PROTOCOLOS DE ROTEAMENTO EM REDES MÓVEIS AD-HOC (MANET): UMA REVISÃO SISTEMÁTICA

Erika Harumi Akashi (PIBIC/CNPq/FA/UEM), Elvio João Leonardo (Orientador), e-mail: ra110568@uem.br

Universidade Estadual de Maringá / Centro de Tecnologia / Maringá, PR

Área e sub-área do conhecimento: Ciência da Computação / Sistemas de Computação.

Palavras-chave: Protocolos, roteamento, MANET.

Resumo:

As redes Ad-Hoc (MANET) são redes do tipo não infraestruturadas móveis. Devido à alta mobilidade dos nós, a topologia da rede é altamente mutável, e problemas como seleção e manutenção de rotas são um dos principais envolvendo este tipo de rede. Protocolos de roteamento em redes MANET são essenciais, pois nesta etapa diversos problemas podem ocorrer, como falha no *link*, que afeta a estabilidade da rota, *overhead*, perdas de pacote, *delay*, ameaças de segurança e problemas relacionados ao consumo de energia, contribuindo na degradação da rede. Neste trabalho, são abordados alguns protocolos, modelos e esquemas que visam otimizar o processo de roteamento, além de analisar os desafios e possíveis soluções para as questões a respeito de protocolos de roteamento em redes MANET.

Introdução

As redes de comunicação sofreram uma rápida evolução nos últimos anos. Robustez, estabilidade e velocidade são as características mais almejadas. Além disso, a alta demanda por redes de comunicação sem fio (*wireless*), incorporadas em diversas aplicações do cotidiano, exigem topologias e protocolos cada vez mais avançados.

As redes móveis do tipo Ad-Hoc são consideradas descentralizadas, pois a comunicação é feita por meio da utilização de seus nós como roteadores e/ou receptores. O nó remetente utiliza os nós vizinhos para estabelecer uma rota até o nó de destino, sem a necessidade de estruturas físicas fixas para realizar a comunicação.

Como a rede é descentralizada e a comunicação e estabelecida diretamente entre os nós, é necessário selecionar o caminho, por meio do roteamento, para encaminhar os pacotes de dados entre os nós, ou ainda, selecionar e estabelecer um caminho entre redes distintas. Neste caso, os *gateways* desempenham um papel de passagem ou portal, permitindo que a correta comunicação entre diferentes tipos de rede seja realizada.

As características das redes móveis Ad-hoc, como a descentralização, ausência de estruturas físicas e flexibilidade permitem sua implementação em locais inóspitos ou de emergência, áreas de monitoramento.

Entretanto, essas mesmas características trazem outros problemas, como a necessidade de rápida adaptação devido à topologias muito complexas, problemas de escassez de energia e interferência.

Materiais e Métodos

Por se tratar de uma revisão sistemática, foram considerados artigos acadêmicos de acesso livre da plataforma IEEExplore publicados entre 2018 até a data atual, de acordo com sua relevância. Os tópicos de publicação foram filtrados para encontrar resultados focados na apresentação de novos protocolos e otimizações daqueles já consolidados na área. Como milhares de resultados surgiram, mesmo com a aplicação de todos os critérios acima, foram desconsiderados artigos muito específicos de VANET (Vehicular Ad-hoc Networks) e FANET (Flying Ad-hoc Networks), revisões sistemáticas e trabalhos que não apresentavam simulações, resultando em 17 trabalhos para a revisão.

Resultados e Discussão

Os desafios atuais dos protocolos de roteamento das redes MANET, incluem o Quality of Service (QoS) segundo Nisar et al. (2020), que se trata de uma métrica que avalia diversos parâmetros, inclusive os que foram descritos acima, para determinar a qualidade dos protocolos.

A segurança e o consumo de energia também são grandes preocupações envolvendo a expansão das redes MANET. Como a topologia da rede é dinâmica e muito flexível, nós maliciosos podem se juntar a rede, performando diversos tipos de ataques, como Abdel-Fattah et al. (2019) relata em seu trabalho. Essa mesma flexibilidade que confere às redes MANET maior vulnerabilidade a ataques, também dificulta sua manutenção, já que são geralmente encontradas em ambientes inóspitos ou de difícil acesso. Segundo Singh; Prakash (2020), a economia de energia é um fator de extrema relevância, visto que os dispositivos pertencentes à rede, podem não ter a possibilidade de trocas constantes de bateria.

Dentre os protocolos e esquemas analisados, incluem àqueles que tem como objetivo a seleção da melhor rota (geralmente a mais curta), ou gateway, tendo o QoS como critério de avaliação de performance, seja pela robustez da rota como o caso do *Bio-inspired gateway selection scheme,* Synchronized Fuzzy Ant System (SynfAnt) e o ACO-*non-root-base* que utilizam modelos biológicos para encontrar rotas mais estáveis mesmo em ambientes altamente dinâmicos. Já outros protocolos priorizam a seleção da rota mais curta, considerando rotas alternativas, caso a principal venha a apresentar falhas, como é o caso do *Topological change Adaptive Ad Hoc on-Demand Multipath Distance Vector* (TA-AOMDV), *Zone-based Route Discovery Mechanism* (ZRDM) e *Link Disjoint Multipath* (LDM).

O *Ad Hoc on-Demand Multipath Distance Vector with fitness function* (AOMDV-FFn) utiliza de parâmetros determinados pelo *Fitness Function* (FF)

combinado com o protocolo *Ad Hoc on-Demand Multipath Distance Vector* (AOMDV), com a finalidade de traçar a melhor rota seguindo as métricas determinadas pelo FF, que incluem: (i) energial residual de cada nó. (ii) distância de cada possível rota. (iii) congestionamento e (iv) desconsideração de perdas randômicas e perdas por congestionamento.

