Técnicas de Avaliação e Punição ao Mau Comportamento em Redes Ad hoc

Reinaldo B. Braga e Otto Carlos M. B. Duarte*

[1]Grupo de Teleinformática e Automação (GTA)
PEE/COPPE/UFRJ
Universidade Federal do Rio de Janeiro (UFRJ)
Rio de Janeiro, RJ – Brasil

{reinaldo,otto}@gta.ufrj.br

Abstract. *Ad hoc networks uses collaborative routing to allow the communication between nodes. These networks suffer from temporary problems of packets forwarding caused by connectivity failures, transmission errors, collisions, and mobility which can be detected as a misbehavior. This paper proposes two techniques to evaluate and punish misbehaving station on ad hoc networks. The goal is to increase the identification precision and the treatment given to misbehaving station, reducing the false positives, which occurs when stations are incorrectly detected as misbehaviored and punished. The techniques are defined based on the network tolerance level, being classified as intolerant and tolerant. On the intolerant technique the station can be blocked due to just one detected misbehavior. On the other hand, the tolerant technique presents to misbehaving stations computational challenges before blocking them. Results from the mathematical analysis of the both proposed techniques are also presented on this paper.*

Resumo. *Redes ad hoc sem fio se servem de roteamento colaborativo para a comunicação entre estações. Ao mesmo tempo, estas redes sofrem de problemas temporários de não encaminhamento de pacotes por causa de falta de conectividade, erros de transmissão, colisão e mobilidade que podem ser detectados como mau comportamento. Este artigo propõe duas técnicas de avaliação e punição ao mau comportamento de estações em redes ad hoc. O principal objetivo da proposta é aumentar a precisão na identificação e na resposta às estações mal comportadas, reduzindo a quantidade de falso-positivos, ou seja, punições injustas para estações incorretamente detectadas como maliciosas. As técnicas são definidas de acordo com o nível de tolerância da rede, sendo classificadas como intolerante e tolerante. Na técnica intolerante a estação pode ser bloqueada na realização de um único mau comportamento detectado. A técnica tolerante atribui desafios computacionais para a estação mal comportada antes de bloqueá-la. Por fim, são apresentados os resultados da análise matemática realizada para as duas técnicas propostas.*

1. Introdução

Em redes ad hoc as estações devem se comportar de forma colaborativa, já que as estações também exercem funções de roteamento, encaminhando pacotes aos seus vizinhos. De-

*Este trabalho foi realizado com recursos do CNPq, FINEP, RNP, FAPERJ e CAPES

vido a esta característica, uma estação maliciosa pode prejudicar o funcionamento da rede através da criação, repetição, descarte ou modificação de pacotes [Hu e Perrig, 2004]. Portanto, torna-se necessária a utilização de mecanismos de segurança capazes de evitar estes maus comportamentos realizados por estações maliciosas.

As propostas convencionais de soluções contra o mau comportamento utilizam mecanismos criptográficos que objetivam a identificação e a autenticação dos emissores de pacotes e, também, a proteção do conteúdo das mensagens. Entretanto, a autenticação assume que toda estação autenticável não realiza maus comportamentos e que todas estações não autenticáveis são estações maliciosas. Desta forma, estes mecanismos são incapazes de proteger as redes ad hoc de estações autenticadas que realizam comportamentos maliciosos. Por exemplo, a autenticação não impede que os ataques de descarte de pacotes sejam realizados [Fernandes et al., 2006]. Portanto, são necessárias técnicas de detecção e punição aos maus comportamentos.

De acordo com [Maccabe e Servilla, 1990], mau comportamento pode ser definido como qualquer ação que comprometa a integridade, a confidencialidade ou a disponibilidade dos recursos. Atualmente, existem dois modelos para detecção de mau comportamento em redes [Kang e an Honavar V., 2005]. O primeiro modelo, baseado em assinaturas, realiza detecções ao identificar comportamentos previamente classificados como maliciosos. Assim, os eventos que não possuem um padrão conhecido de mau comportamento são classificados como comportamentos normais, adotando uma atitude otimista. O segundo modelo, baseado em anomalias, é considerado pessimista por classificar como mau comportamento todo evento desconhecido. Estes modelos utilizam dois métodos de detecção, que podem ser executados por rede ou por estação. Na detecção por rede existe um ponto central responsável pela detecção. Já na detecção por estação, cada estação da rede realiza individualmente o procedimento de detecção.

