SecOverlay – Redes Overlay sobre Redes de Sensores Sem Fio para Transmissão Segura de Dados

Leonardo B. Oliveira[1], **Eduardo Habib**[2], **Daniel Camara**[2],
Hao Chi Wong[3], **Antonio A. F. Loureiro**[2], **Ricardo Dahab**[1],

[1] Instituto de Computação
Universidade Estadual de Campinas (UNICAMP)
Campinas, SP

[2]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais (UFMG)
Belo Horizonte, MG

[3]Palo Alto Research Center (PARC)
Palo Alto, CA, EUA

{leob,rdahab}@ic.unicamp.br,{habib,danielc,loureiro}@dcc.ufmg.br,{hcwong}@parc.com

Resumo. *Este trabalho avalia o uso de redes overlay (ROs) para segurança em Redes de Sensores Sem Fio (RSSFs). Os resultados preliminares da pesquisa indicam que para ataques comuns como blackhole e selective forwarding as ROs podem prevenir, respectivamente, a perda de 35,9% e 18,6%, das mensagens prioritárias em redes com 5% de nós atacantes.*

Abstract. *This paper evaluates the use of overlay networks (ONs) for securing wireless sensor networks (WSNs). The preliminary results indicate that the use of ONs can prevent, 35.9% of data loss under a blackhole attack and 18.6% under a selective forwarding attack, in networks with 5% of compromised nodes.*

1. Introdução

Redes de Sensores Sem Fio (RSSFs) [1] são redes ad hoc compostas basicamente por pequenos nós sensores de recursos limitados e uma ou mais estações rádio base (ERBs). Além das vulnerabilidades de segurança inerentes à comunicação sem fio, RSSFs enfrentam problemas adicionais [2]. Elas comumente são dispostas em ambientes abertos e são fisicamente acessíveis a adversários, isto as torna suceptíves a uma nova gama de ataques – *blackhole* e o *selective forwarding* [3], por exemplo.

Já Redes *Overlay* (ROs) são redes construídas sobre redes físicas tradicionais, com o intuito de migrar parte da complexidade de roteamento para a camada de aplicação [4]. Baseadas em um dado critério, ROs são capazes de monitorar a rede e fornecer caminhos alternativos ao usuário. Tais caminhos são construídos através da atuação de nós *overlay* como intermediários no envio de dados.

RSSFs podem ser organizadas de maneiras diversas [1]. Por exemplo, em *RSSFs hierárquicas* [1], a rede é em geral organizada em grupos (*clusters*). Enquanto membros comuns são responsáveis pelo sensoriamento, líderes (CHs – *clusters-heads*) são responsáveis por tarefas adicionais, tais como coletar e processar o dado sensoriado pelos demais membros do grupo, e reencaminhar os resultados para a ERB. Note-se que uma estratégia de segurança eficiente para uma dada organização pode não ser eficiente para outra.

O objetivo deste trabalho é avaliar o emprego de ROs para aumentar a segurança de RSSFS hierárquicas. Na verdade, ao empregar redes ROs sobre RSSFS, esperamos aumentar a taxa de entrega de mensagens cujas informações sejam valiosas. Nosso especial interesse por redes hierárquicas deve-se ao melhor custo-benefício de tais organizações [5].

2. Trabalhos Relacionados

Atualmente, um número razoável de trabalhos lidam com segurança em RSSFs ([7, 8], por exemplo). Por outro lado, poucos são os trabalhos especialmente voltados para segurança em RSSFs hierárquicas.

Kong *et al.* [9] e Bohge e Trappe [10] projetaram soluções para redes hierárquicas e heterogêneas. Todavia, eles supõem nós muito poderosos, capazes de executar algoritmos de chave pública, o que não é viável em RSSFs.

Mais recentemente, sugiram propostas que dependem apenas de primitivas simétricas de criptografia [11, 12]. Ferreira *et al.* [11] propuseram SLEACH, uma extensão segura do protocolo hierárquico LEACH que possibilita fusão de dados, e Oliveira *et al.* [12] propuseram LHA-SP, um conjunto de protocolos de segurança para RSSFs hierárquicas com número arbitrário de níveis.

Alternativamente, existem trabalhos que empregaram ROs em redes tradicionais visando o aumento da segurança [13, 14]. Entretanto, tais trabalhos não levam em conta as restrições de recursos dos nós sensores e não são aplicáveis às RSSFs.

3. ROs sobre RSSFs

Neste trabalho a RO é constituída apenas pelos CHs, deixando aos demais nós, em geral de menor poder energético e computacional, apenas o encargo de sensoriar a rede.

Cada nó da rede *overlay* possui um grupo de vizinhos, que podem ser utilizados como intermediários em rotas alternativas à rota padrão – aquela determinada pelo protocolo de roteamento.

Em nossa proposta, existem duas classes de mensagens: as prioritárias e as não prioritárias. Utiliza-se as mensagens não prioritárias como forma de angariar informações da rede. Entende-se por mensagens não prioritárias aquelas que, caso sejam perdidas, não representam grandes danos ao funcionamento da rede.

