Novas Tecnologias de Comunicação para Smart Grids: Uma abordagem utilizando o 6LowPAN

Bolívar M. Silva[1], Pedro Wessel[1], Tiago A. Rizzetti[1]

[1]Colégio Técnico Industrial de Santa Maria – Universidade Federal de Santa Maria (UFSM)
Av. Roraima n^0 1000 – 97.105-900 – Santa Maria – RS – Brasil

{bolivar,pedrowessel}@redes.ufsm.br, rizzetti@ctism.ufsm.br

Abstract. *This article describes the use of various technologies, encompassing the concept of Internet of things and smart grids. Sensor networks are increasingly common amid the constant technological developments in which we live. In this context, the article focuses on the use of wireless sensor networks using 6LoWPAN as a means of communication to exchange messages and information.*

Resumo. *Este artigo descreve a utilização de várias tecnologias, englobando o conceito de internet das coisas e Smart Grids. As redes de sensoriamento são cada vez mais comuns em meio as evoluções tecnológicas constantes em que vivemos. Nesse contexto, o artigo foca na utilização de redes sensores sem fio, utilizando 6LoWPAN como meio para realizar a troca de mensagens e informações.*

1. Introdução

Nos últimos anos, o conceito de Internet das Coisas (*Internet of Things - IoT*) vem sendo aplicado cada vez mais ao nosso dia a dia. Nesse contexto, podemos destacar o crescimento da utilização de redes inteligentes, denominadas Smart Grids, mais especificamente no que diz respeito a redes elétricas inteligentes [Shelby and Bormann, 2009].

Redes elétricas inteligentes são redes dotadas de sensores capazes de fornecer informações em tempo real. Nesse contexto a geração, transmissão e consumo de energia, são monitorados por um conjunto de sensores que possibilitam reconhecer, de forma precisa, informações relativas aos parâmetros elétricos do sistema. Desta forma possibilitando seu gerenciamento através de sistemas que poderão atuar resolvendo problemas rapidamente, de forma automática. Até mesmo será possível a atuação preventiva, minimizando a ocorrência. Assim contribuindo para aumentar a disponibilidade do sistema. [CGEE, 2012].

Pensando em aplicações onde é imprescindível uma rede com grande capacidade de endereçamento, baixo consumo de energia e que atenda a demanda de tecnologia necessária para aplicações, um grupo de desenvolvedores denominado 6LoWPAN (*IPv6 over Low power Wireless Personal Area Network*) foi criado. Esse grupo tem como principal objetivo tornar possível a utilização do protocolo IPv6 em redes padrão

IEEE 802.15.4, as quais são caracterizadas pelo uso de dispositivos de baixo poder de processamento e baixo consumo de energia.

Nesse contexto, este artigo visa descrever o uso de 6LoWPAN para comunicação em redes de sensores sem fio (*Wireless Sensor Network - WSN*), abordando alguns aspectos como: vulnerabilidades, segurança, compressão do cabeçalho IPv6 e modo de endereçamento.

2. Internet das Coisas

A Internet das Coisas (*Internet of Things - IoT*) consiste na interligação de objetos heterogêneos localizados em diferentes lugares, utilizando protocolos que são padrões da Internet. A ideia é criar ambientes autônomos usando objetos com a capacidade de trocar informações e tomar decisões. Sensores e atuadores conectados poderão dar aos usuários a possibilidade de monitoramento e rastreamento de qualquer objeto remotamente e em tempo real. Muitas aplicações do nosso dia a dia poderão se beneficiar deste conceito como: saúde, transporte, meio ambiente, gestão de cidades, entre outras [Shelby and Bormann, 2009], [Atzori et al., 2010]. Para possibilitar esse amplo emprego de dispositivos de comunicação faz-se necessário a utilização de tecnologias de redes que permitam um endereçamento abrangente, escalável e amplamente testado.

3. Tecnologias de Comunicação Emergentes

Para a comunicação em redes *Smart Grid* é essencial uma forma confiável, resiliente e segura, de troca de informações. Por conta do acelerado crescimento característico desse tipo de rede, os novos dispositivos incorporados não devem afetar sua confiabilidade e disponibilidade.

As tecnologias empregadas em *Smart Grid* devem ser capazes de prover escalabilidade a rede, possibilitando que todos os dispositivos possam ter um endereço IP público. Nesse contexto, a utilização do protocolo IPv6 surge como uma alternativa, para manter a compatibilidade e acessibilidade, dos dispositivos na rede.