No modelo baseado em assinaturas é mantida uma base de assinaturas representando os tipos de mau comportamento conhecidos. Qualquer evento igual a alguma das assinaturas é considerado malicioso. Para uma maior eficiência, são necessárias atualizações constantes da base de assinaturas a fim de detectar os novos tipos de mau comportamento. Neste modelo, o método de detecção pela rede é realizado por uma estação central que observa as assinaturas dos eventos de todas as estações da rede e as compara com a base de assinaturas. No método de detecção por estação, cada estação possui sua base de assinaturas e realiza esta comparação de forma independente.

No modelo baseado em anomalias são definidos padrões de normalidade para o correto funcionamento da rede. Qualquer evento diferente do padrão é definido como um mau comportamento. Neste modelo, caso seja utilizado o método de detecção pela rede, a estação central deve observar o comportamento de todas as outras estações e identificar as que estão agindo fora do padrão de normalidade. No método de detecção por estação, o monitoramento é descentralizado, pois cada estação monitora independentemente as outras estações da rede.

Tanto o modelo baseado em assinaturas, quanto o modelo baseado em anomalias, existem os falso-positivos e os falso-negativos quando aplicados em redes ad hoc. Os falso-positivos ocorrem quando uma estação que se comporta corretamente é classificada como mal comportada como, por exemplo, devido aos problemas temporários de não

encaminhamento de pacotes por causa de falta de conectividade, erros de transmissão, colisão e mobilidade. Em uma rede ad hoc é comum que estações sofram problemas temporários de conectividade e erros de transmissão causando uma ocorrência significativa de falso-positivos e, portanto, muitas estações não maliciosas são punidas desnecessariamente. Assim, nas redes ad hoc, é primordial o uso de mecanismos que permitam refinar a avaliação dos falso-positivos.

O objetivo deste trabalho é propor um sistema de alta precisão na avaliação e punição das detecções realizadas pelos detectores de mau comportamento, reduzindo a quantidade de punições em estações bem comportadas que são detectadas como maliciosas, ou falso-positivos. A idéia chave é tornar menos abrupta a punição de uma estação detectada como maliciosa, possibilitando um maior número de chances da estação provar que não é maliciosa, pois o mau comportamento detectado foi por causa de problemas temporários.

De acordo com [Zhang e Lee, 2000], as técnicas do modelo baseado em assinaturas possuem menos ocorrências de falso-positivos quando comparadas com as técnicas do modelo baseado em anomalias. Isto ocorre devido a incapacidade que os mecanismos baseados no modelo de anomalias têm de identificar o tipo de mau comportamento, o que não é verdade para os mecanismos baseados em assinaturas, que conhecem o comportamento de toda detecção realizada. Entretanto, as técnicas baseadas em assinaturas são mais susceptíveis a ocorrência de falso-negativos, ou seja, estações mal comportadas que realizam eventos maliciosos e não são identificadas, pois existe a possibilidade de um novo mau comportamento não está presente na base de assinaturas. Já nas técnicas baseadas em anomalias a ocorrência de falso-negativos é menor porque uma estação não consegue realizar um ataque seguindo o padrão de normalidade definido.

Na Figura 1 é mostrado como as técnicas propostas são aplicadas, utilizando as informações coletadas pelos detectores de mau comportamento, tanto de eventos bons como maus. Ao coletarem essas informações, realizam a avaliação e a punição de acordo com um limiar de tolerância da rede. As técnicas propostas se aplicam aos dois modelos de detecção, pois a ocorrência de falso-positivos existe em ambos os casos. Porém, tornam-se mais eficiente no modelo baseado em anomalias, no qual possui uma quantidade de falso-positivos superior ao modelo baseado em assinaturas [Zhang e Lee, 2000]. As duas técnicas propostas no artigo observam todos os eventos realizados pelas estações

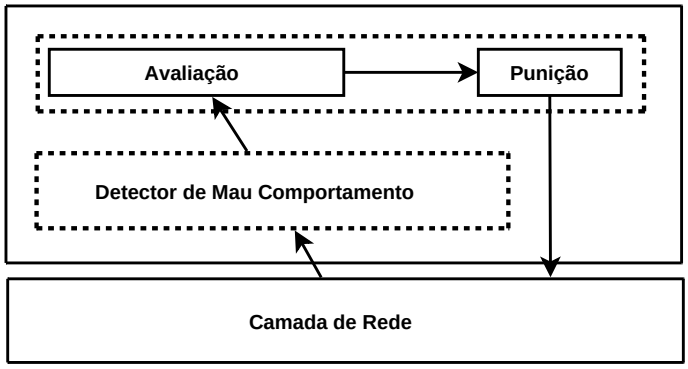

Figura 1. Arquitetura de avaliação e punição.

vizinhas e calculam uma probabilidade a partir das detecções de maus comportamentos.

