

Um Sistema de Reputação Fuzzy para Segurança Orientada a Serviços em Redes de Banda Larga sem Fio

Alexandre Gomes Lages¹, Flávia C. Delicato², Luci Pirmez¹

¹Universidade Federal do Rio de Janeiro – Núcleo de Computação Eletrônica
Prédio do CCMN - Bloco C, Caixa Postal: 2324 - CEP: 20.010-974

Cidade Universitária - Ilha do Fundão, Rio de Janeiro, RJ

²Universidade Federal do Rio Grande do Norte – Departamento de Informática e Matemática Aplicada

Campus Universitário Lagoa Nova, 59072-970, Natal, RN

{alexandrelages, luci}@nce.ufrj.br, flavia.delicato@dimap.ufrn.br

Abstract. *The increasing development of the Wireless MAN technologies will allow the exchange of services directly among subscriber stations. Schemes to assure the safety of services should preferably adopt a distributed architecture, such as the Reputation System architectures, commonly used in P2P, in order to keep the network scalability. This work proposes the use of a service oriented Reputation System based on fuzzy logic, as a solution for increasing the safety level of a Wireless MAN.*

Resumo. *O desenvolvimento da tecnologia de Redes Sem Fio Metropolitanas permitirá que novos serviços sejam oferecidos diretamente entre estações-assinantes. Os esquemas adotados para garantir a segurança destes serviços devem utilizar uma arquitetura distribuída, como a dos Sistemas de Reputação, usados em redes P2P, de forma a não comprometer a escalabilidade da rede. Este artigo propõe o uso de um Sistema de Reputação orientado a serviços e baseado em lógica nebulosa, como forma de aumentar o nível de segurança de uma Rede Sem Fio Metropolitana*

1. Introdução

O padrão IEEE (*Institute of Electrical and Electronics Engineers*) para redes metropolitanas (MANs) sem fio 802.16 deverá ter um papel importante como solução para o acesso banda larga sem fio às redes IP, através de uma redução significativa de investimentos de infraestrutura necessários, de uma imediata facilitação da distribuição do acesso, e de um conseqüente barateamento do serviço para os usuários finais. Entretanto, para que estes objetivos sejam atingidos é necessário o suporte de uma infra-estrutura de segurança para o acesso e a troca de serviços entre as estações.

A segurança de acesso disponível nessas redes baseia-se na utilização da subcamada de segurança definida no padrão IEEE 802.16, denominada *Privacy Sublayer*, que provê mecanismos de autenticação e criptografia das mensagens em nível de enlace. Entretanto, se faz necessária a existência de primitivas que possam ser utilizadas pelas aplicações, para o incremento da segurança ao nível de utilização de serviços entre as estações. Os modelos baseados em Sistemas de Reputação [1, 2, 3] são bastante utilizados em redes *Peer-to-Peer* (P2P) e se baseiam em interações prévias ocorridas entre os *peers*. Para o cálculo da reputação podem ser utilizados métodos estatísticos ou Lógica Nebulosa (*Fuzzy Logic*). A Lógica Nebulosa proporciona a realização do cálculo da reputação de um *peer* através da utilização de um conjunto de regras do tipo *se-então*, de forma que o seu desenvolvimento possa ser realizado em um curto espaço de tempo.

Após um *peer* utilizar um serviço de outro, é atribuído ao *peer* um conceito pela utilização deste serviço. De acordo com as interações passadas e com os conceitos que um *peer* possui, pode ser gerado um indicador sobre possíveis ações que um *peer* pode realizar no futuro. Dessa maneira, como a reputação é formada a partir da opinião de outros *peers*, um problema que pode afetar os Sistemas de Reputação é a possibilidade da formação de **Conluíus**, que é a organização de um grupo de *peers* que visa aumentar ou diminuir a reputação de um ou vários *peers* da rede.

Neste trabalho propõe-se a utilização de um Sistema de Reputação com uma abordagem orientada a serviço em uma MAN sem fio do tipo *Mesh*, como uma forma de aumentar o nível de segurança dessas redes, através da realização do cálculo da reputação atribuída ao par *peer-serviço*. Em um ambiente de serviços existirão comunidades específicas que utilizam um determinado serviço, como por exemplo, comunidade de usuários de Vídeo-Conferência e comunidade de Voz sobre IP, e um *peer* pode pertencer a uma ou várias destas comunidades. Para o cálculo da reputação atribuída ao par *peer-serviço* são utilizados os valores de reputação dos *peers* não somente dentro de uma comunidade (denominada **Reputação Local**), mas os valores obtidos de todas as comunidades a que este pertence (**Reputação Agregada**). Outra contribuição importante é a utilização de um filtro no momento de atualização da reputação de um *peer*, evitando-se assim, que um determinado valor de reputação diminua consideravelmente a reputação de um *peer*, sem levar em consideração o seu histórico de reputações.

Este artigo está organizado em quatro seções. A Seção 2 apresenta o modelo de segurança distribuído proposto para redes de banda larga sem fio com topologia *Mesh*. Na Seção 3 é apresentada a forma como é calculado o grau de reputação do par *peer-serviço*, através da utilização de Lógica Nebulosa. Por fim, a Seção 4 apresenta as considerações finais.

