VI Simpósio de Iniciação Científica 2023
Ciência como ferramenta de transformação da sociedade

Levantamento do Estado da Arte em Medidores Inteligentes

Getúlio Victor Faustino Moreira[1] (IC), Otávio de Souza Martins Gomes[2]
[1]*Estudante do curso Engenharia Eletrônica, Universidade Federal de Itajubá (UNIFEI),*
[2]*Doutor pela Universidade Federeal de Itajubá (UNIFEI).*

Palavras-chave: Smart Meters, Medidores Inteligentes, Privacidade, Internet of Things, Smart Grid, Segurança da Informação, IoT, Criptografia, Vulnerabilidades, AMI, Advanced Metering Infrastructure.

Introdução

O conceito Smart Grid representa um dos sistemas os quais dependem diretamente de componentes interconectados, sendo um dos principais os medidores inteligentes. Os medidores inteligentes são capazes de otimizar ainda mais as características presentes nos medidores de energia comuns, além de adicionar a camada da conectividade, tarifas adaptáveis ao consumo de cada usuário, maior controle sobre o consumo de equipamentos, dentre outros atributos [1].

As informações coletadas estão disponíveis para as empresas associadas à disponibilização dos serviços e, em grande parte, para o usuário. Devido ao volume de dados coletados, é preciso implementar soluções de segurança baseadas em hardware e software, com o intuito de zelar pela privacidade dos usuários e qualidade dos serviços prestados [2].

Garantir que os princípios da segurança da informação sejam respeitados é fundamental para que os componentes da smart grid não caiam nas mãos de agentes maliciosos. Proteger tais sistemas é importantíssimo para que eles não sejam utilizados para realizar os mais diversos ataques a alvos direcionados.

Em vista desta contextualização, a justificativa do estudo do estado da arte desses instrumentos, é evidenciada pela crescente necessidade de implementar soluções de segurança as quais no momento atual se encontram deficientes ou negligenciadas. O intuito deste trabalho é entender mais a respeito dos medidores inteligentes com foco nos tipos de ataques realizados e suas contramedidas, principais vulnerabilidades presentes em protocolos de comunicação, firmware e hardware. Com o intuito de servir de base para trabalhos futuros nesse tema.

Metodologia

A metodologia abordada durante o trabalho pode ser classificada como pesquisa bibliográfica, de caráter quantitativo e de natureza aplicada. O processo de pesquisa passou por três etapas. A primeira etapa constituiu pela definição dos objetivos da pesquisa e revisão técnica detalhada a respeito da literatura, com o foco em compreender os estudos anteriores relacionados às características dos medidores inteligentes, componentes presentes na rede em que se conectam, e sobre a infraestrutura de medição avançada (AMI) [3].

Na segunda etapa foi realizado um breve estudo a respeito do funcionamento dos tipos de criptografia e os principais algoritmos utilizados para o armazenamento de informações nos dispositivos embarcados, isto é, computação de borda (edge computing).

Posteriormente, após entender mais a respeito da confidencialidade e como implementá-la no nosso contexto, o levantamento de vulnerabilidades presentes nos protocolos de comunicação, firmware e hardware do medidor. Por fim, após o levantamento de todas essas informações foi determinada uma conclusão para o que foi analisado e, as expectativas futuras em relação a trabalhos futuros envolvendo a mesma problemática.

Este trabalho se limita a apresentar algumas das diversas vulnerabilidades presentes nos medidores inteligentes, portanto, não apresenta a totalidade dos riscos existentes atualmente.

Resultados e discussão

Um medidor inteligente é um sistema embarcado o qual possui três componentes principais: medidor elétrico, unidade de processamento e módulo de comunicação [1]. O medidor elétrico mede o consumo e traduz as leituras para a unidade de processamento, após isso, essa unidade irá processar e armazenar a informação gerada tanto pelo medidor elétrico quanto pelo módulo de comunicação.

A comunicação entre a HAN (Home Area Network) e a unidade central de controle é mantida pelo módulo de comunicação. Os smart meters permitem que os consumidores observem detalhadamente o seu consumo e a partir dessas informações, e com base nisso, podem decidir como devem utilizar a energia elétrica [3].

Contudo, apesar de possuir vantagens, um grande ponto crítico do smart meter é a segurança, ao implementar em um dispositivo a comunicação de via dupla, gera a oportunidade para que possa ser invadida por agentes maliciosos. Devido a sua grande complexidade de implementação e gerenciamento, falhas de segurança ocorrem com certa frequência.