A eficiência de ambas as técnicas são apresentadas através de uma análise matemática realizada na ferramenta Matlab 7.0 [Moler, 1980]. A técnica denominada intolerante pode punir a estação no instante da primeira detecção de mau comportamento, seguindo a distribuição geométrica de variável aleatória discreta. Na técnica tolerante, as punições são realizadas através de desafios computacionais enviados após a detecção de um ou mais maus comportamentos detectados, seguindo uma distribuição binomial negativa de variável aleatória discreta.

Para as duas técnicas é utilizado um limiar que determina a quantidade de bons comportamentos exigidos para o correto funcionamento da rede, que é comparado com a média de bons eventos realizados pela estação até ser detectada como maliciosa. Este limiar no modelo intolerante determina se a estação será punida ou não e, no modelo tolerante, auxilia na atribuição do grau de punição.

O restante do artigo está organizado da seguinte maneira: a Seção 2 discute os trabalhos relacionados e a Seção 3 descreve as duas técnicas de avaliação e punição ao mau comportamento. A análise matemática das técnicas é mostrada na Seção 4 e os resultados são analisados na Seção 5. Por fim, são apresentadas as conclusões e os trabalhos futuros na Seção 6.

2. Trabalhos Relacionados

Em [Marti et al., 2000] foi apresentado o *Watchdog* como o primeiro protocolo de detecção de mau comportamento baseado em monitoramento através de escutas às estações vizinhas em redes ad hoc. O *Watchdog* foi implementado utilizando o protocolo *Dynamic Source Routing* (DSR) [Johnson e Maltz, 1996] e faz com que cada estação observe o encaminhamento dos pacotes realizados por seus vizinhos na rota formada entre uma origem e um destino. A idéia principal é escutar a transmissão dos vizinhos e verificar se o pacote é encaminhado sem sofrer qualquer alteração. Os autores destacam que se a rota de origem não é usada, então uma estação mal comportada pode tentar enganar o *Watchdog* modificando a rota original e transmitindo por difusão para outra estação não existente na rota. Tendo em vista os problemas do *Watchdog*, os autores procuram reduzir os efeitos das estações mau comportadas através do *Pathrater*, que cria uma rota da origem para o destino baseando-se em uma métrica de confiança atribuída à cada estação, além de considerar o menor caminho definido pelo protocolo de roteamento. Como observado em [Buchegger e Boudec, 2002], os autores não realizam punições às estações maliciosas que participam do processo de roteamento.

Tendo como base o *Watchdog*, [Buchegger e Boudec, 2002] criaram o *Neighborhood Watch*. A proposta é independente do protocolo DSR, mas cada nó continua observando os eventos dos seus vizinhos. Os autores introduzem o conceito de gerenciador de confiança, sistema de reputação e gerenciador de caminhos. Cada estação possui uma máquina de estados finita que calcula a confiança na rota que é criada. A rota é escolhida considerando a métrica para o caminho mais seguro. A desvantagem do *Neighborhood Watch* está na validade das informações obtidas por experiências passadas de outros vizinhos, que podem ser estações maliciosas que adquiriram a confiança das estações da rede para, posteriormente, passarem informações erradas. Além disso, não são apresentadas análises de resultados obtidos a partir da proposta.

[Patwardhan et al., 2005] implementam um protocolo de roteamento seguro base-

ado no *Ad hoc On-demand Distance Vector* (AODV) sobre IPv6, adicionando um mecanismo de detecção de mau comportamento baseado no modelo de anomalias. O protocolo *Secure routing protocol based on AODV* (SecAODV) foi implementado em dispositivos móveis e utilizou pacotes criptografados, considerando as características de mobilidade para a detecção de mau comportamento. Os autores desta proposta criaram um cenário de testes usando o protocolo IPv6. O problema está na utilização do protocolo TCP sem considerar suas problemáticas em redes sem fio, principalmente com relação à mobilidade. O trabalho não apresentou resultados com relação aos falso-positivos.

Em [Liu et al., 2006], os autores propõem um modelo baseado em anomalias e uma arquitetura em camadas, no qual cada estação coleta e analisa os eventos antes de decidir como proceder na detecção e na resposta ao mau comportamento. Além disso, é apresentado um mecanismo de resposta que pode ser global, envolvendo toda a rede, ou local, no qual cada estação pode agir independentemente. A maior desvantagem deste artigo está no cenário montado para a avaliação da proposta que, apesar de ser baseada no modelo em anomalias, exige que seja identificado o tipo de mau comportamento para determinar o grau de punição.