3.1. IPv6

O protocolo IPv6, uma evolução do amplamente utilizado protocolo IPv4, possui 128 bits para endereçamento, que possibilitam o endereçamento de aproximadamente 340 undecilhões endereços públicos na Internet. Considerando que a menor rede recomendada aos usuários finais é uma rede com máscara /64 tem-se um número de endereços maior do que todo o espaço de endereçamento da rede IPv4 mundial, que é de aproximadamente 4,3 bilhões [Bucke and Brito, 2013].

Para a implementação de redes elétricas inteligentes, é necessário uma forma de endereçar um grande número de dispositivos. Desse modo, foi desenvolvida uma tecnologia que permite a utilização do protocolo IPv6 em redes de sensores, com baixo poder de processamento, denominada 6LoWPAN.

3.2. 6LoWPAN em Redes Elétricas Inteligentes

6LoWPAN é um grupo criado pela IETF (*Internet Engineering Task Force*), responsável por criar e manter as especificações de conexão, transferência de arquivos e as demais regras que permitem o uso de IPv6 em redes do padrão IEEE 802.15.4.

O padrão IEEE 802.15.4 especifica a camada física e oferece os fundamentos de implementação de uma rede de área pessoal sem fio (WPAN), que objetiva fornecer um modelo de transferência de dados confiável, baixo consumo de energia e de fácil instalação. Os dispositivos 6LoWPAN trabalham utilizando esse padrão, dada suas necessidades e características.

O 6LoWPAN possibilita que pacotes IPv6 sejam transportados sobre redes sem fio de baixo consumo de energia. O mesmo pode se beneficiar da infraestrutura já existente de redes TCP/IP, por utilizar o mesmo padrão, ou seja, podem prover a interoperabilidade, além de uma maior facilidade de configuração [Montenegro et al., 2007].

A possibilidade de operar com baixo consumo de energia é um dos fatores que caracteriza as redes 6LoWPAN, sendo essa, uma das principais vantagens da utilização dessa tecnologia. Uma das formas que colabora para a redução do consumo de energia é diminuir o processamento do dispositivo, através da compressão do cabeçalho IPv6.

3.3. Compressão do Cabeçalho IPv6

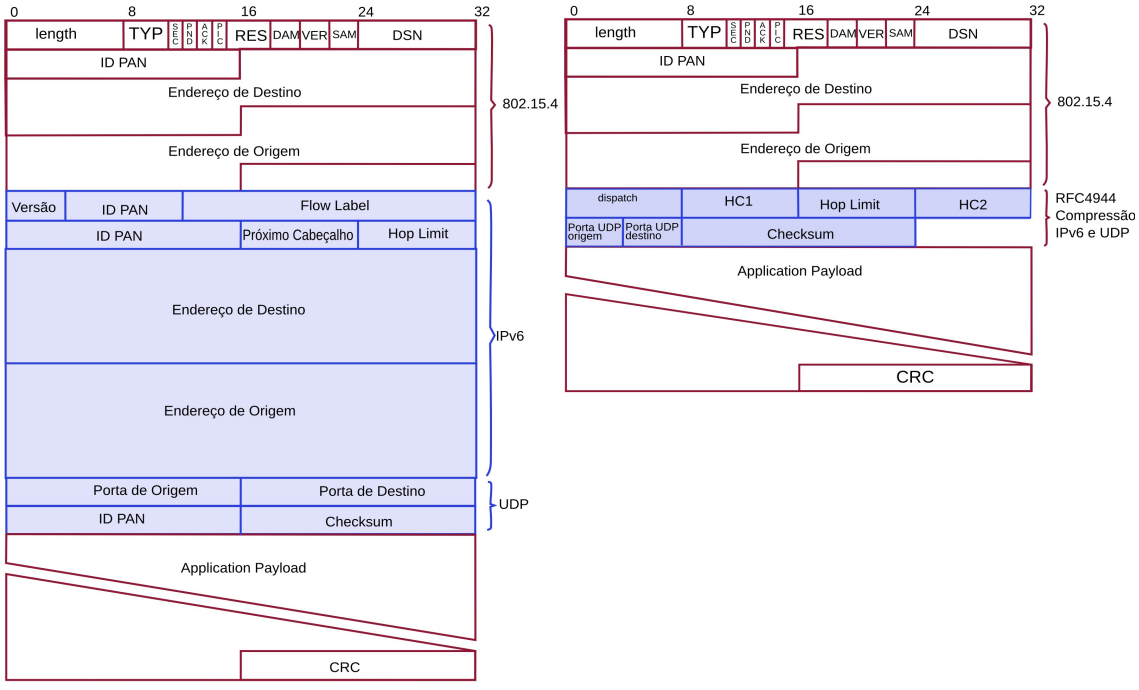

Figura 1: Compressão do cabeçalho IPv6

Fonte: http://wiki.sj.ifsc.edu.br/wiki/index.php/Equipe-2-2014-1-RCO3

LOWPAN_IPHC é uma codificação, definida na RFC 4944 que tem como objetivo fazer a compressão do cabeçalho IPv6 para que possam ser transmitidos em redes padrão IEEE 802.15.4. Essa codificação utiliza 13 bits, dos quais 5 bits estão localizados mais a direita, responsáveis por informar o tipo de envio. Além disso, essa

codificação poderá utilizar mais um octeto, se necessário [Montenegro et al., 2007].

