Serviços Confiáveis em MANETs Baseado em Sistema de Quórum Tolerante a Má-conduta

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. *Operational services in MANETs need to deal with node mobility and resource constraints to support applications. The reliability and availability of these services can be assured by data management approaches, as replication techniques using quorum systems. However, these systems are vulnerable to selfish and malicious nodes, that intentionally do not collaborate with replication operations or spread malicious data while replicating data. This paper evaluates the performance of QS^2, a scheme to tolerate selfish and malicious nodes in replication operations on quorum system supporting operational services in realistic scenario for MANETs. This scheme is distributed and self-organized and allows each node to independently exclude misbehaving nodes. Simulation results shows that QS^2 improves by 45% the reliability in realistic scenarios, detecting more than 55% of misbehaving interaction.*

Resumo. *Os serviços de operação em MANETs devem lidar com a mobilidade dos dispositivos e com as restrições de seus recursos a fim de suportar as aplicações. A confiabilidade e a disponibilidade dos serviços podem ser obtidas por meio de abordagens de gerenciamento de dados, como técnicas de replicação usando sistemas de quórum. Contudo, esses sistemas são vulneráveis a nós que intencionalmente não colaboram ou disseminam dados maliciosos enquanto participam da replicação. Este trabalho avalia o desempenho do QS^2, um esquema para tolerar nós de má-conduta em operações de replicação, em um sistema de quórum apoiando serviços de operação em cenários realísticos de MANETs. O QS^2 é distribuído e auto-organizado, e permite que cada nó tenha autonomia para excluir os nós de má conduta. Os resultados de simulação mostram que o QS^2 aumenta 45% a confiabilidade em cenários realísticos, e detecta mais de 55% das interações maliciosas dos nós.*

1. Introdução

Os avanços das tecnologias de comunicação sem fio reforçam o desenvolvimento e a utilização de diferentes redes sem fio em direção a criação das redes do futuro [Conti et al. 2011]. As redes *ad hoc* móveis (MANETs) fazem parte dessas redes e têm como objetivo suportar diversas aplicações em áreas como saúde, transporte e entretenimento. As MANETs são formadas dinamicamente por dispositivos (nós) móveis e portáteis, tais como *notebooks*, *smartphones* e *tablets*. Nelas, os serviços e as aplicações são fornecidos de uma forma distribuída e auto-organizada, e juntamente com outras redes sem fio, devem convergir a fim de suportar as aplicações das redes do futuro.

Essas novas redes devem causar um impacto substancial na sociedade. Contudo, juntamente com as facilidades previstas, surgem numerosos desafios e requisitos. Um desses desafios é a necessidade de oferecer aplicações continuamente apesar de falhas, acidentes, ataques ou qualquer outras condições adversas da rede [Conti et al. 2011]. Devido à esperada complexidade das redes do futuro e a participação de diferentes entidades autônomas, surge a necessidade de projetar serviços confiáveis em todos os segmentos de rede, inclusive nas MANETs. As características das MANETs podem facilmente ocasionar a sua partição, tornando os serviços indisponíveis e sustentando informações desatualizadas [Zhang et al. 2008]. A falta de informação ou o uso de informações desatualizadas influenciam na operação dos nós, dos serviços e das aplicações, comprometendo o desempenho de toda a rede e até mesmo podendo causar a sua inutilização.

Nesse sentido, a gerência de dados é essencial para o fornecimento de serviços e aplicações confiáveis. Os serviços de operação da rede, tais como os serviços de localização de recursos e de gerenciamento da mobilidade, apoiam as aplicações através do monitoramento e do gerenciamento de dados de controle. Esses serviços têm como principal função o envio de informações para os nós, para que eles sejam capazes de se antecipar e de se adaptar às situações adversas provenientes das próprias características das MANETs, como as constantes mudanças de topologia que provocam quebras de enlace e o consequente particionamento da rede. Por isso, é necessário que os serviços de operação de rede sejam seguros e robustos, com garantia de disponibilidade e de confiabilidade dos dados. Uma das formas comumente empregadas para prover a disponibilidade dos dados é por meio da redundância, obtida através das técnicas de replicação dos dados [Derhab and Badache 2009, Sardiña et al. 2011].

As abordagens clássicas de replicação de dados, quando aplicadas em MANETs, apresentam um alto custo. A replicação por sistema de quórum [Malkhi and Reiter 1997] é uma alternativa atraente, que busca um balanceamento da carga entre os servidores. Contudo, os sistemas de quórum propostos para MANETs apresentam vulnerabilidades que resultam na perda da confiabilidade dos dados diante de nós egoístas e nós maliciosos nas operações de replicação [Mannes et al. 2009]. 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.

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 que detectam esses nós [Yang et al. 2002, Zhu et al. 2007]. Porém, a maioria deles gera uma sobrecarga de mensagens devido à troca de recomendações ou utiliza entidades centralizadas, que não são adequadas para as MANETs. O QS^2 (*quorum system + quorum sensing*) [Mannes et al. 2011] detecta nós egoístas e nós maliciosos por meio da análise autônoma do comportamento de cada nó, e de forma auto-organizada ele evita que os nós de má-conduta façam parte da replicação dos dados. Além disso, o QS^2 não gera sobrecarga de mensagens na rede, pois envia suas informações juntamente com as mensagens de replicação.

Este trabalho avalia o uso do QS^2 para suportar a replicação confiável em sistemas de quórum em dois cenários realísticos de MANETs: em ambientes urbanos e em ambientes de transporte. Os resultados de simulação mostram que o QS^2 aumenta a confiabilidade dos dados em mais de 55% diante de ataques de injeção de dados. Além disso, observa-se que com o uso do QS^2 a quantidade de dados comprometidos por nós

de má-conduta é inferior a quantidade de dados desatualizados no sistema, em ambos os cenários simulados. Essa confiabilidade atende aos requisitos de aplicações em que a disponibilidade sobrepõe o custo de lidar com eventuais inconsistências. Exemplos dessas aplicações são o monitoramento de ambientes, o envio de alertas e informação de tráfego para veículos e a disseminação de informações para pedestres.