3. Técnicas de Avaliação e Punição

Este trabalho propõe duas técnicas de avaliação e punição ao mau comportamento através do monitoramento de eventos realizados por vizinhos. O mecanismo de monitoramento segue a proposta descrita em [He et al., 2004], onde cada estação observa o comportamento dos seus vizinhos. O objetivo da proposta é aumentar a precisão na punição de estações mal comportadas e reduzir a quantidade de punições injustas às estações classificadas erroneamente como maliciosas. Assume-se que a cada análise matemática todas as estações bem comportadas da rede executam o mesmo modelo de detecção e a mesma técnica de avaliação e punição aos maus comportamentos, podendo seguir qualquer um dos modelos de detecção, ou seja, o baseado em assinaturas ou o baseado em anomalias.

A seguir serão descritas as duas propostas: a técnica intolerante e a técnica tolerante. Para as duas técnicas temos como parâmetros o número e de eventos realizados, o cálculo da probabilidade de bloqueio $P_B(e)$ para o modelo intolerante e o cálculo da probabilidade de punição $P_P(e)$ para a técnica tolerante. Além disso, será apresentado o mecanismo de punição através de desafios computacionais utilizado pela técnica tolerante.

3.1. Técnica Intolerante

Na técnica intolerante são observados e eventos e, na ocorrência da primeira má ação detectada, é calculada a função de probabilidade de massa (PMF) $F(e)$ para a estação mau comportada. Em seguida, definimos $P_B(e)$ como uma função de distribuição cumulativa (CDF) calculada a partir desta PMF, seguindo uma distribuição geométrica de variável aleatória. A PMF geométrica da técnica intolerante é definida por:

$$F(e) = p(1-p)^{e-1}, \tag{1}$$

onde p é a probabilidade da ocorrência de um evento malicioso e $(1-p)$ é a probabilidade da ocorrência de eventos bons. Tendo como base os valores encontrados, calculamos M_I

como a média de bons eventos até a ocorrência de um mau evento:

$$M_I = \frac{1}{p}, \tag{2}$$

e $P_B(e)$ como a probabilidade de bloqueio da estação mau comportada:

$$P_B(e) = \sum_{1}^{e} F(e). \tag{3}$$

Para um mecanismo de detecção mais justo com estações afetadas pelos falso-positivos, propomos que a punição seja executada com base em um limiar L, que será comparado com o valor obtido em M_I da equação 2. Portanto, temos:

- $L \leq M_I$, estação não será bloqueada;
- $L > M_I$, estação será bloqueada.

Ao analisarmos um cenário de rede ad hoc, o limiar L é definido de acordo com o nível dos problemas típicos de redes sem fio, tais como elevadas taxas de perda, saturação da rede, mobilidade, dentre outros. Como um exemplo para esta técnica temos: se L é igual a dez e M_I é igual a cinco, sabemos que a cada cinco eventos realizados por uma estação, um será considerado como mau comportamento, fazendo com que a estação seja bloqueada.

3.2. Técnica Tolerante

Na técnica tolerante os maus comportamentos são admitidos até que sejam observados D detecções. Após D maus comportamentos detectados são enviados desafios computacionais que a estação deve resolver para não ser bloqueada. Somente após $k - 1$ desafios computacionais enviados o bloqueio será realizado, mesmo que a estação tenha resolvido todos os desafios. Nesse caso, a execução de um bloqueio depende da quantidade de punições enviadas k. A probabilidade de punição P_P obtida através da tolerância de maus comportamentos D. Para escolher o valor de D é necessário o conhecimento das características dos tipos de cenário de redes ad hoc.

Diferentemente da técnica intolerante, o limiar L é utilizado para determinar o grau de punição que será enviado. A probabilidade de punição para esta técnica segue uma distribuição binomial negativa, pois agora é calculada quando a estação realizar D maus comportamentos. Ocorridos esses D maus comportamentos a estação receberá punições através de desafios computacionais e bloqueios.

Quando o valor de D for igual a um, a distribuição binomial negativa será reduzida a uma distribuição geométrica, ou seja, o cálculo da probabilidade de punição seguirá o mesmo da técnica intolerante. Entretanto, com essa técnica, serão enviados desafios computacionais ao invés de permitir que a estação detectada como mal comportada retorne a rede sem receber qualquer punição. De acordo com estas características de tolerância aos maus comportamentos, é calculada a função de probabilidade de massa (PMF) da distribuição binomial negativa:

$$F(e) = \binom{e-1}{D-1} p^D (1-p)^{e-D}, e = D, D+1, D+2, ...; \tag{4}$$

a média de D ocorrências de eventos mau comportados:

$$M_T = \frac{D}{p}; \tag{5}$$

e a probabilidade de punição:

$$P_P(e) = \sum_{1}^{e} F(e). \tag{6}$$

Para o limiar L são considerados os seguintes aspectos:

- $L \leq M_T$, estação recebe um desafio computacional com o tempo de resolução aumentado linearmente;
- $L > M_T$, estação recebe um desafio computacional com o tempo de resolução aumentado exponencialmente;
- Na ocorrência de k punições, a estação será bloqueada.

