Scalable Interconnection of Industrial Networks:KDC Placement Problem in Secure VPLS

Mohammad Borhani - Linköping University
SWITS23

Abstract

Industry 4.0 has transformed industrial operations by incorporating Internet-enabled devices to collect, process, and store data both on-premises and in the cloud. This connectivity enables remote monitoring and control of industrial devices, enhancing operational efficiency and facilitating remote work. Industrial sectors, including healthcare, transportation, and grid systems, have implemented Internet connectivity to automate processes and enhance productivity, efficiency, and safety.

In addition, within the Coronavirus outbreak, most individuals have shifted to remote work, relying on the Internet to maintain daily activities. Unfortunately, many production facilities were forced to close down because they could not provide secure remote control of their equipment or continue operations exposing their employees to infection risks. As industries become increasingly reliant on Internet connectivity for efficacy, it is crucial to recognize that this reliance makes them susceptible to cyberattacks. The Stuxnet attack on critical industrial infrastructure more than a decade ago was just the beginning; industries now face more frequent cyberattacks that can affect operations and reliability. Our study of device scanners in Sweden uncovered hundreds of ICS/SCADA devices with known exploitable vulnerabilities.

While it is not possible to disconnect a wide range of Industrial Internet-of-things (IIoT) devices from the Internet, cloaking (hiding) may be employed to keep their functions inaccessible to the public Internet while still allowing for remote data management and updates. The idea behind Virtual Private LAN Services (VPLS) is to connect islands of such devices to a single virtual local-area network through a set of encrypted tunnels. The Host Identity Protocol (HIP)-based VPLS (HIPLS) provides an appropriate approach for establishing IPsec ESP tunnels with a base exchange, maintaining them with keep-alive UPDATE messages, and closing them gracefully when no longer required within a secure VPLS. Session key-based HIPLS (S-HIPLS) is a VPLS architecture based on HIP that implements security mechanisms such as authentication, encryption, etc. using a Key Distribution Center (KDC). However, it has limited scalability.

Using multiple distributed KDCs would provide numerous benefits, such as decreased workload per KDC, distributed key storage, and enhanced scalability while concurrently removing a single point of failure of S-HIPLS. It would also necessitate optimal placement of KDCs within the provider network. We formulate the KDC placement (KDCP) problem for a secure VPLS network as an Integer Linear Programming (ILP) problem. The latter is NP-hard, indicating a high computational cost for exact solutions, particularly for large deployments. We motivate the use of a primal-dual algorithm to produce near-optimal solutions efficiently. Extensive evaluations on large-scale network topologies, such as the random Internet graph, demonstrate the proposed method's time efficiency and its improved scalability and usefulness compared to HIPLS and S-HIPLS.