Um esquema bio-inspirado para a tolerância à má-conduta em sistemas de quórum para MANETs

Elisa Mannes, Michele Nogueira, Aldri Santos

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2)
Universidade Federal do Paraná – Curitiba – Brasil

{elisam, michele, aldri}@inf.ufpr.br

Abstract. *Network operation services in MANETs, such as resource location, deal with node mobility and lack of resources to support applications. The reliability and availability of these services can be assured by replication techniques, such as quorum systems. However, these systems are vulnerable to selfish and malicious nodes, that either intentionally do not collaborate with replication operations or spread malicious data while participating in data replication. In order to handle these issues, this paper proposes QS^2, a bio-inspired scheme to tolerate selfish and malicious nodes in replication operation of quorum systems. Differently from existing works on the literature, QS^2 is distributed and self-organized, and nodes are independent to exclude misbehaving nodes. It is inspired in quorum sensing and kin selection, both biological mechanisms resident in bacteria. Simulation results show that QS^2 increases 87% the reliability of a quorum system for MANETs, detecting more than 80% of misbehaving nodes participating in replication operations.*

Resumo. *Os serviços de operação das redes em MANETs, como a localização de recursos, precisam lidar com a mobilidade e a falta de recursos dos dispositivos a fim de suportar as aplicações. Esses serviços necessitam de garantias de disponibilidade e de confiabilidade, que podem ser obtidas pela replicação de dados através de sistemas de quóruns. Contudo, esses sistemas são vulneráveis a nós egoístas e maliciosos, que não colaboram com suas operações ou modificam as informações, negando os serviços da rede. Para lidar com essas vulnerabilidades, esse artigo propõe QS^2, um esquema bio-inspirado para a tolerância de nós de má-conduta em sistemas de quórum. Diferentemente dos sistemas existentes na literatura, o QS^2 é auto-organizado e distribuído, permitindo uma autonomia na exclusão de nós de má-conduta. Ele é inspirado nos mecanismos biológicos de sensoriamento em quóruns e de seleção por parentesco encontrados em bactérias. Resultados de simulações mostram um aumento de até 87% na confiabilidade dos sistemas de quórum, detectando mais de 80% da participação de nós de má-conduta nas operações de replicação.*

1. Introdução

Devido aos recentes avanços das tecnologias de comunicação sem fio, a operacionalização de várias aplicações críticas, como as aplicações relacionadas à segurança nas rodovias, à segurança militar e ao apoio a situações de emergência podem ser mediadas pelas redes *ad hoc* móvel (MANETs). Porém, a mobilidade e a escassez de recursos dos dispositivos (nós), características peculiares das MANETs, podem ocasionar o particionamento da

rede. Além disso, a dependência na colaboração dos nós pode tornar as aplicações indisponíveis ou resultar em informações desatualizadas [Zhang et al. 2008]. Dessa forma, a confiabilidade da rede é comprometida, e as consequências da falta de informação ou de informações desatualizadas podem inutilizar a rede. Uma das formas de tolerar as falhas causadas pelas características da rede é por meio da redundância das informações, obtida através das técnicas de replicação dos dados [Derhab and Badache 2009].

Dentre as técnicas de replicação para garantir a disponibilidade dos dados e a tolerância a falhas em MANETs destacam-se os sistemas de quórum. Estes sistemas são uma forma efetiva de replicação, garantindo tanto a consistência quanto a disponibilidade dos dados. Os sistemas de quórum consistem em conjuntos de nós que se intersectam, e cada operação de leitura e de escrita acontece em apenas um dos conjuntos (quóruns) [Malkhi and Reiter 1997]. Entre as vantagens de seu uso, comparado com outros modelos de replicação, estão a economia de recursos computacionais e de comunicação, o que torna esses sistemas atraentes às MANETs. Os sistemas de quórum que se baseiam na construção probabilística da intersecção dos quóruns são os mais adequados às MANETs, pois diminuem o uso de recursos e tornam a replicação mais dinâmica [Luo et al. 2003].

Contudo, os sistemas de quórum probabilísticos propostos para MANETs apresentam vulnerabilidades que resultam em uma perda na confiabilidade dos dados diante de nós egoístas e nós maliciosos nas operações de replicação [Mannes et al. 2009]. Os nós egoístas buscam a economia de seus recursos e assim não colaboram com as operações, enquanto que os nós maliciosos têm como objetivo a negação do serviço da rede, injetando dados falsos ou modificando o comportamento da replicação. Para serem empregados de forma confiável no apoio aos serviços de operação de rede, os sistemas de quórum precisam evitar que os nós de má-conduta interfiram em seu funcionamento.

Apesar de existirem sistemas de quórum tolerantes a nós de má-conduta [Malkhi and Reiter 1997], tais sistemas assumem a existência de uma infraestrutura fixa e canais de comunicação confiáveis, atributos que não são encontrados em uma MANET e que tornam inviável o uso de tais sistemas nesse tipo de rede. Uma forma de auxiliar os sistemas de quórum a evitar a interação com os nós de má-conduta é por meio do uso de sistemas de detecção de nós de má-conduta [Yang et al. 2002, Zhu et al. 2007]. Porém, a maioria deles divulga a recomendação sobre um nó para todos na rede, gerando uma sobrecarga de mensagens, ou utiliza entidades centralizadas, que não são adequadas para as MANETs. Desta maneira, é necessário proporcionar a tolerância a nós de má-conduta nos sistemas de quórum, preferencialmente de forma descentralizada e com o uso de poucos recursos. Essas características são naturalmente encontradas em diversos sistemas biológicos, e assim, projetar soluções inspiradas neles facilita a inclusão de características como a descentralização e a autonomia necessárias em MANETs.

Este trabalho propõe o QS^2 (*quorum systems + quorum sensing*), um esquema inspirado nos mecanismos biológicos encontrados em bactérias, para a tolerância de nós de má-conduta nas operações de sistemas de quórum em MANETs. Diferente de outras propostas encontradas na literatura, o QS^2 detecta nós egoístas e nós maliciosos por meio da análise autônoma do comportamento de cada nó, e de forma auto-organizada evita que eles façam parte da replicação dos dados. Os resultados de simulação mostram que o QS^2 garante pelo menos 80% de confiabilidade dos dados em um sistema de quórum probabilístico para MANETs diante de nós maliciosos em operações de escrita, e detecta

mais de 80% da ação desses nós com uma taxa de falsos positivos inferior a 2%. A confiabilidade garantida pelo QS^2 é aceitável para a replicação de dados em aplicações cujo o requisito por disponibilidade sobrepõe o custo de lidar com eventuais inconsistências.