Em resumo, D representa a tolerância em relação a quantidade de detecções de maus comportamentos suportados até enviar, por $k-1$ vezes, desafios computacionais para a estação. M_T é definido como a média de bons eventos até a ocorrência de D maus eventos. Na ocorrência de k punições a estação será bloqueada. Outra forma de ocorrer um bloqueio é quando a estação não resolve um desafio computacionasl dentro do intervalo de tempo previsto para a resposta. Assim, enquanto a estação estiver resolvendo desafios, ela não poderá participar de qualquer atividade com a estação remetente do desafio e nem com os seus outros vizinhos que ouviram o desafio ser enviado, fazendo com que rotas alternativas sejam utilizadas. Desta forma, é possível que os vizinhos da estação mau comportada a evitem, já que é assumido que todas as estações utilizam a mesma técnica de detecção e resposta.

Supondo, por exemplo, que D seja igual a dois e que o segundo mau comportamento foi detectado no vigésimo evento realizado pela estação, então p será igual a $2/20 = 0,1$ e a média M_T será igual a 20. Supondo um valor para L igual a quinze, um desafio será enviado para a estação e o tempo de resolução deste desafio aumentará linearmente para o próximo desafio, pois $L \leq M_T$. O processo continuará e esta estação receberá $k-1$ desafios antes de ser bloqueada.

Além da detecção e resposta ao mau comportamento em redes ad hoc, esta técnica oferece um mecanismo que forçam estações egoístas a compartilharem os seus recursos, pois receberão desafios e serão bloqueadas caso não se comportem cooperativamente na rede ad hoc. Por exemplo, uma estação egoísta que deixa de retransmitir pacotes recebe desafios que a bloqueia temporariamente, podendo sofrer um bloqueio definitivo com a reincidência de maus comportamentos.

3.3. Desafios Computacionais

Os desafios podem ser utilizados para punição de estações mau comportadas. O primeiro tipo de desafio são os *Human Interactive Proofs* (HIPs) [Rui e Liu, 2003], que dependem da intervenção humana para a sua realização. O tipo mais comum de HIP é o desafio onde uma pessoa deve digitar palavras contidas em uma imagem. Os desafios também podem

ser desafios computacionais. Neste artigo são utilizados apenas Desafios Computacionais, seguindo o mecanismo *hashcash* [Back, 2002]. Este mecanismo envia como desafio uma determinada seqüência de dados que deve ser trocada a cada desafio. Com base nesses dados, é requisitada uma seqüência de resposta que, concatenada ao desafio, resulte nos primeiros n bits iguais a zero quando for aplicada uma função *hash* no conjunto do desafio e resposta. O valor de n é escolhido com base no período de tempo que a estação deve passar resolvendo a função.

Se for escolhido um valor para n que resulte em desafios que demorem em torno de um minuto, a estação detectada como mau comportada deve resolver a função *hash* durante este intervalo de tempo. Caso contrário, ela será bloqueada da rede. Se a estação resolver o desafio, ela poderá participar da rede novamente. Na reincidência de mau comportamento, o próximo desafio será enviado com um tempo crescente exponencialmente ou linearmente, dependendo do valor da média calculado na punição anterior.

Neste contexto, surge o problema de uma estação mal comportada enviar desafios periódicos aos seus vizinhos para prejudicá-los. Para resolver este problema, é proposto que as estações vizinhas verifiquem se a estação que está punindo é mal comportada.

4. Considerações da Análise

Na análise das técnicas tolerante e intolerante de avaliação e punição ao mau comportamento foram definidos alguns valores para exemplificar o funcionamento e a eficiência das técnicas propostas. Para a análise foi utilizada a ferramenta Matlab 7.0 e os seguintes casos foram avaliados:

1. Para a distribuição geométrica foram definidos valores de p variando entre 0,25 e 1, com intervalos de 0,25. As funções de probabilidade de massa foram calculadas a partir de um número de eventos e variando entre 1 e 50, com intervalos de 1.

2. Para o cálculo da probabilidade de bloqueio da distribuição geométrica foi realizado o somatório de todos os valores da função de probabilidade de massa. Assim, foi obtida a função distribuição cumulativa para cada probabilidade de ocorrência de mau comportamento p.