Em uma rede local de sensores, no melhor dos casos, a codificação LOWPAN_IPHC consegue comprimir um cabeçalho até o tamanho de dois octetos, sendo que um octeto ficará para a codificação e o outro para envio de dados. Já quando encaminhado para links externos, ou seja, em casos onde o pacote terá que sair da rede local, o menor tamanho de cabeçalho IPv6 possível será de 7 octetos, sendo que 1 octeto será para expedição, 1 octeto para LOWPAN_IPHC, 1 octeto para *Hop Limit* (número máximo de saltos), 2 octetos para endereço de origem e 2 octetos para endereço de destino. É importante salientar que o octeto utilizado para contar o número de saltos, não poderá ser compactado, o mesmo precisa ser decrementado a cada salto [Montenegro et al., 2007].

A Figura 1, ilustra a compressão de um pacote IPv6, feita através da codificação LOWPAN_IPHC. Conforme podemos observar, ao lado esquerdo, as partes destacadas em azul correspondem ao cabeçalho IPv6 e o UDP. Ao lado direito, está a imagem que ilustra o cabeçalho IPv6 reduzido.

3.4. Modo de endereçamento

Segundo o padrão IEEE 802.15.4, o endereçamento pode ser de 16 bits (curto) ou 64 bits (estendido). Dentro de redes PAN, normalmente são utilizados endereços curtos de 16 bits, porém, segundo a RFC 4449, algumas restrições adicionais são impostas para redes 6LoWPAN, além das já impostas pela IEEE 802.15.4. Essas restrições foram atribuídas pensando na escalabilidade da rede, uma vez que um endereço curto de 16 bits é relacionado com cada dispositivo, através de um coordenador, responsável pela atribuição dos endereços IPs. Problemas como possíveis defeitos nesse coordenador ou mesmo o fim do tempo de vida de um endereço IP, ou ainda, simplesmente qualquer acidente que possa ocorrer com o coordenador, colocará em risco o funcionamento de toda a rede.

Existem pontos positivos e negativos em cada uma das formas de endereçamento. No endereçamento de 16 bits, existe o problema de centralização. A forma de endereçamento estendida (64 bits) não necessita de um controle centralizado para atribuições de endereços, porém precisará de maior processamento [Montenegro et al., 2007].

3.5. Segurança

A preocupação com a segurança é um fator importante, independente do tipo de rede, ainda mais em situações onde a integridade e autenticidade dos pacotes são de vital importância, que é o caso de redes elétricas inteligentes. Decisões tomadas baseadas em dados alterados, poderiam ocasionar em sérios problemas a equipamentos e até mesmo, colocar em risco a vida de pessoas [Le et al., 2012].

Uma das formas de aumentar a segurança e a confidencialidade dos dados de uma rede é a utilização de criptografia. Em redes 6LoWPAN, existem algumas limitações provenientes do baixo poder de processamento característico dos dispositivos empregados nesse tipo de rede, sendo assim, formas de criptografias muito complexas não poderiam ser implementadas [Le et al., 2012].

As WSN utilizam criptografia AES (*Advanced Encryption Standard*), para a camada de enlace de dados. Essa criptografia é um método, que utilizada uma chave simétrica, para cifrar uma mensagem escrita em texto plano. A mesma não exige grande poder de processamento e oferece uma proteção considerável contra ataques de força bruta [Stallings, 2008].

Outra forma de garantir a segurança, em uma rede de sensores, é utilizando o protocolo IPsec (*IP Security Protocol*). Esse pode ser visto como uma suíte de protocolos, que atuam na camada de rede do modelo de referência OSI, provendo a capacidade de tunelamento, criptografia e autenticação dos dados trafegados [RFC 6071, 2011]. No caso de redes que utilizam 6LoWPAN, o IPsec precisa sofrer algumas alterações, visando se adaptar as restrições.

A camada PHY (camada Física) é uma interface entre a subcamada MAC e o canal de rádio, responsável pela transmissão e recepção de bits, que compõem a PPDU (PHY Protocol Data Unit). Essa camada não oferece nenhuma forma de segurança baseada em criptografia.

