ANÁLISE COMPARATIVA SOBRE SEGURANÇA DE PROTOCOLOS VOLTADOS À SMART GRIDS

André R. Eichner[1], Ricardo C. Branco[1], Lucas V. Dias[1], Tiago A. Rizzetti[1]

[1]Curso Superior de Técnologia em Redes de Computadores
Colétio Técnico Industrial de Santa Maria – CTISM
Universidade Federal de Santa Maria – UFSM
Caixa Postal 97.105 - 900 – Santa Maria – RS – Brazil

{eichner, branco, lucas_dias}@redes.ufsm.br, rizzetti@ctism.ufsm.br

Abstract. *In the context of smart grids, the advanced metering infrastructure are systems that integrate smart meters, communication networks and data management systems, allowing communication between the generator, distributor and home network. security is essential in any communication network, whereas this paper does a survey of the vulnerabilities found in two of the main communication protocols used in smart grids, in order to minimize the risks attack on these networks.*

Resumo. *No contexto de redes elétricas inteligentes, infraestruturas de medição avançada são sistemas que integram os medidores inteligentes, redes de comunicação e sistemas de gerenciamento de dados, permitindo uma comunicação bidirecional entre a geradora, distribuidora e rede cliente. A segurança é essencial em qualquer rede de comunicação de dados, ao passo que este trabalho faz um levantamento das vulnerabilidades encontradas em dois dos principais protocolos de comunicação utilizados em redes elétricas inteligentes, a fim de minimizar os riscos de ataques nestas redes.*

1. Introdução

Advanced Metering Infrastructure (AMI) é um modelo de Redes Elétricas Inteligentes (REI), que vem reduzindo as vulnerabilidades de ataques externos, trabalhando com coletor, medidor, analisador dos dados de uso da energia da rede [Wang and Leung 2011]. Uma AMI é responsável por transmitir estes dados para os concentradores de dados e para os sistemas centrais no lado da concessionária [Faisal et al. 2012].

Na literatura, a geração de energia elétrica não cabe apenas a concessionária, pois nesta visão de geração de energia de maneira distribuída, os clientes possuem um papel de suma importância, tanto na geração quanto na distribuição e realocação de recursos. O fluxo da energia elétrica não fica restrito apenas da distribuidora para o cliente, mas também o cliente pode ofertar a energia elétrica gerada por ele à rede da distribuidora. O que torna isso possível é a instalação de *Smart Meters*, ou Medidores Inteligente (MI), no lado do cliente, onde este é capaz de medir o fluxo bidirecional da energia elétrica, entre outras funções, como desligamento e religamento de forma remota e balanceamento de carga [Falcão 2009].

Toda informação que trafega em uma REI, leva consigo dados que comprometem diretamente o cliente. Com as REI crescendo gradativamente nos últimos tempos, não

teve-se um longo período de avaliação dos riscos, mas sabe-se que com a interceptação destes dados é possível saber os horários em que o usuário encontra-se em sua residência, potencializando assim o roubo de energia ou até mesmo praticar um atentado diretamente ao consumidor final. Os MIs mostram quase em tempo real o consumo e a geração de energia elétrica, tanto ao usuário quanto à distribuidora. Os dados gerados pelos MIs são enviados através de sistemas de supervisão e aquisição de dados (SCADA), localizados muitas vezes na concessionária. Estes são transmitidos através da rede de comunicação de dados hierárquica AMI, esboçada na Figura 1.

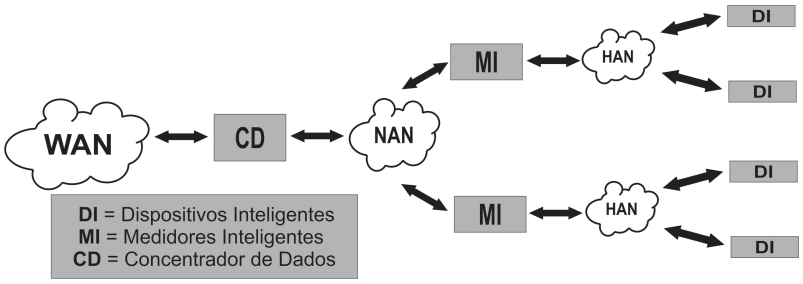

Figura 1. Estrutura de uma AMI. FONTE: Autor.

O primeiro nível de hierarquia da rede, é a HAN (*Home Area Network*), neste nível se encontram os MI, que armazenam os dados das *microgrids* no domínio do usuário final. As informações geradas por um conjunto de MI são enviados à um concentrador do nível NAN (*Neighborhood Area Network*). Por fim, os dados são enviados à um concentrador de dados que está conectado na central de gerenciamento de medição, formando o nível WAN (*Wide Area Network*)[Yu et al. 2011].