3. Para a distribuição binomial negativa foi definido um valor de p fixo igual a 0,25. Para serem comparadas as tolerâncias, os valores de D foram variados entre 1 e 5 a partir dos eventos e, que variaram entre 1 e 50, ambos com intervalo de 1.

4. Atribuídos os valores na distribuição binomial negativa, a função probabilidade de massa pôde ser calculada para cada valor de D entre 1 e 5, com intervalos de 1 e p igual a 0,25. A partir destes resultados, a probabilidade de punição foi encontrada para cada valor de D. Desta forma, a probabilidade de bloqueio será proporcional a probabilidade de punição calculada por k vezes.

5. Resultados

Nesta seção, serão analisados e comentados os resultados obtidos a partir dos casos descritos na seção anterior. Em primeiro lugar são mostrados os resultados da função probabilidade de massa (PMF) da distribuição geométrica utilizada na técnica Intolerante.

Logo após, será apresentada a probabilidade de bloqueio encontrada a partir da PMF geométrica. Por conseguinte, será realizada a análise dos resultados da distribuição binomial negativa da técnica tolerante, através dos valores obtidos no cálculo da PMF, assim como a probabilidade de punição.

5.1. Técnica Intolerante

A Figura 2 mostra a função de probabilidade de massa da distribuição geométrica em função do número de eventos. Para um melhor entendimento foi variado o valor da probabilidade de ocorrência de maus comportamentos p. Este resultado permite observar o conjunto de probabilidades associadas a cada um dos possíveis valores da variável aleatória, seguindo uma distribuição geométrica.

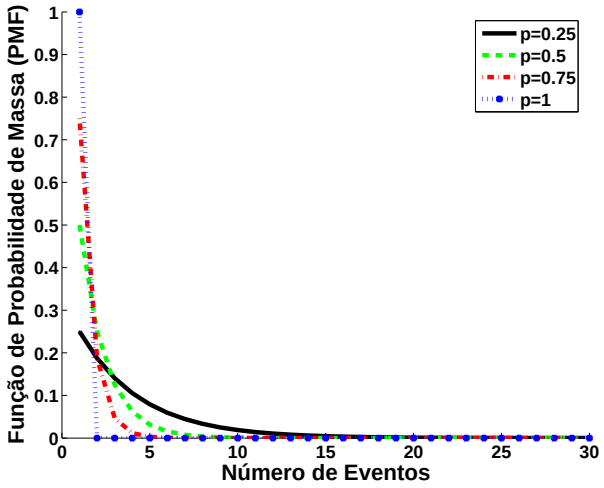

Figura 2. Função de probabilidade de massa da técnica intolerante.

A partir dos valores encontrados no gráfico da PMF, foi calculada a probabilidade de bloqueio para cada probabilidade p de realização de mau comportamento, através da função distribuição cumulativa (CDF) da distribuição geométrica, como mostrado na Figura 3. Com o cálculo de cada probabilidade de bloqueio para um valor de p é possível observar que quanto maior for a probabilidade de ocorrência de um mau comportamento, maior também será a probabilidade de bloqueio desta estação. De acordo com a Figura 3, a representação do valor igual a um significa que o primeiro evento desta estação foi mau comportado, logo será bloqueada no primeiro evento. Para o valor de p igual a 0,25 a curva cresce mais suavemente, significando que devem ser observados mais eventos antes de um bloqueio ser executado, pois a probabilidade de ocorrência de um mau evento é menor.

Na técnica intolerante existe uma forte tendência de bloqueios injustos na ocorrência de um falso-positivo nos primeiros eventos monitorados. Nesse caso, a média de ocorrência de maus comportamentos M_I é muito baixa e a estação será bloqueada injustamente, já que M_I tende a ser menor que L. Tendo em vista os problemas de injustiças deste tipo, a técnica Tolerante procura resolver o problema de injustiça observando mais eventos após a primeira detecção.

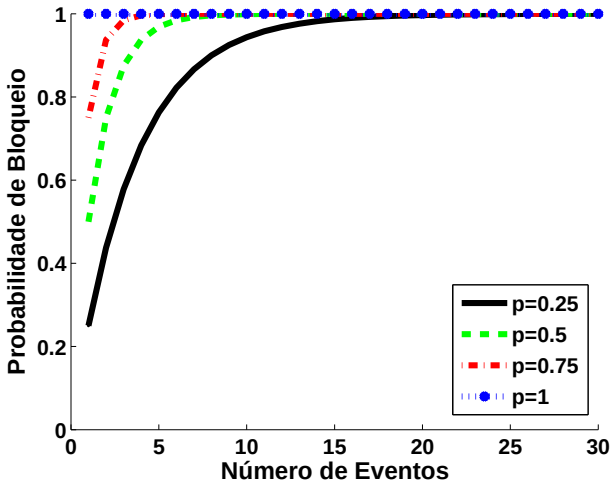

Figura 3. Probabilidade de bloqueio da técnica intolerante.

