Technical Disclosure Commons

Defensive Publications Series

February 20, 2019

INTEGRATED SECURITY-TAGGING FOR DETERMINISTIC ETHERNET

Maik Seewald

Robert Barton

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Seewald, Maik and Barton, Robert, "INTEGRATED SECURITY-TAGGING FOR DETERMINISTIC ETHERNET", Technical Disclosure Commons, (February 20, 2019)
https://www.tdcommons.org/dpubs_series/1969

This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

INTEGRATED SECURITY-TAGGING FOR DETERMINISTIC ETHERNET

AUTHORS:
Maik Seewald
Robert Barton

ABSTRACT

Techniques are described herein for enhancing Time-Sensitive Networking (TSN) in network fabrics by dynamically assigning Secure Group Tags (SGTs) based on the stream configuration in a TSN controller. The TSN controller communicates stream details to a policy engine which creates a policy and assigns an SGT for the stream. The TSN controller pushes regular stream scheduling to the network switches, but also pushes a function that maps the stream identification based on the multicast Media Access Control (MAC) to a specific SGT. The TSN stream is now protected by the correct SGTs end-to-end.

DETAILED DESCRIPTION

Many industrial networks (e.g., manufacturing, oil and gas, utilities, etc.) use time sensitive applications where end-to-end latency must not only be minimized, but must also be predictable. In light of this, IEEE 802.1 Time Sensitive Networking (TSN) has been developed for industrial applications. TSN is a scheduling mechanism where each node along the path is presented with a transmission schedule for a particular application stream.

User are increasingly benefiting from overlay technologies in Operational Technology (OT), such as Software-Defined Access (SDA). A key component of SDA is Secure Group Tags (SGTs), a technology used to create logical groupings of devices. SGTs have the advantage of decoupling access control mechanisms from fixed definitions such as Media Access Control (MAC) / Internet Protocol (IP) addresses and Virtual Local Area Networks (VLANs), which is highly desirable in dynamic environments such as mining or oil and gas. SGTs are typically used by switches, routers, and firewalls to establish access control and to make forwarding decisions. However, there are many limitations with this technology in industrial environments. For example, today SGTs (and SDAs in general) are not compatible with TSN, meaning there is a roadblock to deploying Software Defined Networking (SDN) fabrics in industrial environments.

Accordingly, techniques described herein provide a mechanism to apply SGT as an integral part of the stream configuration process in TSN. Because TSN networks are fully scheduled networks, a network controller is used to configure streams (providing the schedules) in end-stations (devices) and network components (switches). SGTs are combined with a stream configuration in the process of TSN configuration. Stream configuration is based on the definitions and calculations provided by a network controller. Combining the stream configuration with the process of applying the SGT enables end-to-end security in a granular manner from the beginning. A security framework may be integrated with the network controller used in the scope of TSN.

The following example method uses a security framework / policy engine. First, the application scheduling requirements are configured by an administrator in the Central User Configuration (CUC). Second, the TSN network controller is integrated with the policy engine (via an Application Programming Interface (API)), which is the policy engine that defines the SGTs. The network controller calculates the network definitions (schedules, streams) and provides the results to the policy engine. Third, based on existing network policies in the policy engine and the configuration data (the path through the TSN-enabled network provided by the network controller), the policy engine applies an SGT to the definitions and returns the results to the network controller.

Fourth, the network controller holds all information to configure TSN streams in the underlying network. Thus, the network controller communicates TSN configuration details to the endpoints and the TSN switches in the network. The network controller is now responsible for providing the SGT configuration along with the TSN stream details. TSN streams are defined based on multicast MAC addresses and VLANs. In essence, the network controller is pushing a mechanism to the switches where TSN streams are authorized on ingress to the switch, and the correct SGT is automatically applied. In addition, the SGTs provided by the policy engine allow fine-granular segmentation of the underlying industrial control network. Stream configuration and tagging is executed in one process, highly automated and fully integrated.