O restante do artigo está organizado como descrito a seguir. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 define o modelo do sistema e as asserções consideradas no esquema proposto. A Seção 4 descreve o esquema QS^2, seus módulos e suas funções. A Seção 5 apresenta os resultados do desempenho e da eficiência do QS^2, obtidos por meio de simulação. A Seção 6 conclui o artigo e apresenta os trabalhos futuros.

2. Trabalhos Relacionados

Os sistemas clássicos de replicação de dados [Saito and Shapiro 2005] têm como característica comum o uso de servidores estáticos, a garantia de entrega e a ordenação das mensagens de replicação. A tolerância de nós de má-conduta nesses sistemas é garantida pela validação das operações por pelo menos $t + 1$ nós, em que t é a quantidade de nós de má-conduta presente na rede [Malkhi and Reiter 1997]. Esses sistemas requerem que a quantidade de nós bons sobreponha a quantidade de nós de má conduta a fim de evitar que eles prejudiquem a replicação. Além disso, esses sistemas trocam várias mensagens entre os nós para a conclusão de uma operação, o que gera uma sobrecarga na rede. Por estas razões, esses sistemas clássicos não são aplicáveis em MANETs, visto que estas redes não conseguem garantir os requisitos básicos para o funcionamento correto da tolerância a falhas necessários a esse tipo de replicação.

A replicação por sistemas de quórum é a mais adequada para ambientes dinâmicos como as MANETs. Estes sistemas tendem a diminuir a quantidade de recursos de processamento e de comunicação usados na replicação [Malkhi and Reiter 1997]. Os sistemas de quórum específicos para as MANETs diminuem ainda mais o uso de recursos através da escolha probabilística dos quóruns [Luo et al. 2003]. Entretanto, apesar de existirem sistemas de quórum probabilístico tolerantes aos nós de má-conduta [Malkhi et al. 1998], esses sistemas possuem os mesmos requisitos que os sistemas clássicos, como a garantia de entrega das mensagens, sendo que as características das MANETs tornam esse modo de tolerância a falhas inviável para o uso na replicação de serviços.

Os sistemas de replicação para MANETs [Bellavista et al. 2005] geralmente tratam da segurança com o auxílio de mecanismos de detecção de má-conduta, como os sistemas de reputação [Salmon et al. 2010] Contudo, muitos desses sistemas dependem da confiança entre os nós para a troca de mensagens de detecção, o que pode ser explorado por nós de má-conduta através do envio de informações falsas. Abordagens para a detecção de injeção de dados falsos [Zhu et al. 2007] estão consolidadas na replicação de dados em redes de sensores sem fio, devido ao foco que essas redes mantém na coleta de dados. A validação dos dados geralmente ocorre por meio de criptografia, da verificação dos dados por uma determinada quantidade de nós ou ainda pelo uso de *firewalls*. Porém, esses sistemas utilizam entidades centrais, o que pode ser aceitável para alguns tipos de rede, mas trazem limitações para redes descentralizadas como as MANETs.

Apesar dos sistemas de detecção de nós de má-conduta apresentarem separadamente características de autonomia, descentralização e uso de poucos recursos, nenhum deles as compreende na mesma solução. Além disso, nenhuma solução é capaz de mitigar nós egoístas e maliciosos isoladamente. Devido às suas características, as MANETS

necessitam que atributos como a auto-organização, a autonomia e o uso de poucos recursos estejam incorporados nessas soluções. Essas características são encontradas em várias soluções bio-inspiradas, como protocolos de roteamento inspirados em colônias de formigas, ou sistemas de detecção de ataques inspirados no sistema imunológico humano [Meisel et al. 2010]. Assim, o esquema proposto é inspirado nos sistemas biológicos, de forma a aproveitar as vantagens oferecidas por esses sistemas.

3. Modelo do sistema

Esta seção descreve as suposições e os modelos assumidos para a definição do esquema proposto. Primeiramente são apresentados os sistemas de quórum probabilísticos para MANETs. Também são definidos o modelo de rede empregado e o modelo de má-conduta que pode afetar esses sistemas. Por fim, são descritos os conceitos de sensoriamento em quórum e seleção por parentesco, que são utilizados como inspiração para o esquema.

3.1. Sistema de quórum probabilístico para MANETs

O sistema de quórum probabilístico é caracterizado pela escolha probabilística dos quóruns, que são conjuntos de nós que realizam a replicação. Nesse caso, o sistema garante que quóruns de leitura e de escrita, ambos selecionados aleatoriamente, se intersectem com uma dada probabilidade. Em geral, os sistemas de quórum para MANETs [Luo et al. 2003, Tulone 2007, Gramoli and Raynal 2007] têm seu fundamento nos quóruns probabilísticos, e portanto, compartilham as mesmas características. Apesar de existirem vários sistemas de quórum para as MANETs, o PAN (*probabilistic quorum system for ad hoc networks*) [Luo et al. 2003] foi escolhido neste estudo para representar os sistemas de quórum probabilísticos para MANETs, pois propõe o uso de um número reduzido de mensagens para a replicação ao introduzir o conceito de quóruns assimétricos, além de acessar os quóruns de leitura e de escrita de forma distinta. No PAN, o acesso ao quórum de leitura é realizado por mensagens *unicast*, endereçada para cada nó do quórum de leitura, enquanto que os quóruns de escrita são acessados por meio do protocolo *Gossip*, em que um nó envia as escritas para o quórum de escrita com a ajuda dos outros nós.

3.2. Modelo de rede

Assume-se que a rede é formada por um conjunto P composto por n nós identificados por $\{s_0, s_1 \ldots s_{n-1}, s_n\}$, sendo que cada nó $s_n \in P$ tem um endereço físico e um identificador único. Os nós são similares quanto ao poder de processamento e a quantidade de energia disponível. Eles se comunicam através de um canal sem fio, cujo raio de transmissão é igual para todos. Considera-se que a comunicação entre os nós é assíncrona, isto é, o tempo de transmissão é variável e desconhecido. O canal de comunicação não é confiável, e está sujeito à perda de pacotes devido a colisões ou à entrada e saída de nós, que também pode causar a partição da rede.