Mais precisamente, os nós *overlay* enviam periodicamente mensagens não prioritárias à ERB. Essas mensagens ora são enviadas pela rota padrão, ora por rotas alternativas por intermédio de vizinhos *overlay* do nó remetente. A ERB mantém um registro das últimas n mensagens recebidas. Como a granularidade do envio de mensagens é conhecida, a ERB pode então inferir sobre o nível de segurança das rotas com base na taxa de chegada de mensagens. Sempre que houver mudança deste nível em uma rota, a ERB dissemina esta informação à RO, de forma que mensagens prioritárias são sempre enviadas pelas rotas mais seguras.

4. Experimentos

Em nosso modelo a ERB têm potência suficiente para alcançar todos os nós da rede e, desta forma, pode transmitir informações diretamente para cada um dos CHs sobre a melhor rota num determinado momento.

Dois tipos de ataques foram simulados, *blackhole* e *selective forwarding*. No primeiro ataque o nó malicioso simplesmente some com toda e qualquer mensagem enviada a ele. No segundo, *selective forwarding*, o nó não repassa apenas algumas mensagens. O segundo tipo de ataque é mais difícil de detectar que o primeiro, pois pode facilmente ser confundido com falhas normais do funcionamento da rede.

Os experimentos foram realizados utilizando-se o simulador NS (*Network Simulator*). A simulação foi baseada em uma rede com 100 nós, 10 deles CHs, dispostos em um área de $100m \times 100m$. Tanto o modelo de eleição de CHs quanto o modelo de energia são os mesmos apresentados por Heinzelman *et al.* [6]. O resultados apresentados são uma média de 33 execuções de cada cenário simulado, sendo que cada execução alimentou o gerador de números aleatórios do simulador com uma semente distinta das demais.

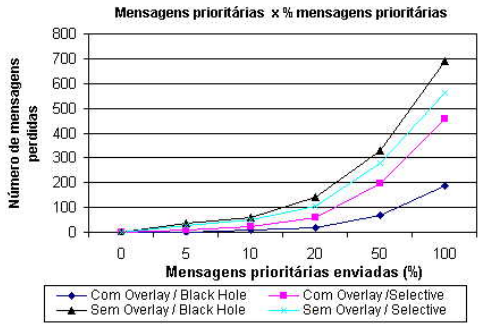

Figura 1: Msgs prioritárias: perdidas vs enviadas

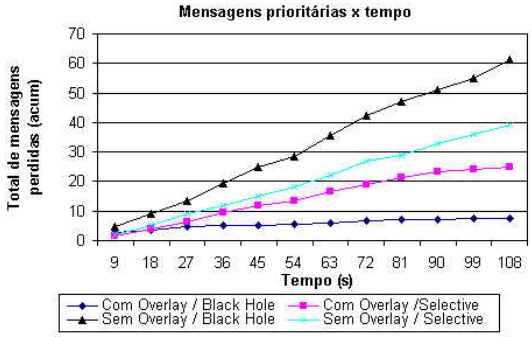

Figura 2: Msgs prioritárias perdidas vs tempo

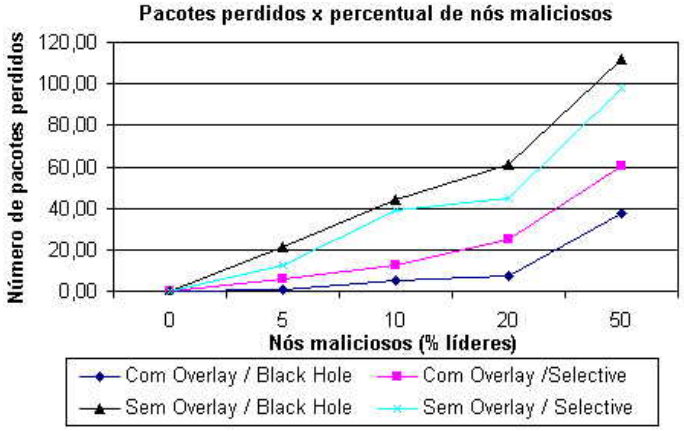

Figura 3: Msgs prioritárias perdidas vs nós maliciosos

A Fig. 1 apresenta o número de mensagens prioritárias perdidas em função do percentual de mensagens prioritárias enviadas. Como esperado, com o aumento do número de mensagens prioritárias ocorre também um aumento no número de mensagens prioritárias perdidas. Contudo a utilização das ROs aumentou o número de mensagens prioritárias entregues consideravelmente. Mesmo quando temos 100% de mensagens prioritárias, e mensagens prioritárias precisam ser utilizadas para testar as rotas, a utilização de ROs aumentou a taxa de entrega em 5,16% em ataques de *selective forwarding* e em 25,21% em ataques de *blackhole*. Com 5% de mensagens prioritários a melhoria foi de 18,6% e 35,9%, respectivamente.