Para entender melhor sobre esse componente da Smart Grid é preciso explorar mais a respeito sobre a infraestrutura em que o medidor faz parte. A infraestrutura de medição avançada (AMI) descreve toda a infraestrutura de energia elétrica, ela pode comunicar-se com os consumidores e é a estrutura principal da smart grid [2]. Seus principais objetivos consistem em realizar medições remotamente livres de erros, identificar problemas na rede, auditoria da energia, etc. Essa infraestrutura consiste de diversas soluções em hardware e software. Dentre os componentes técnicos principais encontramos os:

- Smart Meters: Responsáveis por realizar a medição de energia, água e gás, transmitir esses dados para as companhias que oferecem os serviços através de uma rede de comunicação, e por fim receber sinais de cobrança e transmiti-los para os consumidores.
- Rede de comunicações: Geralmente suportam comunicação entre 2 pontos (2 vias). Exemplos: Comunicação via fibra óptica, redes públicas, Banda Larga na Linha de Transmissão, comunicação via linha de transmissão, etc.
- Sistema de Aquisição de Dados do Medidor: Engloba aplicações de controle central (hardware e software) na unidade concentradora de dados, sendo ela responsável por buscar os dados do medidor pela rede de comunicação e enviá-los para o sistema de gerenciamento de dados do medidor.
- Sistema de gerenciamento de dados do medidor (MDMS): Sistema principal (host) que recebe, armazena e analisa as informações obtidas na medição [3].

Ao utilizar a AMI podemos observar benefícios operacionais, financeiros, relacionados aos consumidores ou a segurança. A precisão na leitura da medição, identificação de furto de energia, redução no custo de manutenção, aumento na precisão e flexibilidade das tarifas direcionadas ao consumidor, segurança das informações trocadas entre o medidor e concessionária, são alguns dos principais fatores que contribuem para a implementação dessa infraestrutura.

As informações presentes nos dados coletados pelos medidores inteligentes possuem grande sensibilidade, pois estão diretamente atrelados aos hábitos de consumo dos usuários. Para que esses dados não caiam nas mãos de agentes maliciosos é preciso adicionar camadas de proteção, levando em consideração as restrições físicas e lógicas dos componentes, para reduzir os ataques direcionados a Smart Grid.

Uma solução computacional já bem estabelecida são os algoritmos de criptografia, como o AES ou ECC, essas técnicas criptografam os dados para que eles possam ser armazenados e transmitidos de forma segura e, somente quem possui o acesso autorizado a essas informações que tem a permissão para visualizar o conteúdo presente.

O ECC, mais especificamente sua versão dedicada para aplicações de baixo consumo (Lightweight ECC), garante a autenticação e confidencialidade [4]. Isso ocorre pois esse algoritmo é uma cifra assimétrica, a qual utiliza um tamanho de chave maior e, consequentemente, consome mais recursos de memória, isso impacta diretamente em sua escolha em dispositivos IoT, sendo que esses operam com recursos limitados [5-6].

Cada algoritmo determina o modo em que irá gerenciar suas chaves. Contudo, existem três modos de transmissão relacionados ao gerenciamento de chaves que podem estar inclusos, sendo eles o modo de transmissão unicast, multicast e broadcast.

O modo de transmissão unicast é utilizado para comunicação entre dois pontos. Os dados são transmitidos do remetente e são enviados para um destinatário específico. No contexto da rede AMI, esse tipo de transmissão acontece quando um medidor inteligente envia os dados de consumo para a concessionária [7].

No modo de transmissão multicast a comunicação ocorre entre um ponto e diversos pontos específicos, denominados como grupo. No contexto da rede AMI, essa transmissão ocorre quando a concessionária envia mensagens notificando para um grupo de medidores inteligentes na mesma localização ou um grupo de resposta à demanda [8].

Por último, o modo de transmissão broadcast é usado para comunicar entre um ponto e todos os outros pontos da rede. Na rede AMI, a transmissão broadcast acontece quando a concessionária comunica as mudanças no preço das tarifas para todos os consumidores, assim como notificar a respeito de instabilidades na disponibilidade de energia elétrica [9].