O restante do artigo está organizado como descrito a seguir. A Seção 2 apresenta os trabalhos relacionados. A Seção 3 descreve o modelo do sistema. A Seção 4 apresenta uma visão geral do esquema QS^2. A Seção 5 apresenta as métricas de avaliação utilizadas na avaliação e os resultados obtidos por meio de simulação. A Seção 6 conclui o artigo e apresenta os trabalhos futuros.

2. Trabalhos Relacionados

Os sistemas de replicação clássicos não são apropriados para as 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 mais adequada para ambientes dinâmicos como as MANETs, pois 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].

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 confiabilidade e a integridade dos dados geralmente é obtida por meio de técnicas como criptografia e verificação dos dados por uma determinada quantidade de nós. 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. Devido às suas características, as MANETs necessitam incorporar atributos como a auto-organização, a autonomia e o uso de poucos recursos nessas soluções. O esquema QS^2 é inspirado em sistemas biológicos e tem como características a detecção autônoma, a auto-organização na exclusão dos nós e o uso de poucos recursos, tornando-o uma solução adequada para as MANETs.

3. Modelo do sistema

Considera-se que o QS^2 seja aplicado em sistemas de quórum probabilísticos para MANETs apoiando a replicação de dados de serviços de operação de rede, tais como os serviços de localização de recursos e de conectividade. O modelo do QS^2 [Mannes et al. 2011] é composto de três camadas: o **modelo de rede**, o **modelo de gerência de dados** e o **modelo de ataque**. O modelo em camadas é ilustrado na Figura 1.

Modelo de rede - Para a execução do QS^2, assume-se que a rede é formada por um conjunto P composto por n nós identificados por $\{s_0, s_1 ... s_{n-1}, s_n\}$, sendo que todo nó $s_i \in P$ tem um endereço físico ou identificador único. Esses nós se comunicam através de um canal sem fio, cujo raio de transmissão é igual para todos os nós da rede. Considera-se que os processos e os canais de comunicação são assíncronos e não confiáveis, sendo sujeito a perda de pacotes ou à partição da rede devido a colisão ou a entrada e saída de nós. Supõe-se que os nós de má-conduta não podem comprometer a descoberta e a manutenção das rotas. Da mesma forma, assume-se que as mensagens de replicação são relativamente pequenas com no máximo 128 *bytes*. Assume-se também que a rede fornece um esquema de assinatura para a proteção de informações importantes enviadas pelo QS^2, de forma que nós de má-conduta não possam modificar tais informações.

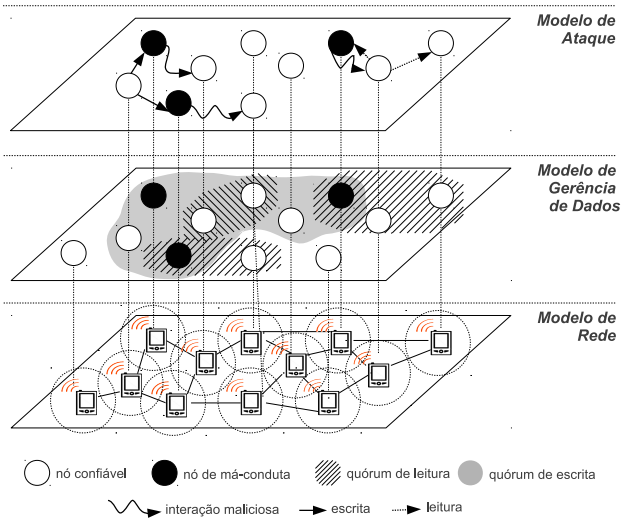

Figura 1. Modelo do sistema em camadas

Modelo de gerência de dados - O gerenciamento de dados é realizado por um sistema de quórum probabilístico, sendo que nesta avaliação utilizou-se o PAN [Luo et al. 2003], embora outros sistemas de quórum probabilísticos possam ser aplicados. O PAN é composto por um sistema de armazenamento (StS) e por nós clientes, servidores e agentes. O StS é composto por nós servidores, que armazenam os dados e gerenciam a replicação. Os nós clientes requisitam dados para os servidores, e os servidores que são contatados diretamente pelos clientes são denominados agentes. Eles são responsáveis por mediar as requisições de leitura e de escrita entre os clientes e o StS. A escrita dos dados é baseada em um protocolo epidêmico, sendo que a sua disseminação entre os nós acontece em intervalos regulares e formam o quórum de escrita (Q_w). Já a leitura é feita por meio de mensagens *unicast* para uma determinada quantidade de nós no StS, formando o quórum de leitura (Q_r). Esse sistema de quórum foi escolhido devido à redução do número de mensagens na replicação, e por ser utilizado na replicação de dados de serviços de operação de rede. Além disso, ele emprega mecanismos que facilitam a gerência do armazenamento dos dados em redes dinâmicas como as MANETs.