A Fig. 2 apresenta o acumulado de mensagens perdidas durante o tempo de simulação. Verifica-se que as redes sem a utilização de ROs apresentam um crescimento contínuo no número de mensagens perdidas. Os experimentos utilizando ROs crescem até começarem a conhecer a rede. A partir daí, apresentam um crescimento menor da curva. Isto ocorre por que é necessário um tempo para que o conhecimento dos nós comprometidos seja efetivado. Podemos ainda observar que no caso do ataque *selective forwarding*, há um maior tempo para a curva se estabilizar. Acreditamos que com o aumento do tempo de simulação isto fique ainda mais evidente.

A Fig. 3 apresenta a perda de mensagens prioritárias em função do percentual de CHs comprometidos na rede. Novamente as ROs apresentaram um ganho significativo em termos de mensagens prioritárias recebidas no destino. Observe que este ganho se manteve mesmo em condições extremas, em que 50% dos CHs são compostos por nós maliciosos.

Uma vez evidentes os benefícios da solução, discutiremos o custo da mesma. Já que em ambos os cenários a densidade da rede é a mesma, e por sua vez a distância entre os nós também o é, o gasto de energia pode ser dado em função do tamanho médio do caminho até a ERB (isto é, número de *hops* médio). Com o emprego de ROs, o caminho médio que era de 3,9 aumentou para 4,5 em média (15% de *overhead*, aproximadamente). Tal resultado era esperado uma vez que a rota mais segura nem sempre é a menor.

5. Conclusão e Trabalhos Futuros

Neste trabalho avaliamos o uso de ROs para segurança em Redes de Sensores Sem Fio (RSSF). Os resultados preliminares indicam que o caminho é de fato promissor, sendo um indicador desta premissa, por exemplo, o aumento significativo no número de mensagens prioritárias entregues.

Dentre as diversas extensões deste trabalho, destacam-se:

- Implementação de outros ataques: caracterizar o comportamento das ROs com relação a outros tipos ataques ou quando mais de um ocorre simultaneamente;
- Ataques localizados: neste trabalho, os atacantes são distribuídos de forma aleatória pela rede. Pretende-se avaliar cenários em que ataques são concentrados em uma parte específica da rede, por exemplo próximo a ERB, ou visando particionar a rede;
- Utilização das ROs em outros tipos de rede: atualmente estamos trabalhando apenas com redes hierárquicas, mas é interessante avaliar a viabilidade da solução em outros tipos de rede.

Referências

[1] Deborah Estrin, Ramesh Govindan, John S. Heidemann, and Satish Kumar. Next century challenges: Scalable coordination in sensor networks. In *Mobile Computing and Networking*, pages 263–270, Seattle, WA USA, 1999.

[2] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, 35(10):54–62, October 2002.

[3] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3):293–315, September 2003.

[4] David Andersen, Hari Balakrishnan, Frans Kaashoek, and Robert Morris. Resilient Overlay Networks. In *The 8th ACM Symposium on Operating Systems Principles (SOSP'01)*, pages 131–145, Banff, CA, Oct. 2001.

[5] Enrique J. Duarte Melo and Mingyan Liu. The effect of organization on energy consumption in wireless sensor networks. In *IEEE Globecom 2002*, November 2002.

[6] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *IEEE Hawaii Int. Conf. on System Sciences*, pages 4–7, january 2000.

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534, September 2002.

[8] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for large-scale distributed sensor networks. In *Proceedings of the 10th ACM conference on Computer and communication security*, pages 62–72. ACM Press, 2003.

[9] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. Adaptive Security for Multi-layer Ad-hoc Networks. *Wireless Communications and Mobile Computing, Wiley Interscience Press*, 2(5):533–547, 2002. Special Issue.

[10] M. Bohge and W. Trappe. An authentication framework for hierarchical ad hoc sensor networks. In *Proceedings of the 2003 ACM workshop on Wireless security*, pages 79–87. ACM Press, 2003.

[11] A. C. Ferreira, M. A. Vilaça, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro. On the security of cluster-based communication protocols for wireless sensor networks. In *4th IEEE International Conference on Networking (ICN'05)*, volume 3420 of *Lecture Notes in Computer Science*, pages 449–458, Reunion Island, April 2005. Springer.

[12] Leonardo B. Oliveira, Hao Chi Wong, and Antonio A. F. Loureiro. Lha-sp: Secure protocols for hierarchical wireless sensor networks. In *9th IFIP/IEEE International Symposium on Integrated Network Management (IM'05)*, pages 31–44, Nice, France, May 2005.

[13] A. Keromytis, V. Misra, and D. Rubenstein. Sos: An architecture for mitigating ddos attacks. *IEEE Journal on Selected Areas of Communications (JSAC)*, 33(3):413–426, 2004. Special issue on Service Overlay Networks.

[14] Jun Li, Peter L. Reiher, and Gerald J. Popek. Resilient Self-Organizing Overlay Networks for Security Update Delivery. *IEEE Journal on Selected Areas in Communications*, 22(1):189–204, Jan. 2004.