3.6. Vulnerabilidades

Tanto em WSN, quanto no próprio protocolo IPv6 existem falhas de segurança, além disso existem vulnerabilidades na camada de adaptação, que é a camada de tradução de pacotes, a qual permite o uso de endereçamento IPv6, com cabeçalho modificado.

As ameaças em redes elétricas inteligentes podem ser voltadas para derrubar a rede, tentativas de roubo de serviços elétricos ou tentativas de comprometer a confidencialidade dos dados do sistema. Quanto à confidencialidade, podemos citar um ataque onde o usuário mal intencionado tenta capturar informações, modificá-las e enviar para outro dispositivo. Para mitigar esse tipo de ameaça, é importante a utilização de mecanismos que garantam a autenticidade do emissor e receptor de uma comunicação. Além disso, a criptografia das mensagens pode garantir que terceiros não acessem as informações que trafegam nessa rede [Le et al., 2012].

O ataque de negação de serviço (*Denial of Service* – DoS) é um exemplo de ataque comum em redes, e é realizado através do envio de um fluxo constante de requisições a um serviço, com objetivo de comprometer seu funcionamento. Esse ataque quando realizado em páginas Web, pode acarretar na indisponibilidade do serviço, resultando em prejuízos financeiros para a empresa. Contudo quando realizado em uma rede de sensores, que controla um sistema de distribuição de energia seria de alto risco, pois comprometeria o funcionamento da mesma, danificando equipamentos como, por exemplo, a explosão de um transformador, além de por em risco a vida de pessoas [Aloul et al. 2012].

Um atacante também pode utilizar os sensores para modificar e transmitir informações alteradas, e ainda usá-los para injetar softwares maliciosos na rede [Shi and Perrig, 2004].

4. Conclusões

Redes inteligentes é inegavelmente uma tendência, não só para redes inteligentes de

energia como também para outras áreas, como redes de distribuição de água, gás, entre outras. Porém para ser possível o desenvolvimento dessas redes, é imprescindível uma rede de sensores capaz de prover uma coleta de dados do ambiente de maneira satisfatória, confiável e escalável.

As redes WPANs que utilizam as especificações 6LoWPAN, possuem as características necessárias para que as redes inteligentes possam ser implementadas e popularizadas, mesmo em ambientes de difícil acesso para a instalação e/ou manutenção dos dispositivos da rede. Outra característica, talvez a mais interessante, é a compatibilidade com o protocolo IPv6, que nos permite um número de endereçamento muito grande, fazendo com que esse não seja mais um obstáculo na criação de *Smart Grid.*

5. Referências

Aloul, F., Al-ali, A. R., Al-dalky, R. and Al-mardini, M. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. *Smart Grid and Clean Energy Smart.*

Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, v. 54, p. 2787–2805.

Bucke B. and Samuel H. (2013). O Novo Protocolo da Internet. 1ª edição.

Centro de Gestão e Estudos Estratégicos (2012). Redes Elétricas Inteligentes: contexto nacional. 16ª edição.

D. Whiting, G., R. Housley, N., N. Ferguson, D. (2003). Counter with CBC-MAC (CCM). *RFC*. https://www.ietf.org/rfc/rfc3610.txt

Frankel, S. and Krishnan, S. (2011). IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap. RFC. http://tools.ietf.org/html/rfc6071.

Hinden, R. and Deering, S. (2003). Internet Protocol Version 6 (IPv6) Addressing Architecture. Request for Comments

Kavitha, T. and Sridharan, D. (2010). Security Vulnerabilities in Wireless Sensor Networks: A Survey. *Journal of Information Assurance and Security*, v. 5, p. 31–44.

Le, A., Loo, J., Lasebae, A., Aiash, M. and Luo, Y. (2012). 6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach. *International Journal of Communication Systems*, v. 25, p. 1189–1212.

Montenegro, G., Kushalnagar, N., Hui, J. and Culler, D. (2007). Transmission of IPv6 Packets over IEEE 802.15.4 Networks. *RFC*. http://www.ietf.org/rfc/rfc4944.txt.

Shelby, Z. and Bormann, C. (2009). *6LoWPAN: The Wireless Embedded Internet*. p. 1–223

Shi, E. and Perrig, A. (2004). Designing secure sensor networks. *IEEE Wireless Communications*, v. 11, p. 38–43.

Stallings, W., (2008). Criptografia e segurança de redes, 4ª edição. São Paulo: Pearson.

Tanenbaum, A. S. (2003). Redes de computadores Quarta edição. *Editora Campus*, v. 18, p. 1–632.