Mecanismo de detecção de ataques *Wormhole* em Redes Tolerantes a Atrasos e Desconexões

Henrique Zelak Leite Bastos e Luiz Carlos Pessoa Albini

***Resumo*— Redes Tolerantes a Atrasos e Desconexões (DTN) são redes sem infraestrutura ou unidade centralizadora e que permitem que os nós troquem mensagens mesmo sem a existência de rotas entre eles. Estes pontos são comumente explorados em ataque à rede. Um desses ataques é o *wormhole*. Ele utiliza uma infraestrutura preexistente para forçar que as rotas usem sempre o nó atacante, obrigando que uma grande quantidade de mensagens passe necessariamente pelos dispositivos atacantes. Desta forma, ele pode interceptar mensagens ou simplesmente neutralizar a rede, enviando informações desconexas para os nós comunicantes. Este artigo apresenta um novo método para detecção de ataques *wormhole* em redes DTN baseado no uso de um GPS pelos nós. Com isso, é possível determinar com precisão a integridade dos nós da rede, melhorando o desempenho de métodos anteriores.**

***Palavras-Chave*— Redes tolerantes à atrasos e desconexões, Ataque *Wormhole*.**

***Abstract*— Delay Tolerant Networks (DTNs) do not have any infrastructure or centralized unit and they allow nodes to exchange messages without routes between them. These points are commonly explored by attackers. One of these attacks is the wormhole. It uses a pre-established infrastructure to force all routes to go through the attacker, forcing a large number of messages to go through such nodes. In this way, the attacker can intercept messages or even neutralize the network. This article presents a new method to detect wormhole attacks in DTNs, based on GPS equipped nodes. Thus, it is possible to precisely determine the integrity of the network nodes, improving the performance of previous methods.**

***Keywords*— Delay tolerant networks, *Wormhole* attack.**

I. INTRODUÇÃO

Redes Tolerantes a Atrasos e Desconexões (*Delay Tolerant Network* - DTN) [1] são casos especiais de redes *ad hoc*. Elas permitem que os nós troquem mensagens mesmo sem a existência de rotas entre eles, i.e. é possível enviar mensagens mesmo que o destino delas esteja inalcançável durante um período de tempo. Assim como as redes *ad hoc*, as DTNs são redes sem qualquer infraestrutura ou entidade centralizadora, nas quais os dispositivos podem se mover livremente, inclusive saindo do raio de cobertura da rede. Além de herdar as características das redes *ad hoc*, redes DTNs possuem as suas próprias características como roteamento específico, baseado no armazenamento de mensagens em nodos intermediários, e conexões intermitentes, que podem variar de poucos milissegundos a dias ou, até mesmo, anos.

Henrique Zelak Leite Bastos e Luiz Carlos Pessoa Albini¸ NR2 - Departamento de Informática, Universidade Federal do Paraná, Curitiba-PR, Brasil, E-mails: hzlb08@inf.ufpr.br, albini@inf.ufpr.br.

A ausência de uma unidade certificadora plenamente confiável, a presença de conexões intermitentes e a incapacidade de determinar se um nó está agindo de maneira íntegra são pontos comumente explorados para atacar a rede. Um desses ataques é o *wormhole*. Este método se utiliza de uma infraestrutura preexistente no cenário para forçar que as rotas usem sempre o nó atacante. O objetivo do ataque *wormhole* é forçar que uma grande quantidade de mensagens passe necessariamente pelos dispositivos atacantes. Desta forma ele pode interceptar mensagens ou simplesmente neutralizar a rede, enviando informações desconexas para os nós comunicantes. Para tanto, dois nós atacantes distantes estabelecem um enlace de comunicação de alta velocidade entre eles e se comunicam com uma taxa de transferência acima do padrão da rede. Com isso, dois nós íntegros que desejam se comunicar utilizarão a rota através dos atacantes, pois eles entregarão as mensagens de maneira mais rápida e com um número menor de encaminhamentos de mensagens. Caso a rede não possua nenhum tipo de método de detecção de ataque *wormhole* e caso ela tenha baixa mobilidade, se estabelecendo ao redor dos atacantes, existe um grande risco de que a rede toda seja comprometida, pois os atacantes podem causar risco à integridade e à inviolabilidade das mensagens trocadas.