2. Modelo de Segurança para Redes Metropolitanas Sem Fio de Banda Larga

Nas redes sem fio metropolitanas que seguem o padrão IEEE 802.16 foram definidas quatro classes de serviços, a saber: (i) serviço de concessão não solicitada (*Unsolicited Grant Service* - UGS); (ii) serviço para aplicações em tempo real (*Real-Time Polling Service* - rtPS); (iii) serviço para aplicações que não necessitam de tempo real (*Non-Real-Time Polling Service* - nrtPS); e (iv) serviço para aplicações de encaminhamento de tráfego através do melhor esforço (*Best Effort Service* - BE). Cada *peer* pode estar associado a uma ou mais classes de serviços. Um *peer* associado a uma dada classe de serviço pode apresentar um comportamento diferente quando associado a uma outra classe de serviço. Consequentemente, esse *peer* possuirá valores de reputação diferentes para cada classe de serviço ao qual está associado.

No Sistema de Reputação com abordagem orientada a serviço proposto, o cálculo do valor da reputação é função do uso de um serviço por um *peer*. As informações sobre as interações com outros assinantes são armazenadas nos *peers* em uma base de reputação local, denominada **Tabela Grau de Reputação de Serviço**. Esta tabela possui quatro campos: um campo para identificar a classe de serviço (IDS); um campo para identificar o *peer* (IDP); um campo contendo o grau de **Reputação** desse *peer* em relação a essa classe de serviço; um campo representado o grau de **Relacionamento** do *peer* que está armazenando a tabela em relação a esse *peer*.

Para a realização da busca de mensagens na rede, uma vez que os valores de reputação estão distribuídos entre os *peers*, um requisito importante é a necessidade da recuperação rápida das reputações distribuídas pelas estações. Neste trabalho, o protocolo *Chord* [4] foi adotado como mecanismo de busca da informação referente à reputação de um dado par *peer-serviço*.

3. Cálculo da Reputação utilizando Lógica Nebulosa

Para o cálculo da reputação de um *peer* são utilizadas as informações referentes aos graus armazenados nos campos Reputação e Relacionamento da Tabela Grau de Reputação de Serviço. Um *peer*, ao receber a solicitação de um serviço, envia requisições para os *peers* identificados pelas chaves retornadas pelos algoritmos de *hash* e também para os *peers* considerados “Amigos” (Alto Grau de relacionamento) em sua Tabela Grau de Reputação de Serviço, em busca de informações de reputação do *peer* solicitante do serviço. Ao receber os valores sobre a reputação do *peer* solicitante, o *peer* hospedeiro do serviço deverá consultar a sua Tabela Grau de Reputação de Serviço e recuperar os graus de Relacionamento sobre os *peers* que retornaram os valores das reputações. De posse das informações recebidas, o *peer* hospedeiro do serviço pode realizar o cômputo da reputação do *peer* solicitante do serviço. Cabe aqui lembrar que os valores de reputação retornados referem-se sempre ao par *peer-serviço* solicitado. O valor da reputação do *peer* solicitante será, então, calculado a partir dos graus de reputação retornados em relação a esse *peer* e do valor do grau de relacionamento que o *peer* hospedeiro do serviço tem dos *peers* que retornaram a informação de reputação. Quando o grau de Relacionamento é baixo, ou seja, refere-se a um *peer* desconhecido, por exemplo, o valor da reputação retornado por esse *peer* terá uma influência baixa no cálculo da reputação do *peer* solicitante.

Para realizar o cálculo da reputação **Agregada** de um *peer*, todos os valores de reputação que o *peer* possui nas quatro classes de serviço são agregados e um valor único de reputação é gerado. Como citado na Seção 2, as classes de serviço possuem prioridades diferentes: a classe de serviço UGS possui prioridade mais alta, enquanto que a classe de serviço BE possui prioridade mais baixa dentre as quatro. Assim, um *peer* que possui uma reputação alta na classe BE (Baixa Prioridade) e um valor baixo na classe UGS (Alta Prioridade) pode ter como resultado um valor baixo de reputação **Agregada**. Para realizar o cálculo da reputação **Agregada** do *peer*, utiliza-se uma média ponderada dos valores das reputações nas classes de serviço que o *peer* já utilizou. Por motivos de restrição de espaço, a discussão quanto ao momento do disparo do processo de avaliação de um Peer após a Utilização de um Serviço está fora do escopo desse trabalho.

Cada *peer* é responsável por manter a Tabela Grau de Reputação de Serviço contendo os valores de reputação e relacionamento de outros *peers* e estes valores serão atualizados de acordo com a frequência com que os *peers* utilizam os serviços existentes na rede. Um *peer* pode receber valores de reputação de diversos *peers* existentes na rede. Para evitar que a tabela seja alterada por *peers* que estão em processo de formação de conluio na rede, antes do armazenamento dos valores na tabela, os mesmos são primeiramente avaliados quanto à natureza da distribuição de todos os valores de reputação recebidos e, em seguida, aplica-se um filtro para o cálculo e armazenamento final da reputação na tabela.