Modelo de falhas - O QS^2 trata de nós de má-conduta que afetam as propriedades de disponibilidade e de integridade dos dados em um sistema de replicação. Esses nós de má-conduta são intrusos e conhecem o funcionamento da rede, tendo permissão e chaves criptográficas para participar das operações. Assume-se que um nó s_i é egoísta se não

colabora com as operações de replicação, e malicioso se modifica ou injeta dados maliciosos no sistema de replicação. Consideram-se dois tipos de comportamento para os nós maliciosos: a injeção de dados falsos, que caracteriza os **ataques de injeção de dados**, e o atraso na propagação dos dados, que caracteriza os **ataques de temporização**. Já os nós egoístas não cooperam com as operações, originando o **ataque de falta de cooperação**. Assume-se que um nó de má-conduta se comporta de modo egoísta ou malicioso durante toda a sua participação na rede, representando um caso de má-conduta extremo. Caso o nó se comporte maliciosamente enviando dados falsos na mesma proporção que um nó confiável envia dados, esses dados falsos logo serão sobrescritos por dados confiáveis, e desta forma, não representa um impacto significativo no sistema de quórum.

4. Visão geral do esquema QS^2

O esquema QS^2 (*quorum system + quorum sensing*) tem como objetivo proporcionar uma forma de excluir nós de má-conduta da participação nas operações de replicação em sistemas de quóruns para MANETs. Cada nó tem uma visão individual do comportamento dos outros nós na rede, que depende da qualidade da interação entre eles. Além disso, cada nó decide a cooperação com outros de acordo com sua própria experiência sobre os demais nós. O esquema é composto por dois módulos: o módulo de monitoramento dos nós e o módulo de decisão de cooperação, conforme ilustrado na Figura 2.

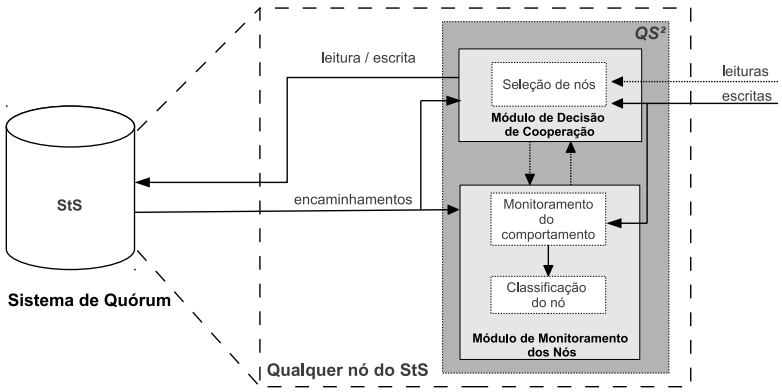

Figura 2. Arquitetura do esquema QS^2

O *módulo de monitoramento dos nós* é responsável pela classificação dos nós em confiáveis ou de má-conduta. Esse módulo é subdividido em dois componentes: o monitoramento do comportamento e a classificação dos nós. O monitoramento do comportamento quantifica a quantidade de escritas e encaminhamentos de escritas enviados por cada nó da rede através dos identificadores dos nós contidos nas mensagens de disseminação dos dados. A cada escrita de um dado no sistema, os nós de origem e os nós que o propagam adicionam seus identificadores juntamente com o dado. Dessa forma, os nós que recebem os dados podem verificar quais nós estão escrevendo no sistema e quais nós estão cooperando na disseminação de tais dados.

A classificação dos nós relaciona cada nó com um dos três estados: confiáveis, egoístas ou maliciosos. Isso depende da contagem de escritas e de encaminhamentos de cada nó e dos limites estabelecidos. Os limiares de envio de escritas $k_{env_{max}}$ e de encaminhamentos $k_{enc_{min}}$ são estimados no comportamento de envio dos dados. Durante as operações de replicação, qualquer nó que esteja além dos limites é identificado como

um nó de má-conduta. Tais limites são obtidos pela análise da quantidade de escrita e de encaminhamentos que cada nó envia à rede.

O *módulo de decisão de cooperação* determina a relação de cooperação entre dois nós, selecionando para interação somente aqueles que tem maior probabilidade de ajudar. Esse módulo é composto pelo componente de seleção de nós, que é apoiado pelo módulo de monitoramento dos nós. Esse módulo também é capaz de tornar a seleção mais flexível e adequar a seleção e a interação entre os nós. Deste modo, pode-se classificar um nó confiável em uma determinada operação e egoísta ou malicioso em outras operações.

O esquema QS^2 é *autônomo*, pois contabiliza individualmente a relação de colaboração entre os nós, e é *auto-organizado* devido à forma com que os nós iniciam a exclusão de outros nós de má-conduta sempre que esses atingem determinada quantidade de escritas ou encaminhamentos,, sendo que essa quantidade é estimada a partir do comportamento da replicação dos dados. Além disso, cada nó tem uma visão independente do comportamento dos nós na rede. O QS^2 não necessita de mensagens extras, o que o torna uma solução com *baixo custo de comunicação*. Ele também não requer pontos fixos de controle e nem depende de outros esquemas de reputação.

5. Avaliação do uso do QS^2 em ambientes realísticos de MANETS

Avalia-se o emprego do QS^2 no suporte ao sistema de quórum PAN em dois cenários realísticos de MANETs. No primeiro cenário, considera-se uma MANET no centro de uma cidade com o objetivo de disseminar informações sobre o comércio local entre os usuários da rede, enquanto que o segundo cenário representa uma MANET em linhas de ônibus, que se destina a disseminar informações de tráfego. Esses dois cenários exemplificam o uso das MANETs no apoio cotidiano aos usuários, representando uma parte importante da aplicação desse tipo de rede. Os parâmetros e os detalhes de configuração dos cenários utilizados são descritos nas seções seguintes.