Em [2] é apresentado um algoritmo para detectar ataques *wormhole* em redes DTN. Este artigo apresenta um novo método para detecção de ataques *wormhole* em redes DTN baseado no algoritmo proposto em [2] e considerando que todos os nós possuem um GPS integrado. Com isso, é possível determinar com precisão a integridade dos nós da rede, criando rotas sem a presença de atacantes e garantindo maior confiabilidade à rede.

II. MÉTODO DE DETECÇÃO

A detecção da presença de um ataque *wormhole* de [2] se baseia na relação trigonométrica. Cada nó deve enviar uma mensagem em *broadcast* para todos os seus vizinhos, solicitando a redução do tamanho do raio de cobertura, quebrando diversas conexões existentes. Para isso, os autores definem que se o nó A pode receber mensagens de B então A é vizinho de B. Considerando os nós A, B e C, B e C de raio R e A de raio r, em que $r = R/2$. Sabendo que $A \in N(B)$ e $B \in N(A)$, então a distância entre eles é $dist(A, B) \leq r$ e $N(A) \subseteq N(B)$. Se $C \in N(A)$ e $A \in N(C)$, analogamente à afirmação anterior tem-se que $dist(A, C) \leq r$ e $N(A) \subseteq N(C)$.

Portanto se $dist(A, C) \leq r$ e $dist(A, B) \leq r$ então $dist(B, C) \leq R$. Como o raio de B e C é igual a R então

$C \in N(B)$ e $B \in N(C)$. Logo, se $C \notin N(B)$ então $dist(A, C) > r$. Assim, tem-se que A e C constituem uma topologia proibida e tais nós estão se comunicando através de mecanismos não regulares à rede. Quando for detectado três vezes que um nó é malicioso, toda a rede é avisada.

Contudo, este método possui alguns problemas. Um dos principais é que cada nó testará à rede em um momento diferente, ou seja, as rotas serão quebradas frenquentemente. Além disso, será gerada uma alta sobrecarga de mensagens para o restabelecimento das rotas. O segundo problema é em relação ao tempo que levará para os nós reduzirem fisicamente os raios, descobrirem seus vizinhos e avisarem o nó que solicitou o teste sobre sua nova vizinhança. Durante este tempo os nós podem entrar ou sair da rede, gerando informações imprecisas. Outro ponto importante é no caso de uma rede esparsa, pois o algoritmo exige que os nós tenham pelo menos dois vizinhos para realizar o teste.

III. Algoritmo

Na abordagem apresentada neste artigo, os nós mantêm informações sobre a localização geográfica da sua vizinhança local, com a utilização de um GPS integrado. Desta forma, não é necessário reduzir fisicamente o raio, evitando a quebra de conexões e todos os problemas decorrentes disso. Os nós trocam informações de vizinhança do mesmo modo que em [2], porém utiliza-se o GPS ao invés da redução do raio de comunicação para estabelecer a vizinhança.

Além disso, os nós são testados quando ocorre o estabelecimento de uma nova conexão e sem a necessidade da presença de, no mínimo, dois vizinhos independentes.