Com estes dados em mãos, a concessionária tem um levantamento histórico de quais regiões da sua rede está consumindo mais ou menos energia em todos os horários do dia, podendo assim planejar um balanceamento de carga na rede e redirecionar mais ou menos energia para certos pontos da rede, evitando apagões – como o ocorrido em 2003 nos Estados Unidos (EUA), no qual, aproximadamente 50 milhões de pessoas foram afetadas pelo que foi considerado o segundo maior apagão da história [Yang et al. 2006].

A fim de minimizar ao máximo os riscos de uma possível invasão, sequestro de informações ou danos ao cliente, foram sendo criados novos protocolos voltados às REI. Neste artigo são apresentados dois destes protocolos, o *Distributed Network Protocol version 3* (DNP3), que é um protocolo de código aberto otimizado para utilização em sistemas de supervisão e aquisição de dados (SCADA), e o padrão ANSI C12.22, sendo este, uma especificação de camada de aplicação para permitir o transporte de dados de medidores, através de uma conexão em rede.

Em função da criticidade e serviços oferecidos através das REI, depara-se com conceitos fundamentais no âmbito de redes de computadores, que são elas, a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irretratabilidade das informações e segurança dos dados que trafegam na rede. Onde são exploradas formas à maximizar a segurança e reduzir os riscos de interceptação destes dados, seja para fins de leitura, interpretação ou modificação os dados, a fim de prejudicar o cliente final.

2. Padrões de troca de dados para AMI

A seguir são apresentados dois protocolos escolhidos para análise de vulnerabilidades, o protocolo DNP3 e o padrão ANSI C12.22.

2.1. ANSI C12.22/IEEE Std 1703

O padrão ANSI C12.22/IEEE Std.1703 é um protocolo de comunicação que especifica o transporte de tabelas ANSI C12.19 pela REI. Especificando uma interface para redes de comunicação de dados e fornece interoperabilidade entre medidores e módulos de comunicação [Darwish et al. 2015]. Como os MI estão sujeitos a ataques físicos, para extração de informações, a robustez das especificações é necessária para a implementação de uma rede segura. O padrão define os formatos de mensagens e protocolos de comunicação na camada de aplicação usado em qualquer segmento da rede. A mensagem é transportada utilizando protocolos TCP ou UDP em redes IP [Wang and Leung 2011].

Para realizar login na rede, basta informar os campos ”*user*”, ”*user_id*”e também definir o tempo de conexão. Porém, se um atacante obtiver êxito na conexão e setar um tempo de conexão relativamente alto, o usuário legítimo não terá acesso a rede de comunicação de dados até que a conexão do atacante expire, pois a plataforma não deve tratar de múltiplas conexões simultâneas. Em contrapartida, se o atacante setar o *timeout* como zero, a mesma permanecerá ativa por tempo indeterminado ou até que o atacante perca o contato com a rede de dados[ANSI 2018]. A Figura 2 mostra o formato de login do protocolo.

<logon>	::=	50_H <user-id> <user> <req-session-idle-timeout>	
<user-id>	::=	<word16>	{User identification code}
<user>	::=	<byte>^{*10}	{10 bytes containing user identification}
<req-session-idle-timeout>	::=	<word16>	{The desired number of seconds a session may be idle on the C12.22 Server side before the C12.22 Server may terminate the session. A value of zero means a request to keep the session open forever.}

Figura 2. Frame *login*. FONTE: [ANSI 2018]

2.2. Distributed Network Protocol version 3 - DNP3

DNP3 é um protocolo aberto, não proprietário e otimizado para redes de aplicações SCADA (Supervisory Control and Data Acquisition) fisicamente separados, também sendo usado em AMI [Jin et al. 2011] [Mohagheghi et al. 2009]. Projetado para atuar no modelo de redes EPA (*Enhanced Performance Architeture*), que possui apenas três camadas (Física, Enlace e Aplicação)[Bagaria et al. 2011], que é uma variação simplificada do modelo de redes OSI (*Open System Interconnection*).

O principal objetivo deste protocolo, é realizar a transmissão dos pacotes de forma segura. A fragmentação destas mensagens em porções menores, representa uma maior segurança envolvida, uma vez que tem-se a adição de verificação de redundância cíclica (CRC) em cada fragmento, além de um bit adicional, que representa o início de cada sequência de dados. Pode-se analisar o modelo de mensagem do protocolo na figura 3, conforme apresentado em [Neeraja et al. 2015].