5.1. Métricas de avaliação

Quatro métricas foram empregadas para a avaliação do QS^2 diante de nós de má-conduta. Essas métricas foram escolhidas por representarem a integridade dos dados [Luo et al. 2003] e a eficiência do QS^2 na detecção dos nós de má-conduta, resultando em um entendimento geral do comportamento do QS^2 em ambientes realísticos de MANETs e na viabilidade do seu uso nesses ambientes. A primeira das métricas utilizadas, o *grau de confiabilidade* (G_c), quantifica as leituras corretas obtidas pelos nós por meio do sistema de quórum. 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 (1) em que C_r representa as leituras que obtiveram resultados corretos e R a quantidade total de requisições de leituras emitidas pelos clientes.

$$G_c = \frac{\sum C_r}{|R|} \tag{1}$$

A métrica *Taxa de detecção* (Tx_{det}) representa a quantidade de vezes em que os nós de má-conduta foram detectados em razão da quantidade de interações desses nós. 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 (2) 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 pelo QS^2 e a é a verdadeira classe (confiável ou de má-conduta) do nó i.

$$Tx_{det} = \frac{\sum D_i}{|A|} \forall i \in A \quad \text{onde} \quad D_i = \begin{cases} 1 & \text{se} \quad d_i = a_i \\ 0 & \text{se} \quad d_i \neq a_i \end{cases} \tag{2}$$

A métrica *Taxa de dados falsos* (Tx_{mis}), descrita na Equação (3), quantifica as leituras que retornaram dados escritos por nós maliciosos no ataque de injeção de dados, em que C_w representa a quantidade de leituras que retornaram dados falsos. A métrica *Taxa de dados desatualizados* (Tx_{out}), calculada de acordo com a Equação (4), quantifica as leituras desatualizadas retornadas pelos nós do StS. A Tx_{out} é dada pela subtração da quantidade de leituras falsas do montante de leituras corretas realizadas pelo sistema.

$$Tx_{mis} = \frac{\sum C_w}{|R|} \tag{3}$$

$$Tx_{out} = G_c - Tx_{mis} \tag{4}$$

5.2. Ataques nos sistemas de quórum

Os ataques foram separados em dois conjuntos: uma situação com ataques de injeção de dados nas operações de escrita e uma situação com os ataques de falta de cooperação, temporização e injeção de dados agindo em conjunto (situação com todos os ataques). Esses conjuntos de ataques foram escolhidos por representarem o pior dano ao sistema de quórum, e desta forma, avalia-se a resiliência do QS^2 diante de casos extremos de má-conduta [Mannes et al. 2009]. Nos ataques de injeção de dados foram considerados cenários com a quantidade de nós de má-conduta (f) igual a 5, 7 e 9 nós, o que representa 20%, 28% e 36% dos nós pertencentes ao StS. Já nos cenários com todos os ataques, foram simulados cenários com f igual a 5, 10 e 15 nós de má-conduta, representando 20%, 40% e 60% dos nós do StS. Os ataques nesse cenário foram os de falta de cooperação nas leituras e nas escritas, temporização com atraso (T) de 3000ms, e injeção de dados na leitura e na escrita, sendo que cada ataque é desempenhado por 20% do total de nós de má-conduta presente em cada cenário.

O ataque de injeção de dados é identificado pela quantidade demasiada de escritas enviadas para o sistema de quórum, enquanto que o ataque de falta de cooperação é detectado pela ausência de cooperação no encaminhamento de mensagens. Os ataques de temporização não possuem um identificador próprio, contudo, esse ataque é identificado como um ataque de falta de cooperação, justamente pela demora na propagação dos dados. Os resultados apresentados estão agrupados por quantidade de nós de má-conduta presente na rede, e apresentam os valores em pontos percentuais. O intervalo de confiança dos valores apresentados é de 95%, e foram obtidos pela média de 35 simulações.

5.3. Ambiente urbano - centro de uma cidade

O cenário urbano utilizado corresponde ao ambiente do centro de uma cidade, onde pedestres e ciclistas se movimentam em direção a pontos de interesse, como *shoppings* e teatros. Este cenário tem como base o descrito em [Becker et al. 2002], que considera

um ambiente que representa, em geral, os centros urbanos de cidades europeias. A ideia dos autores é criar uma rede cuja função seja a disseminação de mensagens informativas, como promoções de lojas e cardápio dos restaurantes, assim como mensagens de utilidade pública e informações sobre condições das vias e do transporte público entre os dispositivos móveis dos transeuntes. Nesse sentido, é necessário que os serviços de operação da rede sejam robustos, garantindo a eficácia da rede e evitando que dispositivos maliciosos comprometam o seu funcionamento e, consequentemente, o funcionamento da aplicação.

Os usuários se movimentam pelas ruas em direção a algum ponto de interesse, seguindo o padrão de mobilidade baseada em grafos (*graph walk*) [Tian et al. 2002]. Foram considerados cenários compostos por 50, 100 e 150 nós, sendo possível avaliar o impacto QS^2 com a variação da densidade da rede. Os nós movimentam-se com velocidades entre 3 e 5km/h, normais para um pedestre, em uma área de 2462 x 1733 metros. Essa área compreende 75 pontos em comum, interligados por 116 ruas. Os nós escolhem randomicamente um dos pontos de interesse, movimentam-se até ele e permanecem no ponto escolhido entre 12 e 20 minutos. O tempo de pausa utilizado representa a parada de pedestres em terminais de ônibus ou *shoppings*. O AODV é empregado como protocolo de roteamento nas simulações e os resultados apresentados são a média de 35 simulações de 1500 segundos, com um intervalo de confiança de 95%.