Os nós não possuem conexão com todos os outros, e deste modo, as mensagens precisam ser roteadas por nós intermediários até o destino. Supõe-se que o roteamento e as camadas inferiores não sofram interferências de nós de má-conduta. Da mesma forma, assume-se que as mensagens contendo os dados replicados são relativamente pequenas e enviadas em pacotes únicos. Além disso, assume-se que a rede fornece um esquema de assinatura para a autenticação de informações importantes enviadas pelo QS^2.

O esquema proposto é aplicado em sistemas de quórum do tipo probabilístico para MANETs, utilizado para a replicação dos dados dos serviços de operação de rede, tais como informações de localização e de mobilidade.

3.3. Modelo de má-conduta

Considera-se que os nós de má-conduta têm como objetivo afetar as propriedades de disponibilidade e de integridade dos dados em um sistema de replicação por quóruns. Esses nós de má-conduta são intrusos e conhecem o funcionamento da rede, tendo permissão e acesso à chaves criptográficas para participar das operações. Assume-se dois tipos de nós de má-conduta: os nós egoístas e os nós maliciosos. Um nó egoísta não colabora com as operações de replicação. Um nó malicioso modifica ou injeta dados maliciosos no sistema de replicação, ou ainda atrasa a propagação dos dados. Um nó pode ser egoísta ou malicioso, ou apresentar ambos os comportamentos ao mesmo tempo. Assume-se que um nó de má-conduta se comporta de modo egoísta ou malicioso durante toda a sua participação na rede, todas as vezes em que for consultado. Além disso, os nós egoístas e maliciosos agem sempre que forem consultados por algum outro nó do sistema, tanto nas operações de leitura como de escrita.

3.4. Sensoriamento em quórum e seleção por parentesco

Na Biologia, o sensoriamento em quórum é um mecanismo biológico de comunicação entre bactérias fundamentado na produção e na detecção de produtos químicos extracelulares chamados de **autoindutores**. Os autoindutores agem como um sinalizador da quantidade de bactérias presentes no ambiente, e permite que elas desenvolvam um comportamento vantajoso para o grupo, dependente da quantidade de bactérias no ambiente [Ng and Bassler 2009]. Porém, esse mecanismo é vulnerável a bactérias egoístas e maliciosas, que não desejam ter o custo metabólico da produção de autoindutores, ou prejudicam o sensoriamento enviando autoindutores modificados. Uma das teorias aceitas para a sobrevivência do sensoriamento em quórum ao ataque de tais bactérias é pela seleção por parentesco, permitindo que as bactérias deem preferência a interagir com aquelas que compartilham o mesmo **material genético**, e tem maiores chances de se comportar corretamente. Dessa forma, as bactérias egoístas e maliciosas são excluídas do processo de sensoriamento. Em conjunto, o sensoriamento em quórum e a seleção por parentesco formam uma solução dinâmica e independente, e são a base para o esquema proposto.

4. QS^2 - esquema bio-inspirado para tolerância a nós de má-conduta

O esquema QS^2 (*quorum system* + *quorum sensing*) tem como objetivo auxiliar os sistemas de quórum para MANETs a excluir os nós de má-conduta das operações de replicação, construindo quóruns com participantes que não prejudiquem as operações. Diferente dos sistemas de detecção propostos, o QS^2 é autônomo e auto-organizado, e não troca informações de reputação entre os nós. A seleção de nós participantes tem como base a observação individual da quantidade de operações de escritas de dados e de encaminhamentos de escritas realizadas, e não depende de informações adquiridas de outros nós. O esquema é composto por dois módulos: o módulo de seleção de nós e o módulo de decisão, conforme ilustra a Figura 1.

O *módulo de seleção de nós* é responsável pela classificação dos nós como bons ou de má-conduta. Esse módulo é subdividido em dois componentes: a contagem de

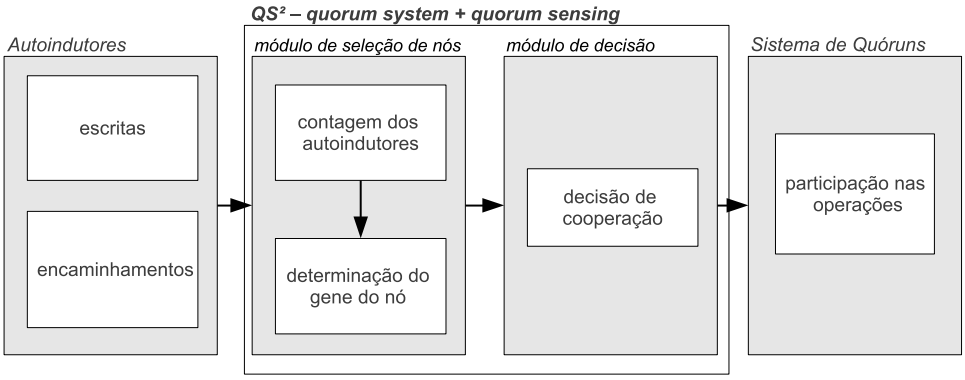


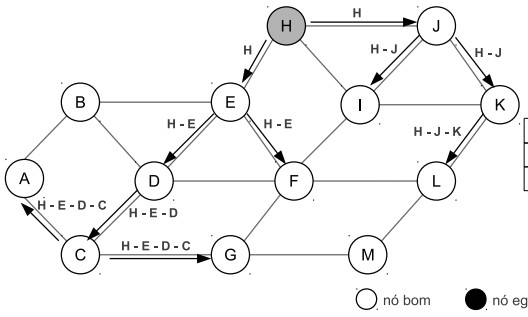
Figura 1. Arquitetura do esquema QS^2

autoindutores e a determinação dos genes do nó. A contagem de autoindutores quantifica os autoindutores enviados por cada nó da rede. Os autoindutores para o QS^2 são as escritas (*AI-W*) e os encaminhamentos de dados realizados (*AI-F*) por cada nó na rede. A determinação dos genes classifica os nós em um dos três estados: bons, egoístas (*C*) ou maliciosos (*M*). Isso depende da contagem de autoindutores de cada nó e dos limites dos autoindutores que caracterizam um bom comportamento. Depois de classificados, os nós são escolhidos de acordo com a semelhança de parentesco com o nó seletor.