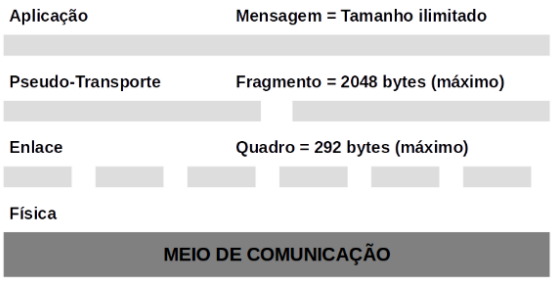

Figura 3. Frame DNP3. FONTE: Adaptado de [Jaimes 2012]

3. Vulnerabilidades e ameaças

Uma ameaça é qualquer coisa que possa causar uma interrupção na operação da rede ou nas funcionalidades do sistema e pode comprometer sua disponibilidade da rede[Darwish et al. 2015]. Podendo também ser vista como uma oportunidade de um invasor adentrar em uma rede e causar alterações ou interrupções, muitas vezes irreversíveis. Deste modo, são discutidos a seguir algumas das principais vulnerabilidades dos protocolos analisados.

3.1. ANSI C12.22

Uma ameaça que tem chamado a atenção, segue a linha de informações necessárias para que o *login* seja feito, ou seja, para um acesso remoto aos dispositivos. A solicitação para abertura de uma sessão de comunicação é realizada apenas com um *user* e um *user_id* da rede, que muitas vezes pode ser obtido utilizando um evento como alvo, já que muitas das vezes o *user* acaba aparecendo por um descuido de quem está configurando o MI. Com estes dados em mãos, o atacante pode utilizar-se de um método de força para descobrir a senha. O mecanismo de segurança 1.2.840.10066.2.1 do protocolo C12.22 [ANSI 2018], suporta o transporte de mensagens em texto simples, autenticado ou criptografado, baseando-se em opções do usuário. Uma vez que este atacante toma posse da senha informada pelo usuário legítimo, basta que o intruso insira um *timeout* igual a zero para que a sessão não seja fechada, gerando assim um bloqueio do operador, pois a plataforma deve limitar-se a apenas uma conexão de cada usuário por vez.

3.2. DNP3

Algumas vulnerabilidades são apresentadas em [East et al. 2009], como por exemplo, o fato de as implementações atuais do protocolo possibilitarem o uso com ou sem autenticação segura, potencializando uma possível penetração de dispositivos não legítimos na rede. Outra ameaça apontada por [Darwish et al. 2015] consiste em que não é definido no protocolo, ou em seus padrões, um mecanismo de segurança para os *Intelligent Electronic Device* (IED), nos quais o acesso remoto é realizado apenas com uma verificação de nome de usuário e senha, apenas na versão segura do protocolo. Esta fragilidade torna-se ainda mais acentuada quando, o fato de que muitos ataques são provenientes de empresas concorrentes ou até mesmo de ex-funcionários da própria concessionárias.

4. Comparações

- ANSI C12.22: Média segurança, pois não emprega por padrão a detecção de erros, apenas criptografia EAX-prime, apenas para mensagens maiores que a chave de

cifra, cujo tamanho é de 16 bytes [Minematsu et al. 2013].

- DNP3: A segurança é moderada, pois a camada de enlace fragmenta e identifica cada um dos fragmentos, isso facilita na identificação de segmentos perdidos ou alterados, evitando a retransmissão da mensagem completa, juntamente com seu algoritmo de detecção de erro [Pereira 2015]. Sincronização automática dos relógios dos dispositivos a cada evento com um indicador de tempo. O sistema de segurança e autenticação é implementado na camada de aplicação, e é baseado na ideia de *Message Authentication Code* (MAC) e *pre-shared key*, já que não ocorre encriptação de dados[Majdalawieh et al. 2007]. Um único quadro enviado em *broadcast*, criado por uma implementação vulnerável, pode travar o processo de recebimento ou criar um *loop* infinito, tornando toda pilha do protocolo inoperável [Crain and Bratus 2015].

O quadro 1 apresenta uma comparação entre os dois protocolos, baseando-se no estudo literários dos protocolos apresentados, seguindo critérios de confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade dos dados (CIDAI).

Tabela 1. Quadro comparativo C12.22 x DNP3

Comparação	**ANSI C12.22**	**DNP3**
Segurança na autenticação do nó	Média	Moderada
Segurança na camada de aplicação	Ausente	Presente
Detecção de erro	Ausente	Presente
Forma de segurança	Criptografia EAX' [Minematsu et al. 2013]	Fragmentação do pacote à cada camada

Análise dos protocolos apresentados. FONTE: Autor.