O quórum de leitura (Q_r) é composto por cinco servidores, incluindo o agente, e o quórum de escrita (Q_w) é formado por todos os nós que recebem a escrita de um dado, sendo que cada nó dissemina os dados para quatro servidores (*F* = 4). O StS é composto por 25 nós, escolhidos randomicamente. As escritas recebidas pelos nós são disseminadas a cada T=200ms. Nas simulações, o intervalo (em segundos) de envio de escritas e leituras de cada nó é modelado seguindo a distribuição de Poisson, conforme utilizado em [Luo et al. 2003], com $\lambda = 100$ para as escritas e $\lambda = 36$ para as leituras. A taxa máxima de escritas é igual a $k_{env^{max}} = 0,018$ escritas por segundo, e a taxa de encaminhamento deve ser superior a $k_{enc^{min}} = 0,15$ pacotes por segundo. As taxas foram calculadas seguindo as equações descritas em [Mannes et al. 2011], que representam as estimativas para a distribuição de dados de um serviço de operação de rede.

5.3.1. Grau de confiabilidade

Os resultados obtidos pela simulação das MANETs criadas para a distribuição de informações no centro de uma cidade, sem o uso do QS^2, são apresentados na Figura 3. A confiabilidade dos dados nesses cenários, tanto diante de ataques de injeção de dados quanto diante de todos os ataques é inferior a 10%. Os resultados são condizentes com estudos prévios [Mannes et al. 2009], e evidenciam que é necessário empregar um mecanismo de segurança para garantir a integridade e a disponibilidade dos dados.

A Figura 4 apresenta a confiabilidade nos dados diante de ataques de injeção de dados no cenário urbano. Nesses cenários, o G_c se apresenta acima de 55%, com um aumento superior a 45% em relação aos cenários sem o uso da solução. Ainda, conforme observado em [Mannes et al. 2011], a mobilidade dos nós atua a favor do QS^2, ajudando na obtenção de informações sobre o comportamento dos demais nós. Contudo, o tempo de pausa prolongado dos nós nesses cenários pode causar um atraso no cálculo das informações do QS^2.

Também observa-se que o G_c é superior em cenários com todos os ataques, e isso ocorre devido a divisão da quantidade total de nós de má-conduta entre todos os ataques, sendo que os ataques de falta de cooperação e de temporização amenizam o impacto dos ataques de injeção de dados.

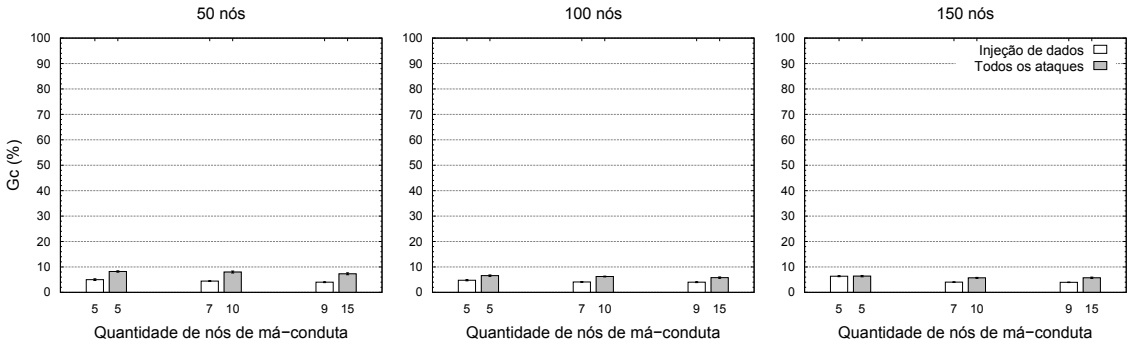

Figura 3. G_c em cenários urbanos sem o uso do QS^2

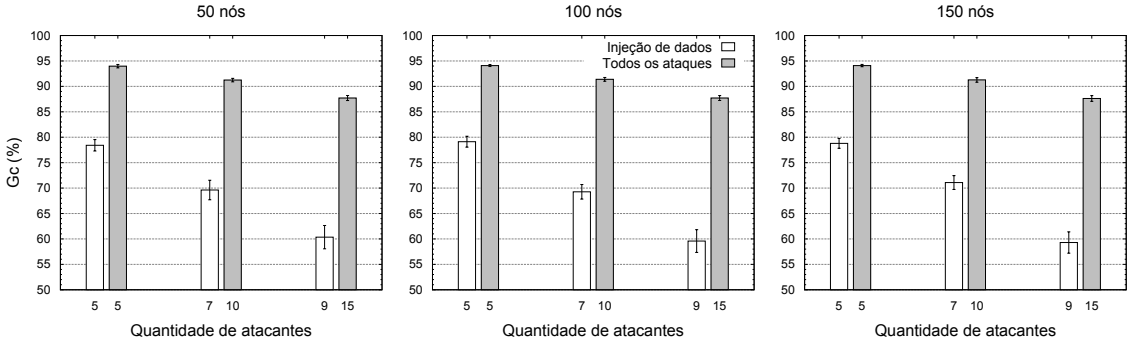

Figura 4. G_c em cenários urbanos

5.3.2. Eficiência

Para os cenários urbanos, a eficiência de detecção dos ataques de injeção de dados é superior à 90%, e aumenta em relação à quantidade de nós de má-conduta presentes na rede. Contudo, esse comportamento não é observado na detecção nos cenários com todos os ataques, em que a Tx_{det} se mantém entre 85% e 90%, independente da quantidade de nós de má-conduta ou da quantidade de nós na rede, observado na Figura 5

5.3.3. Dados falsos *versus* dados desatualizados

Devido à discrepância entre a confiabilidade alcançada e a taxa de detecção apresentada, suspeitou-se que a confiabilidade alcançada em tais cenários não seria devido a ação dos nós de má-conduta ou a perda de eficácia do QS^2, e sim uma perda normal para o ambiente de rede, pelas próprias características do cenário. Para verificar essa suposição, foram quantificadas as taxas de leituras que obtiveram dados falsos (Tx_{mis}) e dados desatualizados (Tx_{out}). Para ambos os ataques, a suposição se mostrou verdadeira.