Por fim, o protocolo *Trust Entropy Optimizes Link State Routing* (TUE-OLSR) implementa algoritmos no protocolo OLSR, atribuído níveis de confiança aos nós e então, aqueles com maior nível de confiança são selecionados para compor a rota.

O *Hybrid Wormhole Attack Detection* (HWAD), *Secure-Neighbor-Selection* (SNS-RR), *Active routing Authentication Scheme* (AAS), *Accurate Prevention and Detection of Jelly fish Attack* (ADP-JFAD), *Black-hole Protected Ad hoc on-Demand Distance Vector* (BP-AODV) e o *Dual-Cooperative Bait Selection Scheme* (D-CBDS), tem por objetivo, a proteção das redes contra ataques vindos de nós maliciosos que adentram a rede. Alguns desses protocolos e esquemas são focados em proteger especificamente contra um tipo de ataque, como é o caso do BP-AODV, HWAD e ADP-JFAD, que protegem as redes MANET contra ataques do tipo, *black-hole*, *wormhole* e *jelly fish*, respectivamente. Vale ressaltar que o BP-AODV é uma otimização do protocolo *Ad hoc on-Demand Distance Vector* (AODV), que não possuía nenhum mecanismo para lidar com ataques do tipo *black-hole*. Já outros esquemas como o AAS, SNS-RR e D-CBDS são esquemas que se propõem a aumentar a segurança da rede independente do ataque, aplicando esquemas de autenticação, como o AAS e o SNS-RR, ou aumentando a quantidade de nós envolvidos no processo de verificação, como é o caso do D-CBDS que é uma otimização do *Cooperative Bait Detection Scheme* (CBDS), implementando dois nós vizinhos no esquema ao invés de apenas um, como era feito no CBDS.

Foi encontrado na pesquisa um protocolo que visa economizar energia, como é o caso do *Link Lifetime and Energy Consumption AOMDV* (LLECP-AOMDV), cujo objetivo é poupar energia na fase de descobrimento de rota, por meio de um *threshold* de energia na fase de seleção. Este nível determina se a energia no nó está abaixo ou não de níveis aceitáveis. Caso esteja, o protocolo reserva o nó para utilizá-lo apenas como destinatários ou remetentes, poupando energia.

Também há o *Retransmission Dual-Busy Tone Multiple Access* (R-DBTMA), visando um esquema de rápida retransmissão, evitando o problema de terminal escondidido (*hidden terminal*), utilizando de sinais de *Negative Acknowledgement* (NACK) para fazer a retransmissão de pacotes.

Por fim, há o esquema *Link Failure Prediction Mechanism* (LFPM), apresentado juntamente ao ZRDM (elaborado pelos mesmos autores no mesmo artigo), cujo objetivo envolve prever falha no link. O esquema checa a estabilidade da conexão periodicamente, e elabora uma nova rota alternativa antes que ocorra falha no link. O nó de destino envia uma mensagem para o remetente, para que este execute novamente o processo de descobrimento de rota, e uma nova seja estabelecida.

Os parâmetros mais analisados pelos autores em seus artigos foram o *packet delivery ratio* (PDR), *end-to-end delay* (E2ED), *overhead* (OH), taxa de transferência e consumo de energia. A maior parte dos protocolos superavam a performance dos outros usados nas simulações, com algumas exceções. Alguns protocolos de

segurança, por exemplo, apresentavam piores resultados em algumas métricas comparado aos demais em situações onde não haviam muitos nós maliciosos presentes. Em contrapartida, conforme o número de nós maliciosos aumentava, a eficiência do protocolo aumentava também.

Conclusões

Como visto na seção anterior, os temas de segurança e otimização de energia são muito recorrentes no cenário de protocolos de roteamento das redes MANET. Vários protocolos e esquemas apresentavam inclusive algoritmos baseados em sistemas e organismos biológicos, como sistemas de colônias de formigas e o algoritmo genético. Os protocolos híbridos apresentaram muitos resultados positivos devido à sua complexidade, e são capazes de se adaptar muito bem a topologia flexível inerente às redes MANET. Entretanto, como discutido na seção anterior, há os *trade-offs*: se por um lado esses algoritmos são capazes de detectar a melhor rota, ou melhorar a segurança da rede, devido à sua alta complexidade, podem apresentar maior latência, OH ou apresentar degradação de outros parâmetros sob determinadas circunstâncias. Por isso, as características da rede (mobilidade, número de nós, velocidade dos nós) onde o protocolo será implementado deve ser bem conhecida, pois o desempenho do mesmo pode variar drasticamente de acordo com as características das mesmas.

Agradecimentos

O presente trabalho foi realizado com o apoio do PIBIC/CNPq-UEM.

Referências

ABDEL-FATTAH, F.; FARHAN, K. A.; AL-TARAWNEH, F. H.; ALTAMIMI, F. **Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs**. IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)), 2019.

NISAR, K.; LAWAL, I. A.; ISMAIL ABDULMALIK, U.; et al. QoS Analysis of the MANET routing protocols with Respect to Delay, Throughput, & Network load: Challenges and Open Issues. 14th IEEE International Conference on Application of Information and Communication Technologies, AICT 2020 - Proceedings. **Anais...** , 2020. Institute of Electrical and Electronics Engineers Inc.

SINGH, S. K.; PRAKASH, J. **Energy Efficiency and Load Balancing in MANET: A Survey**. 6th ICACCSD ed. 2020.