O procedimento responsável pelo cálculo da reputação de um *peer* baseia-se em Lógica Nebulosa e é denominado de “Cálculo de Reputação Nebuloso”. No presente trabalho, o “Cálculo de Reputação Nebuloso” foi implementado no ambiente *Matlab*, utilizando-se o FIS Editor. A primeira etapa na execução do cálculo compreende a definição das variáveis nebulosas, bem como dos conjuntos nebulosos referentes a cada uma das variáveis nebulosas consideradas. Neste trabalho, as definições, tanto das variáveis como dos conjuntos nebulosos, foram feitas a partir de um refinamento do próprio procedimento obtido na fase de testes, através de simulações iniciais. A superfície (a) da Figura 1 sintetiza graficamente as regras usadas e apresenta o valor retornado da reputação em função dos valores de reputação e relacionamento do mesmo. A superfície (B) apresenta o peso de um determinado *peer*

(representado pela variável α) que são gerados, a partir do valor de relacionamento e reputação recebidos de um *peer*. Esta superfície foi gerada através da criação de uma máquina de inferência nebulosa com variáveis de entrada Grau-Reputação (variáveis lingüísticas: Muito Alto, Alto, Médio, Baixo e Muito-Baixo) e Grau-Relacionamento (variáveis lingüísticas: Amigo, Colega e Desconhecido) e variáveis de saída Reputação-Final e Alfa no intervalo [0,1].

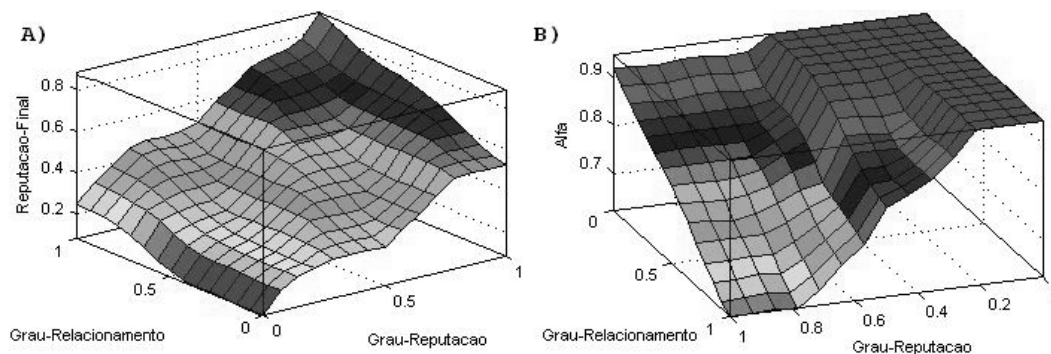


Figura 1 - Superfície para o Cálculo da Reputação (A) e Alfa (B)

4. Considerações Finais

Este trabalho propôs uma nova abordagem para aumentar o nível de segurança em redes de banda larga sem fio. As características inovadoras da proposta são: (i) a utilização de um modelo de reputação, como os comumente adotados em redes P2P, para tratar do controle do acesso aos serviços oferecidos na rede; (ii) a adoção de uma abordagem orientada a serviços, que permite atribuir níveis de confiabilidade não somente a estações (*peers*) isoladas, mas ao par *peers*-serviço utilizado; e (iii) o uso de lógica nebulosa para o cálculo das reputações atribuídas aos pares *peers*-serviço. O mecanismo para a troca de mensagens contendo os valores de reputação referentes aos pares *peer*-serviço baseou-se em um protocolo conhecido, o qual, porém, foi incrementado com etapas adicionais, tirando proveito da existência de uma rede de relacionamento entre os *peers*. Os valores de reputação referentes a cada par *peer-serviços* são alterados dinamicamente, de acordo com os resultados das interações entre os *peers*. A atualização de tais valores baseia-se em mecanismos que buscam evitar ou minimizar a formação de conluíus na rede e, ao mesmo tempo, reduzir o grau de oscilação nos valores de reputação armazenados.

5. Referências

- [1] Resnick, P., Zeckhauser, R., Friedman, E. and Kuwabara, K. (2000) "Reputation Systems". In: Communications of the ACM, Vol. 43, December.
- [2] Song, S., Hwang, k., Kwok, Y. and Zhou, R. (2005) "Trusted P2P Transactions with Fuzzy Reputation Aggregation". In: Security in P2P Systems, IEEE Internet Computing, November-December.
- [3] Kamvar, S., Schlosser, M. and Garcia-Molina, H. (2003) "The EigenTrust Algorithm for Reputation Management in P2P Networks". In Proceedings of the Twelfth International World Wide Web Conference, May.
- [4] Stoicay, I., Morrisz, R., Liben-Nowellz, D., Kargerz, R. Kaashoekz, M., Dabekz, F., (2003) "Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications". In: IEEE/ACM Transactions on Networking, ACM Press, vol. 11, no. 1, pp. 17-32.