5.2. Técnica Tolerante

Para a técnica tolerante, a Figura 4 apresenta os resultados obtidos para cada valor de D assumindo que a probabilidade de ocorrência de um mau comportamento p é igual a 0,25. Desta forma, foram encontrados os valores da função de probabilidade de massa pra cada valor de D, que permitiram o cálculo da probabilidade de punição.

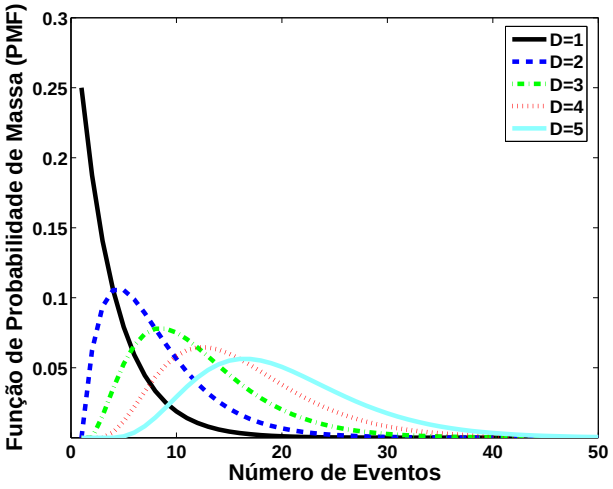

Figura 4. Função de probabilidade de massa da técnica tolerante.

Com o objetivo de evitar injustiças como a citada em 5.1, a técnica tolerante usa a distribuição binomial negativa e observa mais eventos após o primeiro mau comportamento detectado. De acordo com a Figura 5 é possível observar que se o valor de D for igual a um, a probabilidade de punição seguirá a mesma curva da distribuição geométrica,

como demonstrada nas Equações 7 e 8:

$$\begin{aligned} F(e) &= \binom{e-1}{D-1} p^D (1-p)^{e-D} \\ F(e) &= \binom{e-1}{1-1} p^1 (1-p)^{e-1} \\ F(e) &= p(1-p)^{e-1}, \end{aligned} \tag{7}$$

logo

$$P_P(e) = P_B(e) = \sum_{1}^{e} F(e). \tag{8}$$

Por outro lado, quando o valor de D é maior que um, a técnica segue de acordo com a curva da distribuição binomial negativa, tendendo a observar mais eventos antes da execução de a punição e, consequentemente, o bloqueio.

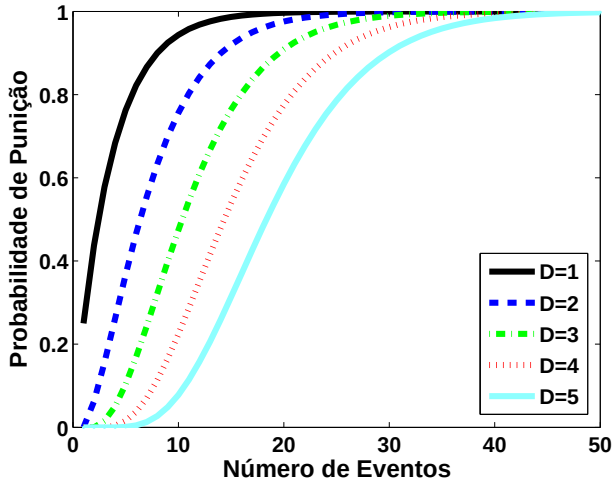

Figura 5. Probabilidade de punição da técnica tolerante.

A partir dos resultados obtidos da análise matemática das duas técnicas, pode-se observar que ambas possuem características que aumentam a eficiência de detecção de mau comportamento em redes ad hoc. Entretanto, a técnica tolerante se mostra mais precisa na punição de estações mal comportadas, evitando punições injustas aos falso-positivos devido a observação de mais eventos antes de executar um bloqueio. Nota-se ainda que, ao utilizar a técnica tolerante, existe um mecanismo que força a participação de estações egoístas na rede, oferecendo outras oportunidades de se comportarem corretamente na rede.