Em suma, a criptografia pode ser implementada

tanto a nível de software, quanto a nível de hardware com a implementação de um módulo de segurança em hardware (HSM), podendo utilizar FPGAs, que consiste em um circuito eletrônico dedicado especialmente para geração e armazenamento de chaves criptográficas. Entretanto, a criptografia das comunicações é somente um dos aspectos importantes a se considerar, devemos levar em consideração quais são os protocolos de comunicação e as vulnerabilidades presentes em cada um desses protocolos, ataques direcionados diretamente ao hardware do dispositivo, dentre outros.

Independentemente da abordagem é necessário analisar se determinada configuração atende aos requisitos necessários para os dispositivos IoT. Uma solução para dispositivos embarcados, dentre as inúmeras existentes, que providencia segurança e ao mesmo tempo é eficiente no gerenciamento de consumo de energia é o coprocessador MAXQ1065. Esse controlador fornece funções criptográficas, que visam garantir a confidencialidade e integridade dos dados, assim como autenticação mútua, inicialização e atualização segura de firmware, comunicação segura, suporte a TLS (Transport Layer Security), dentre outros [10]. Suas principais características e benefícios são o mecanismo de computação ECC, SHA-2, AES (chaves de 128 e 256 bits), interface de alta velocidade para microcontrolador host, comunicações seguras via TLS/DTLS, gerador de números aleatórios, etc.

Existem diversos tipos de ataques sendo eles classificados em físicos e sistemas de comunicação. Os ataques físicos incluem por exemplo, o tampering, que consiste na modificação intencional ou não intencional que altera o funcionamento comum de um equipamento. Essa alteração pode levantar a possibilidade de manipular os dados presentes na memória interna do smart meter e, obter acesso caso bem sucedido, a mecanismo de gerenciamento de senhas, algoritmos de criptografia e autenticação. Para se proteger desses ataques, é preciso implementar sistemas internos, além de possuir sistemas de alarme.

Na categoria de ataques aos sistemas de comunicação (Tabela 1) encontramos as tecnologias com fio e sem fio, conforme a Tabela 2.

Protocolos de Comunicação	Funcionamento	Benefícios
PLCC	Transmissão de sinais digitais via linhas de transmissão	Poucas ou nenhuma interferência a longas e curtas distâncias
Fibra Óptica (OFC)	Transmissão de dados utilizando a luz como meio	Fácil instalação; Altas taxas de transferência
ZigBee	Transmissão de dados via comunicação sem fio de baixo consumo	Alta confiabilidade; Baixo consumo e custo; Autoconfiguração
Long Term Evolution (LTE)	Utilizado pelas operadoras de telefonia para transmissão de dados em baixa latência	Eficiência no consumo de recursos; Pouca interferência
Wi-Fi	Transmissão de dados via sinais de rádio de alta frequência	Amplamente Adotado; Baixo Custo; Protocolo Aberto

Tabela 1 – Funcionamento de Protocolos de Comunicação

Nas tecnologias com fio podemos citar a PLCC (Power Line Carrier Communication) e fibra óptica (OFC) [11][12]. Na comunicação sem fio os exemplos são diversos, porém em especial serão abordados brevemente o Wi-Fi, ZigBee [13][14] e LTE [15].

Protocolos	Vulnerabilidades	Contramedidas
PLCC	Linhas de Transmissão Expostas	Criptografia
Fibra Óptica (OFC)	In-Band Jamming; Out-Band Jamming; Divisores e Acopladores de Cabo.	Sistemas de Detecção de Energia e Detecção de Intrusão
ZigBee	Jamming; Captura de Mensagens; Tampering.	Autenticação; Criptografia; Utilizar um Gateway entre a

		HAN e o SM
Long Term Evolution (LTE)	Ataques por via aérea	2FA; Criptografia
Wi-Fi	Man-in-the-middle ; Sequestro de Sessão; Análise de Tráfego	2FA; Criptografia

Tabela 2 – Vulnerabilidades em Protocolos de Comunicação

Conclusões

Foram apresentadas neste resumo as características de um medidor inteligente e a infraestrutura da qual o mesmo faz parte (AMI), com o intuito de compreender e contextualizar o tema apresentado. Devido a necessidade de proteção foi comentado a respeito de um algoritmo de criptografia em específico, e os possíveis gerenciamento de chave. Por último foi exibido algumas vulnerabilidades presentes nos protocolos utilizados atualmente. Em vista das informações apresentadas na discussão foi possível extrair delas que existe uma crescente preocupação com a necessidade de proteção dos dispositivos relacionados a Smart Grid e sistemas críticos.