O *módulo de decisão de cooperação em quóruns* determina a relação de cooperação entre dois nós. Esse módulo permite uma flexibilização na interação entre os nós, que podem classificar um nó como de má-conduta e mesmo assim decidir interagir com ele. Em conjunto, os módulos de seleção e de decisão de cooperação determinam quais nós são bons, isto é, nós cujo comportamento é colaborativo. Tais nós são posteriormente escolhidos para a participação em quóruns de escrita e de leitura. As subseções seguintes detalham as etapas de contagem de autoindutores, da determinação do gene do nó e da decisão de cooperação do esquema QS^2.

4.1. Contagem de autoindutores

A contagem dos autoindutores *AI-W* e *AI-F* é realizada individualmente por cada nó presente no sistema, que possui um contador de autoindutores para cada nó na rede. Essa contabilização acontece no momento em que o nó recebe uma requisição de escrita de um dado. Os nós enviam junto com o dado a rota por onde o dado trafegou, e dessa forma, é possível incrementar o contador de *AI-F* para cada nó presente na rota de disseminação e o contador de *AI-W* para o nó de origem da escrita. Essa rota é assinada por cada nó que a compõe, de modo que não seja possível forjar a rota ou induzir que nós bons sejam excluídos por outros ao retirar suas participações na rota. A Figura 2 ilustra a contagem dos autoindutores no QS^2. Nela, o nó **H** inicia a escrita de um dado na rede, enviando junto o seu identificador para dois nós. Ao encaminhar o dado, os nós incluem o seu identificador na rota, para que essa colaboração seja contabilizada pelos próximos nós. A tabela exemplifica a contagem de autoindutores *AI-W* e *AI-F* pelo nó **A**, que recebe essa escrita a partir da rota **H - E - D - C**. O nó **A** incrementa a quantidade de *AI-W* para o nó **H**, a origem do dado, e a quantidade de *AI-F* para os nós **E**, **D** e **C**, que encaminharam esse dado até ele.



	A	B	C	D	E	F	G	H	I	J	K	L	M
AI-W	0	0	0	0	0	0	0	1	0	0	0	0	0
AI-F	0	0	1	1	1	0	0	0	0	0	0	0	0

Figura 2. Contagem de autoindutores no QS^2

4.2. Determinação dos genes dos nós

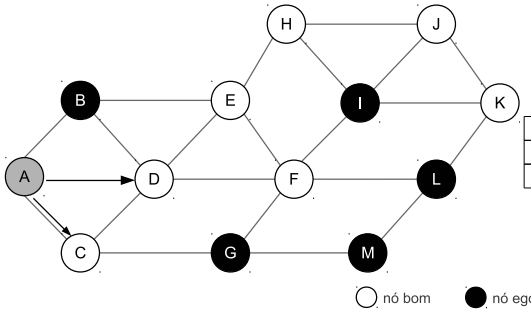
Na identificação dos genes dos nós, o esquema QS^2 verifica a contagem de autoindutores enviada pelos nós e a compara com uma quantia identificada como aceitável para a rede. Para isso, estima-se a taxa esperada de escritas enviadas por um nó, denominada k_{env}, e a taxa de encaminhamentos de escritas, denominada k_{enc}. Essa taxa pode ser estimada de acordo com o comportamento de escritas dos dados replicados. Ambas as taxas são calculadas em função de um determinado período de tempo. A partir dessas taxas, determina-se os limites de envio para os autoindutores *AI-W* e *AI-F*. Qualquer nó que esteja além desses limites é identificado como um nó de má-conduta.

Este trabalho foca na distribuição de dados de serviços de operação de rede e, portanto, assume-se que a taxa de envio de escritas é definida por uma distribuição de Poisson, devido à adequação dessa distribuição ao comportamento desses serviços [Luo et al. 2003]. Contudo, o esquema QS^2 pode considerar outras funções de distribuição. Dessa forma, considerando a média λ de escritas enviadas por cada nó, calcula-se os limites de envio de escrita, $k_{env^{max}}$, e de encaminhamento, $k_{enc^{min}}$, considerados normais para os nós. Um nó é malicioso se ultrapassar o limite máximo permitido de escritas durante um determinado período de tempo, e é egoísta se não atingir e sustentar um limite mínimo de escritas encaminhadas. A taxa máxima de envio de escritas $k_{env^{max}}$ para um nó bom é calculada pela Equação 1, em que δ representa a probabilidade do envio de escritas ser menor do que o $k_{env^{max}}$ estimado. A quantidade mínima de encaminhamentos para um nó é calculada pela Equação 2, em que γ representa a probabilidade dos nós encaminharem menos de $k_{enc^{min}}$. Os nós egoístas e maliciosos possuem taxas k_{env} e k_{enc} arbitrárias, e não respeitam as taxas $k_{env^{max}}$ e $k_{enc^{min}}$ definidas pelo esquema.

$$\sum^{k_{env}} \frac{\lambda^{k_{env^{max}}} \times \mathrm{e}^{-\lambda}}{k_{env^{max}}!} \leqslant \delta \qquad (1) \qquad\qquad \sum^{k_{enc}} \frac{\lambda^{k_{enc^{min}}} \times \mathrm{e}^{-\lambda}}{k_{enc^{min}}!} \geqslant \gamma \qquad (2)$$

A Figura 3 ilustra a determinação dos genes dos nós de acordo com a contagem de autoindutores pelo nó **A**, conforme demonstra a tabela do nó. Os nós contabilizam os autoindutores a medida que ocorrem as operações de escrita. Supondo que os limites $k_{env^{max}} = 5$ escritas por segundo e $k_{enc^{min}} = 2$ encaminhamentos por segundo, o nó **A** classifica os nós **B**, **G**, **I**, **L** e **M** como egoístas (*C*) por estarem abaixo do esperado. Além disso, o nó **B** também é classificado como um nó malicioso (*M*), conforme mostra a tabela, pois enviou mais escritas do que o esperado nesse período de tempo. Com esse cenário, o

nó **A** seleciona os nós **D** e **C** para participar da replicação, pois são considerados bons.



