# Implementação de uma rede mesh segura utilizando o protocolo SOLSR aplicada a Smart Grids

**Alexandre S. Rodrigues[1], Tiago A. Rizzetti[2]**

1. Estudante de IC da Universidade Federal de Santa Maria - UFSM; *alexandre.rodrigues@redes.ufsm.br
2. Professor do CST em Redes de Computadores, Universidade Federal de Santa Maria - UFSM, Santa Maria/RS

Palavras Chave: *Redes mesh, protocolo SOLSR, Smart Grids.*

## Introdução

As redes elétricas inteligentes (*Smart Grid*) destacam-se por utilizarem as tecnologias da informação para facilitar a administração e gerenciamento da rede elétrica convencional, possibilitando a diferenciação nas tarifas em determinados horários e a auto recuperação do sistema em casos de falhas. Para prover essas funcionalidades, é necessário que os equipamentos ativos na rede elétrica troquem informações em tempo real [1].

Nesse contexto, as informações de diversos clientes são coletadas por concentradores. Esses podem estar localizados em pontos geográficos distantes e de difícil acesso. Prover essa comunicação de forma segura é um grande desafio. Além disso, a rede utilizada nessa comunicação requer um elevado índice de disponibilidade, devido à necessidade de comunicação em tempo real entre os equipamentos.

O presente trabalho tem como objetivo apresentar uma proposta para tornar essa comunicação viável, através da utilização de uma rede mesh segura.

Uma rede mesh pode ser vista como diversos dispositivos interligados (nós), onde todos são capazes de atuar como roteadores e se adequar automaticamente a topologia da rede.

Entre os protocolos de roteamento mais utilizados em redes mesh destaca-se o protocolo OLSR (*Optimized Link State Routing*), que utiliza o estado de enlace para selecionar qual melhor rota para transmitir um pacote. Para realizar a atualização de suas rotas e vizinhos, esse protocolo utiliza mensagens de controle que são enviadas em *broadcast* [2]. Dessa forma, é necessário impedir que dispositivos não autorizados possam inserir essas mensagens na rede e modificar as informações sobre a topologia da mesma.

O protocolo SOLSR (*Secure* OLSR) é uma extensão do protocolo OLSR, que utiliza uma chave simétrica de 128 bits para assinar todas as mensagens de controle antes de enviá-las em broadcast. Ao receber uma mensagem, um nó verifica se a assinatura é válida, ou seja, se o seu remente é um nó autorizado a estar na rede [3].

## Resultados e Discussão

Para verificar a eficiência do protocolo SOLSR, foi desenvolvido um cenário de testes, utilizando dispositivos com placa de comunicação sem fio, onde um nó representa um concentrador de dados e dois nós representam os dispositivos instalados na residência dos clientes, conforme pode ser visualizado na Figura 1. Os dispositivos autorizados utilizam a mesma chave para assinar as mensagens. Em relação aos falsos nós que tentarão obter acesso a rede, um terá uma chave incorreta e o outro não assinará as mensagens.

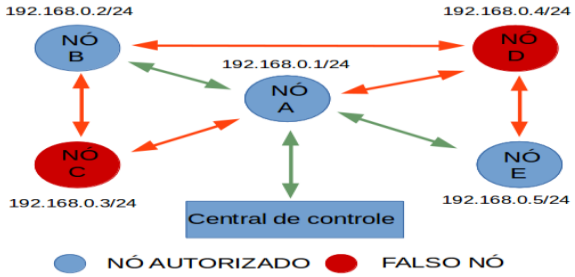


**Figura 1.** Cenário de testes.

Após a inicialização de todos os dispositivos, verificou-se a interação entre os nós autorizados, conforme pode ser visualizado na Figura 2 que apresenta a tabela de roteamento do nó A.

```
      *** olsr.org - 0.6.8-git_0000000-hash_f90f6d7f8b957fff3eea9cf8ba30a665 (2
015-06-17 17:49:32 on alexandre-note) ***

--- 18:27:54.438184 ------------------------------------------------- LINKS

IP address       hyst         LQ       ETX
192.168.0.5      0.000  1.000/0.854    1.169
192.168.0.2      0.000  1.000/1.000    1.000

--- 18:27:54.438205 ---------------------------------------------- NEIGHBORS

    IP address Hyst    LQ      ETX     SYM   MPR   MPRS  will
192.168.0.5     0.000   1.000/0.854     1.169   YES   NO    NO    3
192.168.0.2     0.000   1.000/1.000     1.000   YES   NO    NO    3

--- 18:27:54.438225 ---------------------- TWO-HOP NEIGHBORS

IP addr (2-hop)  IP addr (1-hop)  Total cost
192.168.0.5      192.168.0.2      2.128
192.168.0.2      192.168.0.5      2.528
```

**Figura 2.** Tabela de roteamento do nó A.

As mensagens de controle enviadas pelos falsos nós, foram descartas, conforme pode ser visualizado na Figura 3. Dessa forma, eles não conseguiram ingressar na rede.

```
Recevied hash:
 158  44  37 207 250  18  64 124 241  12 215  25  28 226  93  48
Calculated hash:
 244  81 147 243 221  39  93 217 254   0 159 166 230 171  91 164
[ENC]Signature missmatch
[ENC]Rejecting packet from 192.168.0.3
```

**Figura 3.** Pacotes descartados.

## Conclusões

Com base nos resultados obtidos, o protocolo SOLSR impossibilita que dispositivos não autorizados ingressem na rede. Portanto, a principal contribuição deste trabalho é provar que uma rede mesh pode fornecer uma comunicação segura e pode ser utilizada na implementação de um Smart Grid.

[1] WANG, W. et al. **A survey on the communication architectures in smart grid**. Computer Networks, v. 55, n. 15, p. 3604-3629, 2011.

[2] CLAUSEN, T.; JAQCQUET, P. **Optimized link state routing (OLSR) RFC 3626**. IETF Networking Group. 2003.

[3] HAFSLUND, A. et al. **Secure Extension to the OLSR protocol**. In: Proceedings of the OLSR Interop and Workshop, San Diego, 2004.