A perspectiva futura é que esse trabalho contribua para conscientizar a respeito da necessidade de correção das falhas enunciadas e, em trabalhos futuros, obter resultados práticos a respeito dessas vulnerabilidades, assim como destacar mais a respeito de temas como a privacidade do usuário quando se trata desses dispositivos conectados. As futuras linhas de pesquisa envolvem, a análise de vulnerabilidades e testes de invasão em medidores inteligentes, desenvolvimento de novas técnicas de criptografia, dentre outros.

Agradecimentos

Gostaria de expressar minha imensa gratidão às pessoas e instituições que tornaram a realização desse estudo possível. A princípio gostaria de agradecer ao Otávio de Souza Martins Gomes, pela oportunidade concedida e por orientar durante todo o período da iniciação científica.

Além disso gostaria de agradecer a Universidade Federal de Itajubá pela oportunidade disponibilizada. Assim como prestar os agradecimentos a Fapemig por financiar a bolsa concedida durante todo o período da iniciação científica (PVDI277-2022).

Referências

[1] Costache, M., Tudor, V., Almgren, M., Papatriantafilou, M., & Saunders, C. (2011, September). Remote control of smart meters: friend or foe?. InComputer Network Defense (EC2ND), 2011 Seventh European Conference on (pp. 49-56). IEEE

[2] E. B. Bureau, “The benefits and challenges of using smart energy meters,” ElectronicsB2B, Jan. 23, 2019. https://www.electronicsb2b.com/important-sectors/consumer-electronics-and-gadgets/the-benefits-and-challenges-of-using-smart-energy-meters/

[3] D. Bian, M. Kuzlu, M. Pipattanasomporn and S. Rahman, "Analysis of communication schemes for Advanced Metering Infrastructure (AMI)," *2014 IEEE PES General Meeting | Conference & Exposition*, National Harbor, MD, USA, 2014, pp. 1-5, doi: 10.1109/PESGM.2014.6939562.

[4] Akber Ali Khan, Vinod Kumar, Musheer Ahmad, An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach, Journal of King Saud University - Computer and Information Sciences, Volume 34, Issue 3, 2022, Pages 698-705, ISSN 1319-1578.

[5] Singh, S., Sharma, P.K., Moon, S.Y. et al. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput (2017). https://doi.org/10.1007/s12652-017-0494-4

[6] Muhammad Rana, Quazi Mamun, Rafiqul Islam, Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems, Volume 129, 2022, Pages 77-89, ISSN 0167-739X

[7] T. Aktaş, A. Yılmaz, and E. Aktaş, “Practical Methods for Wireless Network Coding with Multiple Unicast Transmissions,” 2012.. Available: https://arxiv.org/pdf/1112.3208.pdf

[8] N. Din *et al.*, “A typology of secure multicast communication over 5 G/6 G networks,” *International Journal of Information Security*, vol. 22, no. 4, pp. 1055–1073, Mar. 2023, doi: https://doi.org/10.1007/s10207-023-00678-y.

[9] Kebotogetse O, Samikannu R, Yahya A. Review of key management techniques for advanced metering infrastructure. International Journal of Distributed Sensor Networks. 2021;17(8). doi:10.1177/15501477211041541

[10] MAXQ1065 Ultra Low-Power Cryptographic Controller with ChipDNATM for Embedded Devices, https://www.analog.com/media/en/technical-documentation/data-sheets/MAXQ1065.pdf

[11] R. Mahmud, R. Vallakati, A. Mukherjee, P. Ranganathan and A. Nejadpak, "A survey on smart grid metering infrastructures: Threats and solutions," *2015 IEEE International Conference on Electro/Information Technology (EIT)*, Dekalb, IL, USA, 2015, pp. 386-391, doi: 10.1109/EIT.2015.7293374.

[12] Skopik, Florian et al. “A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures.” *International Journal of Smart Grid and Clean Energy* (2012): 22-28.

[13]“UG103.2: Zigbee Fundamentals.” Available: https://www.silabs.com/documents/public/user-guides/ug103-02-fundamentals-zigbee.pdf

[14]“Zigbee Explained: What It Is and How It Works,” *DIY Smart Home Solutions*, Aug. 05, 2019. https://www.diysmarthomesolutions.com/zigbee-wireless-networking/

[15] M. Keerthika, D. Shanmugapriya, Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures. Global Transitions Proceedings,Volume 2, Issue 2, 2021, Pages 362-367, ISSN 2666-285X, https://doi.org/10.1016/j.gltp.2021.08.045.