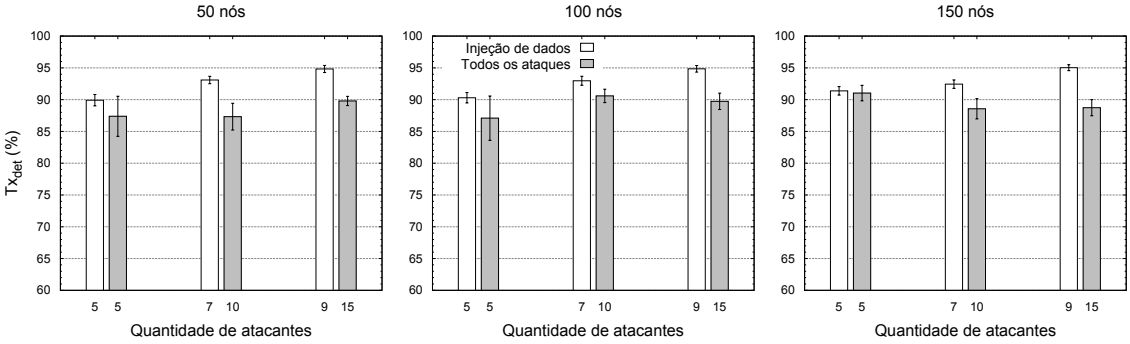

Figura 5. Tx_{det} em cenários urbanos

Nos ataques de injeção de dados, a Tx_{mis}, Figura 6, é inferior a metade da Tx_{out}, Figura 7. Enquanto que a quantidade de dados falsos obtidos com 5 nós de má-conduta é em média de 12%, a quantidade de leituras desatualizadas obtida nesse mesmo cenário é de 39%, em média. Além disso, a Tx_{mis} cresce em torno de 1% com o aumento da quantidade de nós e a Tx_{out} aumenta em média 10% nessas mesmas condições.

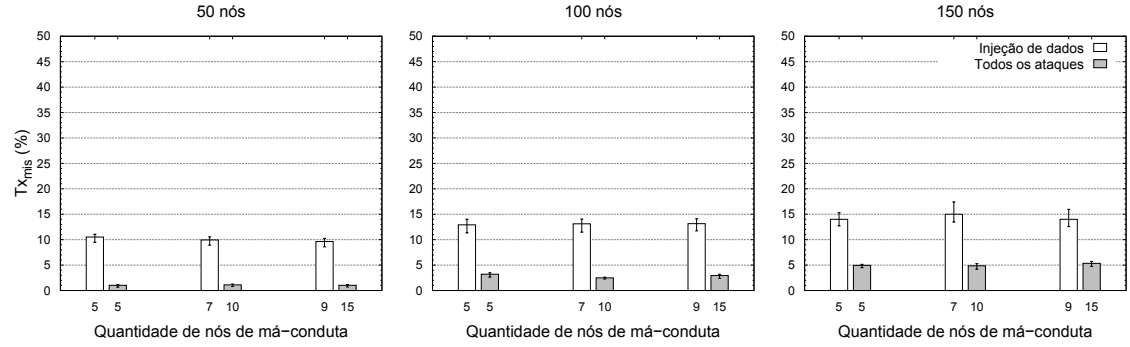

Figura 6. Dados maliciosos no sistema de quórum (Tx_{mis})

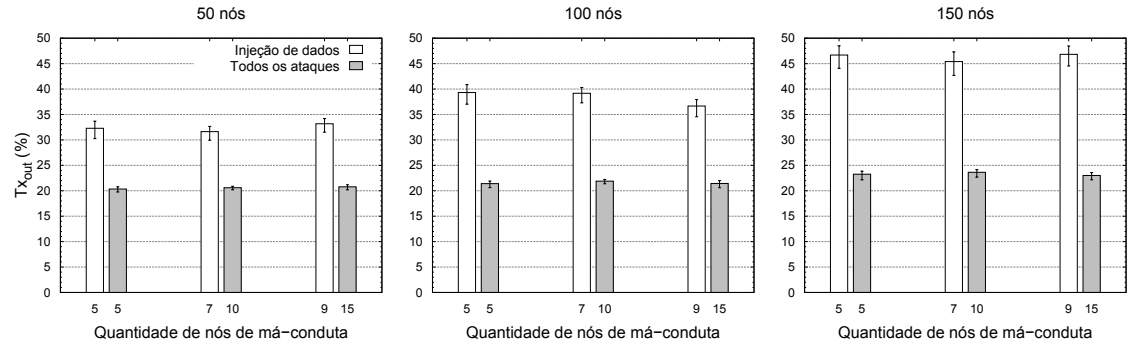

Figura 7. Dados desatualizados no sistema de quórum (Tx_{out})

Isso evidencia que a confiabilidade nesses cenários é prejudicada, em parte, devido à topologia da rede, como o tamanho da área de movimentação e a densidade de nós. Ainda assim, o QS^2 obteve boas Tx_{det} e G_c, sendo a última superior ao alcançado sem o uso do QS^2 em cenários de validação [Mannes et al. 2009].

5.4. Ambiente de transporte - linhas de ônibus

Esse cenário baseia-se no trabalho realizado em [Jetcheva et al. 2003] e é aplicado em um ambiente de transporte suportado por uma arquitetura de roteamento chamada de *Ad Hoc City*. Ela é utilizada para a distribuição de informações entre veículos, usuários e terminais de transporte público e privado, sendo que os usuários podem participar dessa arquitetura utilizando dispositivos sem fio como *notebooks*, celulares ou *tablets*. Nesse tipo de cenário, a mobilidade e a falta de infraestrutura são evidentes e precisam ser gerenciadas para que a aplicação de distribuição de mensagens possa funcionar de maneira adequada. A utilização dos sistemas de quórum para o apoio na tolerância a essas falhas também necessita ser robusta para garantir a entrega de informações íntegras e atualizadas para os usuários. Nós podem comprometer a funcionalidade da rede evitando que os nós confiáveis recebam dados úteis. e desta forma, precisam ser tratados.

