. Ele combina um esquema de partilha de informações baseado no teorema chinês do resto e roteamento multi-caminhos. Cada mensagem é dividida em partes menores sobrepostas, que são enviadas da origem para o destino por caminho disjuntos. No destino, a mensagem original é remontada, mesmo se algumas partes forem descartadas.

O protocolo proposto consegue minimizar o efeito de ataques *blackhole*, sem detecção ou conhecimento prévio do nó atacante. Os resultados mostram que o novo protocolo apresenta uma taxa de entrega sempre superior aos protocolos tradicionais, e.g. AODV e AOMDV, na presença de atacantes. É possível atingir quase quatro vezes a taxa de entrega dos protocolos tradicionais na presença de 60% de atacantes na rede. Conforme foi demonstrado o novo protocolo obteve uma melhora na taxa de entrega e na vazão dos pacotes de dados e uma redução do impacto da ação de nós maliciosos, independentemente do percentual de atacantes na rede. Trabalhos futuros incluem a avaliação do consumo energético do novo protocolo, bem como a análise comparativa dele com outros protocolos de roteamento.

Referências

[1] X. Bangnan and H. sven, "The Role of Ad hoc Networking in Future Wireless Communications," in *International Conference on Communication Technology Proceedings, 2003. ICCT*, 2003, pp. 1353–1358.

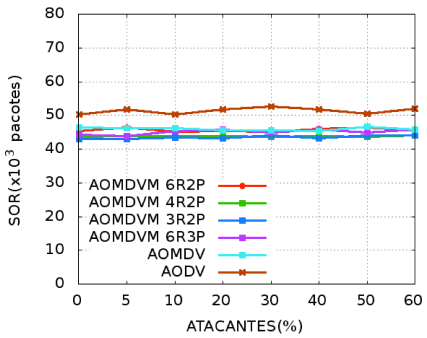
[2] V. Talooki and K. Ziarati, "Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks," in *Communications, 2006. APCC'06. Asia Pacific Conference*, 2006, pp. 1–5.

[3] C. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector (AODV) routing," in *IEEE WMCSA 99*, 1999, pp. 90–100.

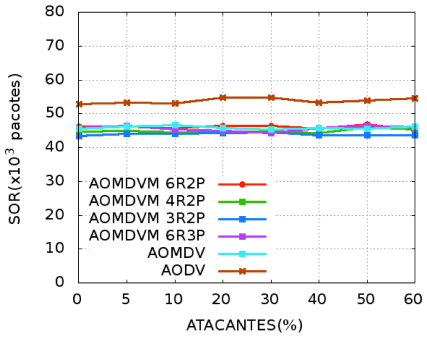
[4] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing for ad hoc networks," *Wireless Communication Mobile Computing*, vol. 6, pp. 969–988, Janeiro 2006.

[5] S. Djahel, F. N. abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," *IEEE communications surveys and tutorials*, pp. 1–14, 2010.

[6] C. Murthy and B. Mano, "Ad hoc wireless networks: architetures and protocols," 2004, prentice Hall Professional Technical Reference.

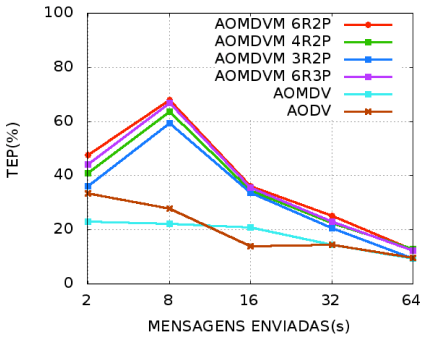


(a) Cenário 1 - Velocidade 1

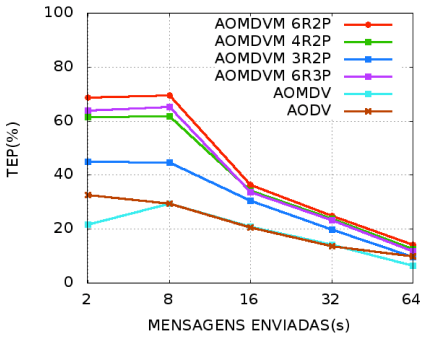


(b) Cenário 1 - Velocidade 8

Fig. 3: Sobrecarga - rede com 1.000m X 1.000m e 100 nós

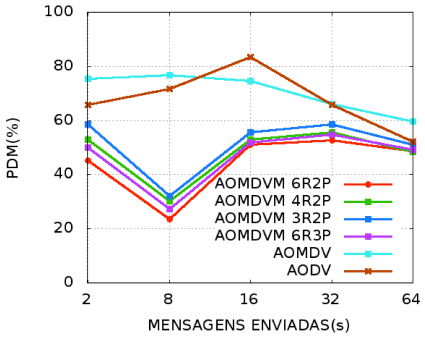


(a) Cenário 2 - Velocidade 1

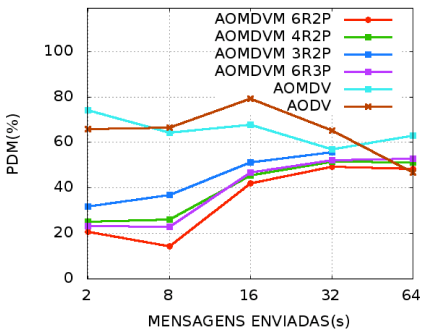


(b) Cenário 2 - Velocidade 8

Fig. 4: Taxa de entrega dos dados - 40% de atacantes



(a) Cenário 2 - Velocidade 1



(b) Cenário 2 - Velocidade 8

Fig. 5: Quantidade de pacotes descartados - 40% de atacantes

[7] A. Hasswa, M. Zulkernine, and H. Hassanein, "Routeguard: an intrusion detection and response system for mobile ad hoc networks," in *Wireless And Mobile Computing, Networking And Communications, 2005.(WiMob' 2005), IEEE International Conference*, 2005, pp. 336–343.

[8] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hocvnetworks," *Wireless Networks*, vol. 11(1), pp. 21–38, 2005.

[9] M. Marina and S. Das, "On-demand multipath distance vector routing for ad hoc networks," *Network Protocols, 2001. Ninth International Conference*, pp. 14–23, Novembro 2001.

[10] H. Krawczyk, "Secret sharing made short," *Proceeding CRYPTO '93 Proceedings of the 13th annual international cryptology conference on Advances in cryptology*, Maio 1994.

[11] A. Parakh and S. Kak, "Space efficient secret sharing for implicit data security," *Journal Information Sciences: an International Journal*, Janeiro 2011.

[12] J. A. Junior, L. F. L. Nascimento, and L. C. P. Albini, "Using the redundant residue number system to increase routing dependability on mobile ad hoc networks," *Cyber Journals: Multidisciplinary Journals in Science and Technology - Journal of Selected Areas in Telecommunications (JSAT)*, pp. 67–73, 2011.

[13] NS-2, "The network simulator - ns-2," 2007. [Online]. Available: http://www.isi.edu/nsnam/ns

[14] M. Gast, "802.11 Wireless Networks. O'Really," 2002.

[15] IEEE., "Draft supplement to part 11: Wireless medium access control (mac) and physical layer (phy) specifications: Medium access control (mac) enhancements for quality of service (qos)," Novembro 2002.