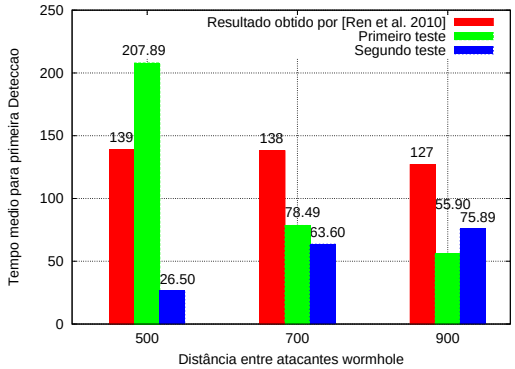
IV. Análise

Com o objetivo de ter uma comparação efetiva, o primeiro teste foi nos moldes do realizado por [2]. O mapa possui dimensão de 2000m x 2000m e os nós usam o modelo de movimentação *Random way point*. Para testar mais efetivamente o efeito de atacantes na rede, foi aumentada a densidade da rede no segundo teste. Este teste foi realizado em um mapa de 1000m x 1000m, usando o modelo de movimentação em *Cluster*. Dez nós produtores de mensagens ficam localizados perto de cada atacante, sendo que os nós só criam mensagens destinadas a nós próximos ao segundo atacante.

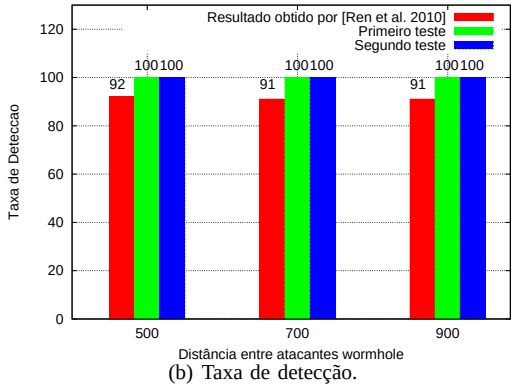
Em ambos os testes, havia 52 nós na rede, sendo 20 transmissores. O protocolo de roteamento utilizado é o PROPHET *(Probabilistic Routing Protocol)*. A velocidade máxima dos nós é 5m/s e a mínima é 1m/s e o raio de cobertura de cada nó é 100m.

A. Resultados

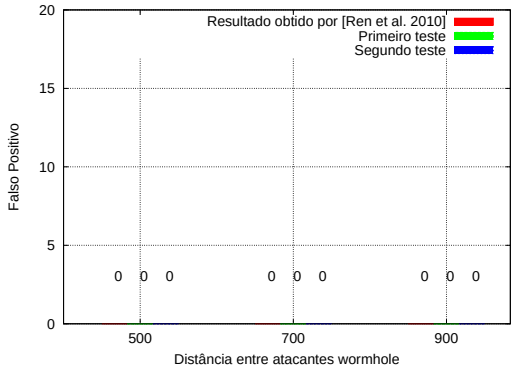
Os resultados apresentados na Figura 1(a) demonstram que o método proposto apresenta um melhor desempenho que o método anterior. Além disso, como esperado, pode-se verificar que quanto mais densa a rede, mais rápida é a detecção de um atacante. A melhora na taxa de detecção de atacantes é apresentada na Figura 1(b). A Figura 1(c) mostra que não há perda na confiabilidade das informações, pois, assim como em [2], nenhum nó detectou um nó íntegro como sendo atacante.



(a) Tempo médio para detecção do primeiro atacante.



(b) Taxa de detecção.



(c) Falso Positivo.

Fig. 1. Resultados dos testes.

V. Conclusão

Um ataque *wormhole* pode comprometer o funcionamento de toda a DTN. Por isso, é importante detectar possíveis atacantes o quanto antes. O método apresentado neste artigo utiliza informações de posicionamento para esta detecção, mesmo que isso represente um aumento no custo de cada dispositivo, já que haverá a adição de um sistema de GPS em cada um. Resultados apresentados demostram uma melhora na eficiência da detecção de atacantes, sem reduzir a confiabilidade dos resultados.

Referências

[1] N. W. GROUP, *Delay-tolerant networking architecture, request for comments: 4838*. http://www.ietf.org/rfc/rfc4838.txt, 2007.

[2] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay-tolerant networks," *Wireless Communications*, vol. 17, pp. 36–42, Oct. 2010.