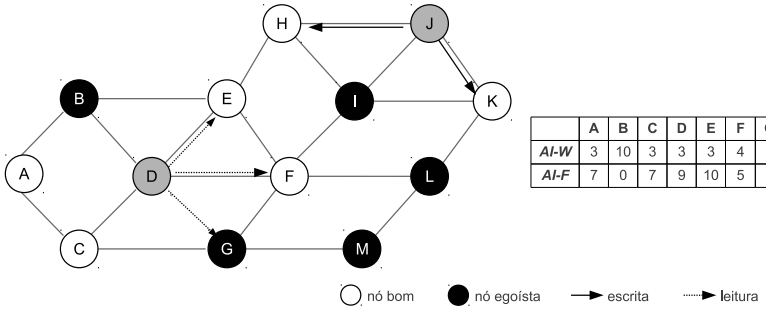
	A	B	C	D	E	F	G	H	I	J	K	L	M
AI-W	-	10	3	3	3	4	0	2	0	2	1	0	0
AI-F	-	0	7	9	10	5	0	7	0	5	5	0	0

Figura 3. Determinação dos genes no QS^2

4.3. Decisão de cooperação

O módulo de decisão de cooperação seleciona os nós que podem participar das operações do sistema de quórum. Essa decisão tem como base os genes identificados pela etapa de determinação dos genes do nó e pelo tipo de operação que o nó deseja realizar. A operação de leitura, por exemplo, pode admitir a escolha de um nó egoísta para compor o quórum de leitura. Isso porque a leitura conta com mais nós em um quórum e a má-conduta egoísta de um componente não prejudica de forma acentuada o andamento da operação. Porém, isso não é possível em uma operação de escrita, em que um nó egoísta compromete por completo a propagação de um dado.

A Figura 4 ilustra a execução da decisão de cooperação em operações de escrita e de leitura. O nó **D** escolhe os nós **E**, **F** e **G** para realizar uma operação de leitura, enquanto que o nó **J** escolhe os nós **H** e **K** para realizar uma operação de escrita. Supondo que a tabela apresentada é a mesma para o nó **D** e **J**, o nó **D** escolhe o nó **G**, apesar de ser identificado como egoísta, porque o nó **D** pode completar a requisição de leitura corretamente mesmo que o nó **G** omita ou modifique essa requisição, devido às características dos sistemas de quóruns. Já o nó **J** escolhe somente nós bons para as escritas, pois a escrita não suporta a interação de nenhum tipo de nó de má-conduta.



	A	B	C	D	E	F	G	H	I	J	K	L	M
AI-W	3	10	3	3	3	4	0	2	0	2	1	0	0
AI-F	7	0	7	9	10	5	0	7	0	5	5	0	0

Figura 4. Decisão de cooperação no QS^2

5. Avaliação do esquema QS^2

O esquema QS^2 foi implementado no simulador de redes NS versão 2.33 e adicionado ao código de um sistema de quórum probabilístico para MANETs, o PAN, sendo chamado

de $PAN + QS^2$. O esquema foi avaliado considerando a interferência de nós de má-conduta nas operações de leitura e de escrita, na forma de ataques de falta de cooperação, temporização e injeção de dados. Nos ataques de falta de cooperação, os nós egoístas não colaboram com as operações de replicação. No ataque de temporização, os nós maliciosos atrasam a propagação da escrita, e nos ataques de injeção de dados eles injetam dados falsos no sistema. Os nós egoístas e maliciosos agem sempre que são consultados por outros nós, e dessa forma sua interação com o sistema e a quantidade de pacotes descartados ou injetados é probabilística. Os resultados obtidos pelo $PAN + QS^2$ são comparados com os resultados do PAN diante desses mesmos ataques, avaliado em [Mannes et al. 2009].

O ambiente de rede simulado é composto por 50 nós, sendo que metade deles replica os dados entre si e são escolhidos aleatoriamente no início da simulação. Os nós se comunicam por um canal sem fio, seguindo o modelo de propagação *TwoRayGround* e movimentam-se de acordo com o modelo de movimentação *Random Waypoint*, em uma área de 1000m x 1000m. O protocolo de roteamento empregado é o AODV, o raio de alcance dos nós é de 250m e a velocidade máxima dos nós varia de 2m/s, 5m/s, 10m/s e 20m/s, com um tempo de pausa de 10s, 20s, 40s e 80s. O quórum de leitura (Q_r) é composto por quatro servidores e o quórum de escrita (Q_w) é formado por todos os nós que recebem a escrita de um dado. As escrita são disseminadas a cada $T = 200$ms, e cada nó dissemina os dados para dois servidores.

Nas simulações, o intervalo de envio de escritas e leituras de cada nó é modelado seguindo a distribuição de Poisson, com $\lambda = 100$ para as escritas e $\lambda = 36$ para as leituras. Desta forma, a quantidade máxima de escritas permitidas para cada nó é de $k_{env^{max}} = 0,018$ escritas por segundo. Já a quantidade mínima $k_{enc^{min}}$ de encaminhamento esperado para cada nó é $k_{enc^{min}} = 0,15$ encaminhamentos por segundo. Todos os nós que eventualmente apresentem taxas que não correspondem ao especificado são considerados nós de má-conduta. A quantidade de nós de má-conduta (f) é igual a 20%, 28% e 36%, que corresponde a 5, 7 e 9 nós. Os resultados apresentados são as médias de 35 simulações de 1500s cada uma, com um intervalo de confiança de 95%.

5.1. Métricas de avaliação

Foram empregadas quatro métricas para a avaliação do QS^2 diante de nós de má-conduta. A primeira delas, o *grau de confiabilidade* (G_c), quantifica o desempenho do QS^2, e representa a quantidade de leituras corretas obtidas pelos nós. São consideradas corretas as leituras que obtém um resultado correspondente a uma escrita previamente realizada no sistema ou a uma escrita ainda em progresso no momento da leitura. O G_c é definido conforme a Equação 3 em que C_r representa as leituras que obtiveram resultados corretos e R a quantidade total de requisições de leituras emitidas pelos clientes.

$$G_c = \frac{\sum C_r}{|R|} \tag{3}$$

As próximas métricas buscam aferir a eficiência de detecção do QS^2. Deste modo, a *Taxa de detecção* (Tx_{det}) representa a quantidade de vezes em que os nós de má-conduta foram detectados em razão da quantidade de consultas a eles. A Tx_{det} é contabilizada para os ataques de falta de cooperação e injeção de dados nas escritas. Ela é calculada de acordo com a Equação 4, em que A representa o conjunto de todas as interações de nós

de má-conduta e os respectivos resultados obtidos pelo QS^2, dado na forma de $A(d, a)$, em que d é o resultado da detecção do QS^2 e a é a verdadeira condição do nó i.

$$Tx_{det} = \frac{\sum D_i}{|A|} \forall i \in A \quad \text{onde} \quad D_i = \begin{cases} 1 & \text{se} \quad d_i = a_i \\ 0 & \text{se} \quad d_i \neq a_i \end{cases} \tag{4}$$