Fifth, the configuration is also provided to the TSN end-stations (e.g., Industrial Internet of Things (IIoT) devices) as well as the other network components (e.g., switches) in the TSN network, to ensure the stream is correctly scheduled. As a result, the TSN network is fully configured in terms of TSN streams and regarding SGTs. This provides not only granularity in access control and segmentation but also protection from attacks on the network (e.g., Denial of Service (DoS)) and/or misconfigured (babbling) devices.

Figure 1 below provides an example overview.

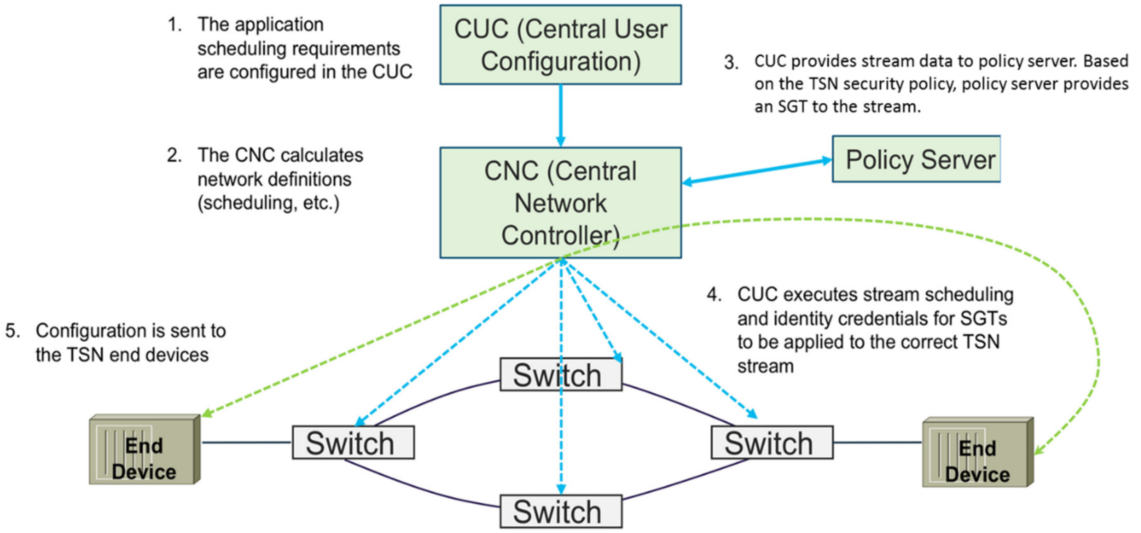
1. The application scheduling requirements are configured in the CUC
CUC (Central User Configuration)
3. CUC provides stream data to policy server. Based on the TSN security policy, policy server provides an SGT to the stream.
2. The CNC calculates network definitions (scheduling, etc.)
CNC (Central Network Controller)
Policy Server
4. CUC executes stream scheduling and identity credentials for SGTs to be applied to the correct TSN stream
5. Configuration is sent to the TSN end devices
Switch
End Device
Switch
Switch
Switch
End Device

Figure 1

The integration of SGT into network and stream configuration in the scope of TSN creates a solution that is secured in an end-to-end scenario. Furthermore, the techniques presented herein promote a highly automated approach, making the configuration process less error-prone. Security is an important requirement and success criteria for industrial control networks where TSN / Deterministic Ethernet is used. A flexible, scalable, and highly automated mechanism is provided to protect TSN-streams using SGTs.

In summary, techniques are described herein for enhancing TSN in network fabrics by dynamically assigning SGTs based on the stream configuration in a TSN controller. The TSN controller communicates stream details to an identity services engine which creates a policy and assigns an SGT for the stream. The TSN controller pushes regular stream scheduling to the network switches, but also it now pushes a function that maps the stream identification based on the multicast MAC to a specific SGT. The TSN stream is now protected by the correct SGTs end-to-end.