Esse cenário se caracteriza por um *backbone* composto por ônibus e veículos de entrega, que cobrem uma área específica na cidade. Esses veículos são organizados de maneira *ad hoc*, e fornecem acesso à rede para a comunicação em geral. Além disso, oito estações fixas são distribuídas ao longo da cidade, com o objetivo de melhorar a escalabilidade da rede e fornecer acesso à Internet aos usuários. O cenário corresponde ao sistema de ônibus (*King County Metro*) da cidade de *Seattle* (USA). O padrão de movimentação dos ônibus foi obtido por [Jetcheva et al. 2003] através de observação da movimentação real dos ônibus durante os períodos da manhã e da tarde durante duas semanas.

Originalmente em [Jetcheva et al. 2003], considera-se a existência de aproximadamente 850 ônibus movimentando-se em uma área de 5100km^2. Devido a limitações computacionais, o cenário foi adaptado para uma topologia de 150 nós, distribuídos em uma área de 1500 x 2000 metros. Os nós seguem o padrão de movimentação dos ônibus, e movem-se entre 0 e 90 km/h. Foram utilizadas 8 estações fixas, distribuídas proporcionalmente no cenário, mantendo o proposto em [Jetcheva et al. 2003].

O quórum de leitura (Q_r) é composto por quatro servidores, incluindo o agente, e o quórum de escrita (Q_w) é formado por todos os nós que recebem a escrita de um dado, sendo que cada nó dissemina os dados para quatro servidores a cada T=200ms. O conjunto de armazenamento (StS) é composto por 30 nós, escolhidos randomicamente. 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, e é dado em segundos. A taxa máxima de escritas é igual a $k_{env^{max}} = 0,018$ escritas por segundo, e a taxa de encaminhamento deve ser superior a $k_{enc^{min}} = 0,15$ pacotes por segundo.

O padrão de movimentação utilizado refere-se a um intervalo de quinze minutos dos registros obtidos por [Jetcheva et al. 2003]. Para simular cenários da rotina dos ônibus pela manhã, considerou-se os registros obtidos das 07:15 às 07:30, e para a tarde, utilizou-se os registros obtidos entre 17:15 e 17:30. Como protocolo de roteamento empregou-se o AODV e as simulações têm duração de 900 segundos.

5.4.1. Grau de confiabilidade

Assim como no cenário urbano, a confiabilidade do sistema PAN sem o uso do QS^2 e diante de ataques é inferior a 10%. Isso se aplica às situações com ataques de injeção de dados e às situações com todos os ataques, apresentados na Figura 8(a). Com o uso

do QS^2, Figura 8(b), a confiabilidade dos dados se mantém acima de 60% para ambos os cenários da manhã e da tarde. As diversas paradas dos ônibus em pontos de embarque para usuários e terminais centrais ocasionam uma aceleração irregular, o que pode gerar perda dos pacotes de dados no meio sem fio. Além disso, o tempo de pausa desses veículos também tem uma grande variação, e esses tempos de pausa prolongados não favorecem a disseminação e a contabilização das mensagens de escrita por todos os nós da rede, influenciando a confiabilidade dos dados.

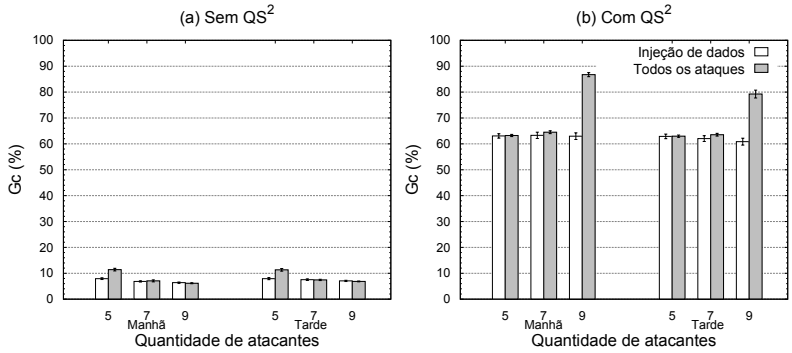

Figura 8. G_c em cenários de transporte sem o uso do QS^2

5.4.2. Eficiência

A eficiência de detecção (Tx_{det}) do QS^2, apresentada na Figura 9, está de acordo com os resultados de G_c obtidos. Enquanto que a Tx_{det} para os cenários com ataques de injeção de dados, Figura 9(a), é superior a 65% e cresce com o aumento do número de nós de má-conduta, a Tx_{det} para os cenários com todos os ataques, Figura 9(b), é inferior a 80%.

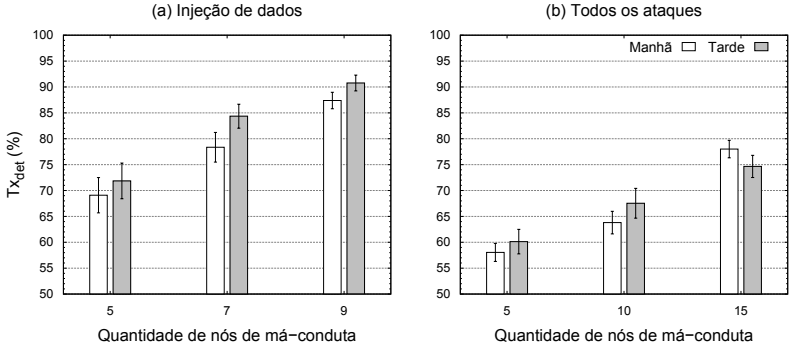

Figura 9. Tx_{det} em cenários de transporte

A eficiência na detecção dos nós de má-conduta em cenários com todos os ataques é menor devido à falta de uma forma adequada de identificação do ataque de temporização, e à demora para a detecção dos nós egoístas, que fazem parte dos nós de má-conduta presente na rede. Além disso, por conta do cenário utilizado, os nós podem encontrar dificuldades na troca de mensagens, e dessa forma, a detecção dos nós pode atrasar. Isso causa menores taxas de detecção dos nós de má-conduta.