A *taxa de falsos negativos* (Tx_{fn}) apresenta a quantidade de vezes em que nós egoístas ou maliciosos foram identificados como nós bons em razão da quantidade de interação dos nós de má-conduta. Essa métrica é calculada pela Equação 5, em que A é o conjunto de todas as interações de nós de má-conduta no sistema e os respectivos resultados obtidos pelo QS^2, dado na forma de $A(d, a)$, em que d é o resultado da detecção realizada pelo QS^2 e a é a verdadeira condição do nó i.

$$Tx_{fn} = \frac{\sum D_i}{|A|} \forall i \in A \quad \text{onde} \quad D_i = \begin{cases} 1 & \text{se} \quad d_i \neq a_i \\ 0 & \text{se} \quad d_i = a_i \end{cases} \tag{5}$$

A *taxa de falsos positivos* (Tx_{fp}) representa a quantidade de vezes que os nós consideraram um nó como malicioso ou egoísta em razão da quantidade de interação dos nós bons no sistema. A Tx_{fp} é calculada de acordo com a Equação 6, em que B representa o conjunto de interações de nós bons no sistema, na forma de $B = (d, a)$, onde d representa o valor da detecção realizada pelo QS^2 e a é a condição real do nó, onde $a = 1$ representa um nó de má-conduta e $a = 0$ representa um nó bom.

$$Tx_{fp} = \frac{\sum D_i}{|B|} \forall i \in B \quad \text{onde} \quad D_i = \begin{cases} 1 & \text{se} \quad d_i \neq a_i \\ 0 & \text{se} \quad d_i = a_i \end{cases} \tag{6}$$

As subseções seguintes apresentam os resultados da avaliação de desempenho e de eficiência do QS^2 obtidas através de simulações.

5.2. Desempenho

As Figuras 5 e 6 comparam os resultados para a métrica G_c obtidos pelo PAN e pelo $PAN + QS^2$ diante dos ataques de falta de cooperação, temporização e injeção de dados. Nos ataques de falta de cooperação, o uso do esquema QS^2 representa um aumento de até 14% em relação ao G_c obtido pelo PAN sem o QS^2, sendo que a confiabilidade dos dados em cenários com ataques nas escritas é acima de 95% e para ataques nas leituras é acima de 98%, mesmo considerando a ação egoísta de 36% dos nós. É interessante observar que a velocidade e a quantidade de nós de má-conduta na rede têm uma influência menor no $PAN + QS^2$, mostrada na Figura 6(a), do que sem a solução, apresentada na Figura 5(a). A variação entre o G_c obtido com nós a 2m/s e com 20m/s é menor que 2%. Essa característica é importante, pois a velocidade dos nós não interfere no funcionamento do QS^2. De fato, a mobilidade garante que os nós recebam dados por rotas diferentes, e contabilizem as escritas e os encaminhamentos de diferentes nós.

Já o ataque de temporização não apresenta um grande impacto no PAN, como ilustra a Figura 5(b), e por isso, o QS^2 não apresenta um aumento significativo nos resultados. Isso também é influenciado pelo fato de que o QS^2 não identifica especificamente os nós que atrasam a propagação, que são considerados egoístas como consequência do seu comportamento na rede. Porém, a classificação deles como nós egoístas é demorada,

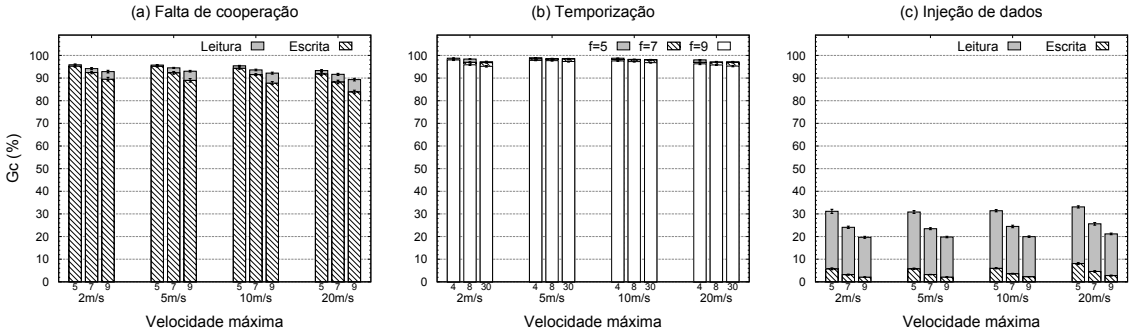


Figura 5. G_c do PAN diante de ataques

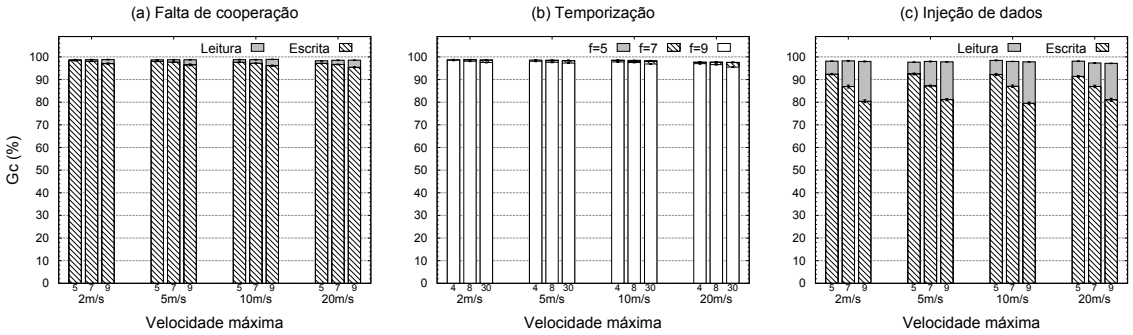


Figura 6. G_c do $PAN + QS^2$ diante de ataques

sendo que em alguns cenários o G_c obtido pelo $PAN + QS^2$ é ligeiramente inferior do que no PAN, apresentado na Figura 6(b). Porém essa variação é pequena, aproximadamente 0,42%. Conforme os nós de má-conduta aumentam o atraso das propagações, o QS^2 apresenta um ganho mais acentuado do G_c, aproximadamente 1,8% em cenários com atraso de 800ms e 2% com $T = 3000$ms. Mesmo assim, em todos os cenários, o G_c obtido está acima de 95%.