5. Conclusão

Foram detectadas vulnerabilidades para o *design*, juntamente com o estudo e análise de falhas dos protocolos ANSI C12.22 e DNP3. Onde o primeiro protocolo, deixa em aberto o modo como muitos serviços deverão ser implementados, porém este fato não desperta muitas vulnerabilidades atualmente, uma vez que o protocolo não tem muito tempo de mercado e ainda possui desenvolvedores trabalhando para obter um melhor desempenho deste protocolo. Por outro lado, o segundo protocolo já conta um vasto mercado e instituições que utilizam-se dele, para a comunicação em REI. A sincronização de tempo, juntamente com a facilidade de integração do DNP3 com outros sistema, o torna o mais indicado para utilização no momento, justamente por trazer mais segurança e aplicabilidade. Algumas das vulnerabilidades, juntamente com a visualização de um nível de segurança mais elevado foram possíveis graças à análise do material literal disponível sobre os protocolos e com a implementação básica em um sistema ao qual a comunicação foi observada com ambos os protocolos. Neste artigo, foram apresentadas as vulnerabilidades mais perceptíveis de ambos os protocolos, baseando-se no estudo literal de ambos.

Referências

ANSI (2018). ANSI C12.22-200x. Technical report, AMERICAN NATIONAL STANDARD. `https://bit.ly/2EZiBKf`, last accessed on 09/30/18.

Bagaria, S., Prabhakar, S. B., and Saquib, Z. (2011). Flexi-dnp3: Flexible distributed network protocol version 3 (dnp3) for scada security. In *2011 International Conference on Recent Trends in Information Systems*, pages 293–296.

Crain, J. A. and Bratus, S. (2015). Bolt-on security extensions for industrial control system protocols: A case study of dnp3 sav5. *IEEE Security Privacy*, 13(3):74–79.

Darwish, I., Igbe, O., Celebi, O., Saadawi, T., and Soryal, J. (2015). Smart grid dnp3 vulnerability analysis and experimentation. In *Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2 nd International Conference on*, pages 141–147. IEEE.

East, S., Butts, J., Papa, M., and Shenoi, S. (2009). A taxonomy of attacks on the dnp3 protocol. In *International Conference on Critical Infrastructure Protection*. Springer.

Faisal, M. A., Aung, Z., Williams, J. R., and Sanchez, A. (2012). Securing advanced metering infrastructure using intrusion detection system with data stream mining. In *Pacific-Asia Workshop on Intelligence and Security Informatics*. Springer.

Falcão, D. M. (2009). Smart grids e microrredes: o futuro já é presente. *SIMPÓSIO DE AUTOMAÇÃO DE SISTEMAS ELÉTRICOS*, 8.

Jaimes, O. E. R. (2012). *Estudios de desempeño de escenarios SCADA que utilizan el Protocolo DNP3*. PhD thesis, Uniandes.

Jin, D., Nicol, D. M., and Yan, G. (2011). An event buffer flooding attack in dnp3 controlled scada systems. In *Proceedings of the 2011 Winter Simulation Conference (WSC)*.

Majdalawieh, M., Parisi-Presicce, F., and Wijesekera, D. (2007). Dnpsec: Distributed network protocol version 3 (dnp3) security framework. In *Advances in Computer, Information, and Systems Sciences, and Engineering*, pages 227–234. Springer.

Minematsu, K., Lucks, S., Morita, H., and Iwata, T. (2013). Attacks and security proofs of eax-prime. In *International Workshop on Fast Software Encryption*. Springer.

Mohagheghi, S., Stoupis, J., and Wang, Z. (2009). Communication protocols and networks for power systems-current status and future trends. In *Power Systems Conference and Exposition, 2009. PSCE'09. IEEE/PES*, pages 1–9. IEEE.

Neeraja, T., Sivraj, P., and Sasi, K. (2015). Sensor based communication network for wacs with dnp3. *Procedia Technology*, 21:76–81.

Pereira, C. C. d. S. (2015). Modelo de simulação ns-2 para o protocolo dnp3 sobre o protocolo de rede sem fio ieee 802.15. 4 para simulação de baixo custo de aplicação smart grid.

Wang, J. and Leung, V. C. M. (2011). A survey of technical requirements and consumer application standards for ip-based smart grid ami network. In *The International Conference on Information Networking 2011 (ICOIN2011)*, pages 114–119.

Yang, B., Vittal, V., and Heydt, G. T. (2006). Slow-coherency-based controlled islanding—a demonstration of the approach on the august 14, 2003 blackout scenario. *IEEE Transactions on Power Systems*, 21(4):1840–1847.

Yu, R., Zhang, Y., Gjessing, S., Yuen, C., Xie, S., and Guizani, M. (2011). Cognitive radio based hierarchical communications infrastructure for smart grid. *IEEE network*, 25(5).