6. Conclusões e Trabalhos Futuros

Este trabalho propõe técnicas de avaliação e punição a estações mal comportadas, capazes de comprometer o desempenho das redes ad hoc. Estas técnicas sugerem duas formas de realizar punições, tentando reduzir a quantidade de bloqueios de estações bem comportadas que foram detectadas como mal comportadas devido a algum erro. A primeira técnica

proposta, descreve uma técnica intolerante de executar as punições, podendo bloquear a estação a partir da primeira detecção de mau comportamento. O bloqueio é determinado através da comparação de um limiar L e uma média de bons eventos até a ocorrência de um mau evento. A segunda técnica, chamada de tolerante, permite que as estações executem D maus comportamentos para depois aplicar uma punição. É considerado que a cada D maus comportamentos a estação recebe uma punição através de desafios computacionais, podendo reincidir por $k - 1$ vezes até se bloqueada no instante k. Esta técnica também compara um limiar L com uma média M_T de ocorrências de maus comportamentos, porém esse limiar é utilizado para definir o tempo de resolução do desafio computacional que será enviado.

As técnicas propostas podem ser utilizadas nos dois modelos de detecção de maus comportamentos, o baseado em assinaturas e o baseado em anomalias. Entretanto, as técnicas têm resultados mais significativos nos modelos baseados em anomalias, pois a ocorrência de falso-positivos tende a ser maior [Zhang e Lee, 2000]. Além disto, os resultados da análise matemática mostraram que a técnica tolerante força a cooperação de estações egoístas a colaborarem com a rede. Caso isto não ocorra, as estações egoístas tendem a passar muito tempo resolvendo desafios computacionais sem utilizar a rede, até que sejam bloqueadas em k reincidências.

Como trabalhos futuros serão realizadas análises em redes ad hoc através de simulações e testes em ambientes reais. Para isto serão consideradas a ocorrências de falso-positivos devido a utilização dos modelos de detecção de mau comportamento em redes ad hoc. Além disso, serão simulados alguns tipos de ataques para verificar a eficiência das técnicas de avaliação e punição em não bloquear estações bem comportadas e bloquear as estações mal comportadas.

Referências

Back, A. (2002). Hash cash - a denial of service counter-measure. Relatório técnico, http://www.cypherspace.org/hashcash/.

Buchegger, S. e Boudec, J.-Y. L. (2002). Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. Em *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing*, p. 403–410, Canary Islands, Spain. IEEE Computer Society.

Fernandes, N. C., Moreira, M. D. D., Velloso, P. B., Costa, L. H. M. K. e Duarte, O. C. M. B. (2006). Ataques e mecanismos de segurança em redes ad hoc. Em *Minicursos do Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais - SBSeg'2006*, p. 49–102, Santos, SP, Brazil. Sociedade Brasileira de Computação–SBC.

He, Q., Wu, D. e Khosla, P. (2004). SORI: A secure and objective reputationbased incentive scheme for ad-hoc networks. Em *Proc. of IEEE Wireless Communications and Networking Conference (WCNC2004)*, volume 2, p. 825–830. IEEE Computer Society.

Hu, Y.-C. e Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security and Privacy Magazine*, 2(3):28–39.

Johnson, D. B. e Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. Em *Mobile Computing*, volume 353, p. 153–181. Mobile Computing (ed. T. Imielinski and H. Korth), Kluwer Academic Publishers.

Kang, D.-K. e an Honavar V., F. D. (2005). Learning classifiers for misuse and anomaly detection using a bag of system calls representation. Em *Systems, Man and Cybernetics Information Assurance Workshop*, p. 118–125. IEE Computer Society.

Liu, Y., Li, Y. e Man, H. (2006). A distributed cross-layer intrusion detection system for ad hoc networks. *Annales des Télécommunications*, 61(3-4):357–378.

Maccabe, R. H. G. L. A. e Servilla, M. (1990). The architecture of a network level intrusion detection system. Relatório Técnico CS90-20, University of New Mexico, Department of Computer Science.

Marti, S., Giuli, T. J., Lai, K. e Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. Em *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, p. 255–265, New York, NY, USA. ACM Press.

Moler, C. B. (1980). Matlab – an interactive matrix laboratory. Relatório Técnico 369, University of New Mexico. Dept. of Computer Science.

Patwardhan, A., Parker, J., Joshi, A., Iorga, M. e Karygiannis, T. (2005). Secure routing and intrusion detection in ad hoc networks. Em *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, p. 191–199, Washington, DC, USA. IEEE Computer Society.

Rui, Y. e Liu, Z. (2003). Excuse me, but are you human? Em *MULTIMEDIA '03: Proceedings of the eleventh ACM international conference on Multimedia*, p. 462–463, New York, NY, USA. ACM Press.

Zhang, Y. e Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. Em *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, p. 275–283, New York, NY, USA. ACM Press.