Já os ataques de injeção de dados representam a maior vulnerabilidade do PAN, como mostra a Figura 5(c). Nesses cenários, a confiabilidade dos dados é inferior a 30%. Logo, o uso do QS^2 diante desses ataques resultou em um ganho significativo para o PAN, que obteve um aumento de até 87% na confiabilidade, como ilustrado na Figura 6(c). Esse comportamento ocorre tanto nos ataques nas escritas como nas leituras, sendo que o G_c é maior para as leituras, já que as escritas comprometem de forma mais eficaz a replicação. Mesmo assim, as escritas em todos os cenários mantém o G_c acima de 80%.

Ainda no ataque de injeção de dados falsos, o G_c possui um comportamento diferente dos ataques de falta de cooperação e temporização, ocasionado pelas próprias características da rede. Elas fazem com que o $PAN + QS^2$ obtenha níveis mais altos de G_c com velocidades maiores. Esse comportamento também é observado no PAN diante de ataques, e acontece porque nesse tipo de ataque os nós maliciosos perdem sua eficácia em velocidades maiores, devido à dificuldade na entrega de pacotes em geral, inclusive de pacotes falsos injetados pelos nós maliciosos. A perda de pacotes também influencia na detecção de nós que estejam com dificuldade de comunicação, que também podem ser considerados egoístas. Neste caso, o QS^2 ajuda o sistema a manter os dados em nós cuja conectividade é boa, facilitando uma posterior consulta pelos clientes.

Para verificar o desempenho do QS^2 diante dos vários tipos de ataque em conjunto, foi simulado um cenário em que os nós iniciam os três tipos de ataques considerados. Foram simulados cenários com f igual a 5, 10 e 15, sendo que cada ataque é desempenhado por 20% do total de nós maliciosos. Os ataques considerados são os de falta de cooperação nas leituras e nas escritas, temporização (T=3000) e injeção de dados na leitura e na escrita. A velocidade média dos nós varia de 0m/s a 20m/s. Os demais parâmetros são os mesmos utilizados na avaliação do $PAN + QS^2$

A Figura 7 apresenta os resultados obtidos com esses cenários. Observa-se que conforme a quantidade de nós de má-conduta aumenta, o G_c diminui, porém enquanto a quantidade de nós de má-conduta é a mesma, a variação do G_c de acordo com a velocidade é pequena, o que evidencia que a solução tende a manter um mesmo nível de leituras corretamente concluídas, independente da velocidade. Essa variação, em todos os cenários de diferentes quantidades de nós de má-conduta, é de aproximadamente 1%. Esse comportamento representa uma vantagem ao sistema, já que os nós das MANETs podem variar a velocidade e o $PAN + QS^2$ mantém a confiabilidade acima de 92% para todos os cenários simulados, mesmo diante de mais de 50% dos nós comprometidos.

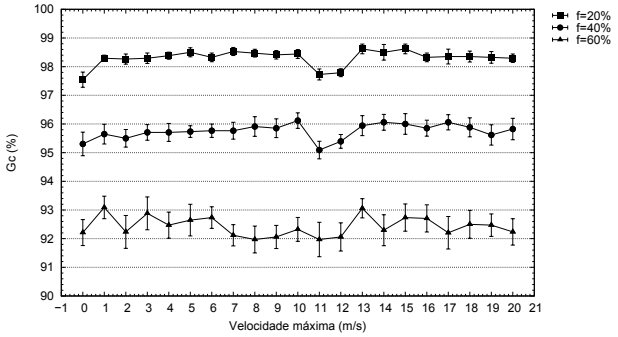


Figura 7. G_c com nós egoístas e maliciosos em conjunto

5.3. Eficiência

As Figuras 8 e 9 apresentam os resultados de Tx_{det}, Tx_{fn} e Tx_{fp} para nós egoístas e maliciosos, referente aos cenários de simulação utilizados para a validação do $PAN + QS^2$. Para os nós egoístas, a taxa de detecção obtida pelo QS^2 é superior a 98,5%, como ilustra a Figura 8(a). Isso se deve à característica do QS^2, em que uma vez identificado como egoísta, um nó só é considerado bom novamente se cooperar com os demais. Essa taxa de detecção se mantém para todas as velocidades e quantidade de nós de má-conduta presentes no ambiente. Para os nós maliciosos, a taxa de detecção é em média de 80%, conforme ilustrado na Figura 9(a). Essa diferença de detecção entre os nós egoístas e maliciosos ocorre porque o QS^2 identifica os nós maliciosos pelo comportamento em um determinado intervalo de tempo, e com o passar do tempo, os nós maliciosos não são mais contatados, diminuindo a interação deles com o sistema. Isso resulta na normalização do nível de autoindutores relativo ao nó malicioso nos demais nós do sistema, ocasionando os nós bons a interagir novamente com eles.

Os falsos negativos obtidos pelo QS^2 na detecção de nós egoístas, apresentado na Figura 8(b), é inferior a 2%. Isso mostra que poucos nós egoístas não são detectados quando selecionados. A falha na detecção de um nó egoísta pode acontecer devido a autonomia na detecção, que permite que os nós contem individualmente os autoindutores,