5.4.3. Dados falsos *versus* dados desatualizados

Da mesma forma que o cenário anterior, as taxas de dados falsos (Tx_{mis}) e de dados desatualizados (Tx_{out}) mostram que a quantidade de dados falsos obtidos pelos nós por

meio de leituras no sistema de quórum é menor do que a quantidade de dados desatualizados. A Figura 10 apresenta as taxas Tx_{mis} e Tx_{out}. Nela, observa-se que em ambos os cenários aproximadamente 50% dos dados obtidos pelos nós são descartados porque não estão atualizados, e apenas cerca de 10% são dados falsos, injetados por nós maliciosos.

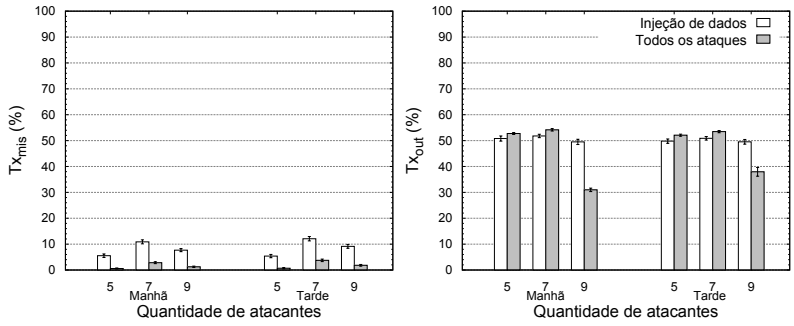

Figura 10. Tx_{mis} e Tx_{out} em cenários de transporte

Tais resultados evidenciam que a rede apresenta dificuldade na entrega de dados, o que possivelmente é consequência do padrão de movimentação dos ônibus. Essa dificuldade em entregar dados, por sua vez, prejudica a disseminação dos dados de replicação e das mensagens utilizadas pelo QS^2 para a detecção dos nós de má-conduta. Porém, o QS^2 continua detectando e excluindo os nós de má-conduta, o que é evidenciado pela maior quantidade de dados desatualizados do que dados modificados por nós maliciosos.plicação em comparação com a quantidade de dados desatualizados.

6. Conclusão

Este artigo avaliou o QS^2, um esquema para a exclusão de nós egoístas e maliciosos das operações de replicação em um sistema de quórum para MANETs. Essa avaliação considerou dois cenários realísticos: a distribuição de informações para pedestres em um ambiente urbano e a distribuição de informações de tráfego em linhas de ônibus. Os resultados obtidos mostram que o QS^2 proporcionou um aumento na confiabilidade de um sistema de quórum para MANETs comparado com o mesmo sistema de quórum sem o uso do QS^2. O aumento em ambos os cenários foi superior a 45% com ataques de injeção de dados nas escritas e com uma combinação de vários ataques. A detecção de nós egoístas obtida pelo QS^2 foi acima de 55%. Além disso, observou-se que a quantidade de dados falsos contidos no sistema de replicação é inferior à quantidade de dados desatualizados, sendo que ambos interferem na confiabilidade dos dados. Como trabalhos futuros, pretende-se estudar e quantificar o comportamento dos serviços de operação de rede em MANETs de forma a identificar limites de escrita e encaminhamentos mais reais. Além disso, propõe-se o estudo e a incorporação de novos indicativos que identifiquem de forma precisa cada tipo de ataque considerado, principalmente o ataque de temporização.

Referências

Becker, C., Bauer, M., and Hähner, J. (2002). Usenet-on-the-fly: supporting locality of information in spontaneous networking environments. In *Workshop on Ad Hoc Communications and Collaboration in Ubiquitous Computing Environments*. ACM Press.

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.

Conti, M., Chong, S., Fdida, S., Jia, W., Karl, H., Lin, Y.-D., Mähönen, P., Maier, M., Molva, R., Uhlig, S., and Zukerman, M. (2011). Research challenges towards the future internet. *Computer Communications*, 34(18):2115 – 2134.

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.

Jetcheva, J. G., Hu, Y.-C., PalChaudhuri, S., Saha, A. K., and Johnson, D. B. (2003). Design and evaluation of a metropolitan area multitier wireless ad hoc network architecture. In *Proceedings of the 5th IEEE Workshop on Mobile Computing Systems and Applications*, pages 32–43.

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*, pages 1–12.

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

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*, pages 71–84.

Mannes, E., Nogueira, M., and dos Santos, A. (2011). Um esquema bio-inspirado para tolerância à má-conduta em sistemas de quórum para manets. In *Anais do XI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 239–252, Brasília, DF.

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*, pages 269–282.

Sardiña, I. M., Boeres, C., and Drummond, L. (2011). Escalonamento estático bi-objetivo e tolerante a falhas para sistemas distribuídos. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 573–583.

Tian, J., Haehner, J., Becker, C., Stepanov, I., and Rothermel, K. (2002). Graph-based mobility model for mobile ad hoc network simulation. In *Proceedings of the 35th Annual Simulation Symposium*, pages 337–, Washington, DC, USA. IEEE Computer Society.

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*, 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*, pages 251 –255.

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.