SECS/GEMsec: A mechanism for detection and prevention of cyber-attacks on SECS/GEM communications in industry 4.0 landscape

ABSTRACT

Industry 4.0 as a driving force is making huge strides, particularly in the manufacturing sector, where all integral components involved in the production processes are getting digitally interconnected. Fused with improved automation and robotics, machine learning, artificial intelligence, big data, cloud computing, and the Internet of Things (IoT), this open network interconnectivity makes industrial systems increasingly vulnerable to cyber-attacks. While the impacts and intentions of cyber-attacks vary, they always have a detrimental effect on manufacturers, including financial losses, supply chain disruption, loss of reputation and competitiveness, and theft of corporate secrets. Semiconductor Equipment Communication Standard/Generic Equipment Model (SECS/GEM) is a legacy Machine-to-Machine (M2M) communication protocol used profoundly in the semiconductor and other manufacturing industries. It is mainly designed to be utilized in a controlled and regulated factory environment separated from external networks. Industry 4.0 has revolutionized the manufacturing industry and has brought SECS/GEM back to the limelight as it lacks security safeguards to protect against cyber-attacks. This paper proposes a digital signature-based security mechanism that offers authentication, integrity, and protection against cyber-attacks. The proposed mechanism is compared with the industry-standard SECS/GEM implementation in terms of processing time, payload overhead, and resilience against cyber-attacks. The results indicate that SECS/GEMsec effectively prevented untrusted entities from establishing communication links with legit industrial equipment while maintaining message integrity by discarding forged messages. Additionally, it protected SECS/GEM communications against Denial-of-Service (DoS) attacks, Replay attacks, and False-Data-Injection-Attack (FDIA) attacks.