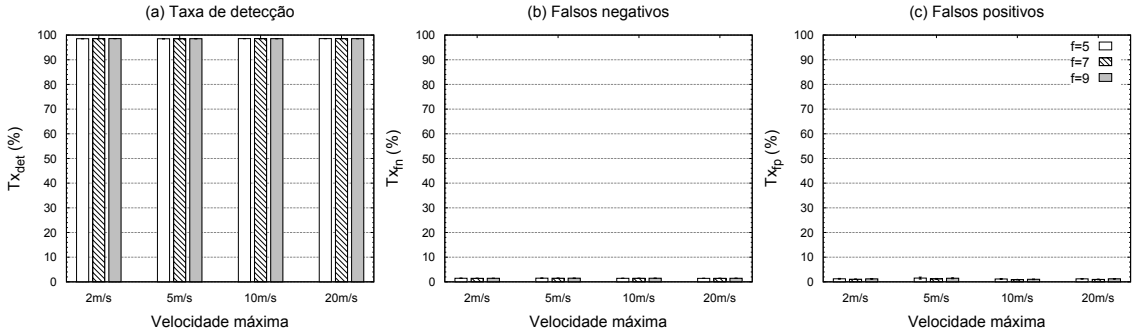


Figura 8. Eficiência na detecção de nós egoístas

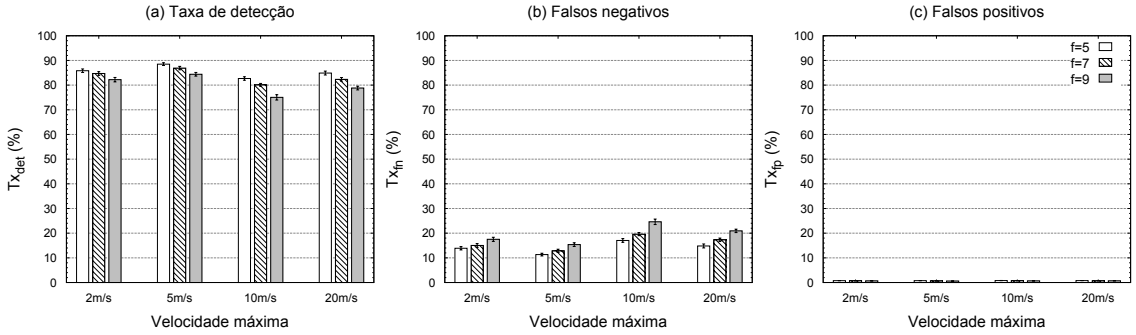


Figura 9. Eficiência na detecção de nós maliciosos

e dessa forma, alguns nós podem demorar a identificar determinados nós como egoístas. Para os nós maliciosos, os falsos negativos são de aproximadamente 20%, conforme apresentado pela Figura 9(b), sendo menor em cenários com menos nós de má-conduta participando na rede. Esse aumento de falsos negativos no ataque de injeção de dados acontece pela normalização dos autoindutores de escrita, já explicada anteriormente.

A taxa de falsos positivos obtidos pelo QS^2, tanto na detecção de nós egoístas, ilustrada na Figura 8(c), quanto de nós maliciosos, ilustrada na Figura 9(c), é inferior a 2%. Algumas detecções equivocadas são esperadas e podem acontecer se um nó está muito distante na rede e apresenta dificuldade em interagir com o restante da rede, ou se um nó faz muitas escritas contínuas para o mesmo grupo de nós. Deste modo, momentaneamente eles são considerados nós de má-conduta, porém conforme ocorre a movimentação e a interação dos nós, eventualmente eles são identificados como nós bons.

6. Conclusão

Este artigo propôs QS^2, um esquema para a exclusão de nós egoístas e maliciosos das operações de escrita e de leitura em um sistema de quórum para MANETs. O QS^2 é inspirado nos mecanismos de sensoriamento em quórum e de seleção por parentesco, ambos encontrados em bactérias. Ele identifica os nós de má-conduta de forma independente através da quantidade de escritas e encaminhamentos enviados por outros nós e não requer a troca de informações de reputação entre eles. Além disso, esse esquema utiliza a própria troca de mensagens de escrita para a detecção dos nós de má-conduta, o que não gera maiores custos de comunicação para os nós da rede.

Os resultados obtidos mostram que o QS^2 aumentou a confiabilidade de um sis-

tema de quórum para MANETs em até 87% diante de ataques de injeção de dados nas escritas. A detecção de nós egoístas apresentou uma eficácia de 98,5% com uma taxa de falsos positivos menor que 2%, e a detecção de nós maliciosos obteve uma eficácia de 80%, com uma taxa de falsos positivos inferior a 1%. Como trabalhos futuros, pretende-se testar o uso do QS^2 em outros cenários de MANETs, variando parâmetros como velocidade, quantidade de nós e quantidade de nós de má-conduta presente na rede.

Referências

Bellavista, P., Corradi, A., and Magistretti, E. (2005). Redman: An optimistic replication middleware for read-only resources in dense manets. *Pervasive Mobile Computing*, 1:279–310.

Derhab, A. and Badache, N. (2009). Data replication protocols for mobile ad-hoc networks: a survey and taxonomy. *IEEE Communications Surveys and Tutorials*, 11:33–51.

Gramoli, V. and Raynal, M. (2007). *Timed Quorum Systems for Large-Scale and Dynamic Environments*, pages 429–442.

Luo, J., Hubaux, J.-P., and Eugster, P. T. (2003). PAN: Providing reliable storage in mobile ad hoc networks with probabilistic quorum systems. In *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '03)*, pages 1–12.

Malkhi, D. and Reiter, M. (1997). Byzantine quorum systems. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing (STOC '97)*, pages 569–578.

Malkhi, D., Reiter, M., Wool, A., and Wright, R. N. (1998). Probabilistic byzantine quorum systems. In *Proceedings of the seventeenth annual ACM symposium on Principles of distributed computing*, PODC '98, pages 321–322.

Mannes, E., da Silva, E., and dos Santos, A. L. (2009). Analisando o desempenho de um sistema de quóruns probabilístico para manets diante de ataques maliciosos. In *Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg '09)*, pages 71–84.

Meisel, M., Pappas, V., and Zhang, L. (2010). A taxonomy of biologically inspired research in computer networking. *Computer Networks*, 54:901–916.

Ng, W.-L. L. and Bassler, B. L. (2009). Bacterial quorum-sensing network architectures. *Annual Review of Genetics*, 43(1):197–222.

Saito, Y. and Shapiro, M. (2005). Optimistic replication. *ACM Computer Survey*, 37:42–81.

Salmon, H. M., Miceli, C., Pirmez, L., Rossetto, S., Rodrigues, P. H. A., Pirmez, R., Delicato, F. C., and Carmo, L. F. (2010). Sistema de detecção de intrusão imuno-inspirado customizado para redes de sensores sem fio. In *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg '10)*, pages 269–282.

Tulone, D. (2007). Ensuring strong data guarantees in highly mobile ad hoc networks via quorum systems. *Ad Hoc Networks*, 5(8):1251–1271.

Yang, H., Meng, X., and Lu, S. (2002). Self-organized network-layer security in mobile ad hoc networks. In *Proceedings of the 1st ACM workshop on Wireless security (WiSE '02)*, pages 11–20.

Zhang, C., Song, Y., and Fang, Y. (2008). Modeling secure connectivity of self-organized wireless ad hoc networks. In *Proceedings of the 27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '08)*.

Zhu, Z., Tan, Q., and Zhu, P. (2007). An effective secure routing for false data injection attack in wireless sensor network. In *Managing Next Generation Networks and Services*, volume 4773, pages 457–465.