Linc: Low-Cost Inter-Domain Connectivity for Industrial Systems

Tony John
OvGU Magdeburg, Germany
tony.john@ovgu.de

Piet De Vaere
ETH Zürich, Switzerland
piet.de.vaere@inf.ethz.ch

Caspar Schutijser
SIDN Labs, The Netherlands
caspar.schutijser@sidn.nl

Adrian Perrig
ETH Zürich, Switzerland
adrian.perrig@inf.ethz.ch

David Hausheer
OvGU Magdeburg, Germany
hausheer@ovgu.de

ABSTRACT

As industrial control systems are becoming increasingly interconnected, there is a rising need for secure and highly available communication as a commodity product. Therefore, we introduce Linc, a communication gateway that leverages SCION, a next-generation Internet architecture, to provide highly reliable and secure inter-domain connectivity for industrial applications.

CCS CONCEPTS

• **Security and privacy** → **Network security**; • **Networks** → **Network properties**; **Network architectures**.

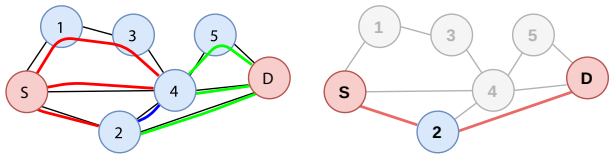
KEYWORDS

Gateway, SCION Internet architecture, path-aware networking, high availability, geofencing

1 INTRODUCTION

Traditionally, industrial control systems (ICSs) were operated as isolated environments within single facilities. However, in recent years, we have witnessed these systems being increasingly interconnected; both with each other, and with secondary systems such as cloud services [2]. Whereas in the past these connections were typically limited to emergency access for remote control, the rise of the Industrial Internet of Things (IIoT) and Industry 4.0 is leading to an increase of both the number of interconnections and the importance of these connections to the control systems. For example, it has become increasingly common for electrical power plants to be operated remotely, without on-site personnel [7]. This became even more prevalent during the Covid pandemic, as many employees were required to work from home.

Because of the high security requirements placed on industrial systems, interconnections between control systems are usually established using dedicated leased lines or MPLS backbones. Doing so not only provides strong traffic isolation properties, but also ensures high availability, a property of paramount importance for ICSs. However, because of the exclusive nature of such circuit-based connections, they come at high monetary cost. Moreover, as one of the core visions of Industry 4.0 is to significantly extend the horizontal system integration across different sites [8], these monetary costs—together with the management overhead—are bound to increase dramatically.



(a) using SCION routing **(b) using BGP routing**

Figure 1: Inter-domain network topologies as perceived by AS S when sending traffic to AS D.

With this paper, we demonstrate Linc (Low-cost Industrial Network Connectivity)—an industrial network gateway that facilitates the deployment of IIoT and Industry 4.0 technologies by providing secure and highly available connectivity at low cost, thus removing the need for dedicated network connections. Linc accomplishes this by leveraging the SCION secure Internet architecture [5]. More specifically, the path-aware nature of SCION networks enables Linc to (i) optimize connectivity based on latency, jitter, bandwidth, and packet-loss requirements; (ii) achieve fast connection failover and perform *make-before-break* connection migration; and (iii) ensure that network traffic only crosses trusted network infrastructure. With SCION, these benefits, while similar to those provided by a leased line connection, can be served over a public network at a much lower cost and reduced management overhead. Moreover, SCION's Dynamically Recreatable Key (DRKey) infrastructure allows Linc to provide source-authentication and end-to-end encryption with minimal configuration overhead.

2 SCION INTERNET ARCHITECTURE

SCION is a secure next-generation Internet architecture designed to provide route control, fault isolation, and explicit trust information for end-to-end communication [5]. SCION inherits the benefits of today's Internet and is designed to overcome its limitations.

One of SCION's key concepts, and simultaneously the primary property Linc leverages, is the use of path-based routing. In a SCION network, senders can select the path their packets will travel on using *path segments*. We illustrate this in Figure 1a, where the available path segments are highlighted in red, green, and blue.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-1-4503-8629-6/21/08.
https://doi.org/10.1145/3472716.3472850

AS S can combine these path segments to create end-to-end paths from S to D, over which packets can then be transmitted. Doing so allows S to use the network path(s) who's properties best match the requirements of its traffic. This stands in contrast with BGP, where, as illustrated in Figure 1b, only a single, network-selected path can be used between ASes S and D.

Today, SCION connectivity can be obtained through seven ISPs worldwide, or by joining the scientific SCIONLab network, which has been in operation since 2016 [4].

3 LINC GATEWAY

We design the Linc gateway to achieve the following goals:

Brownfield compatibility (G1): Linc should be deployable without modifications to end hosts.
Path optimality (G2): Traffic should be sent on the optimal path based on specific metrics, *e.g.*, latency, jitter, bandwidth, and packet loss.
Availability (G3): Traffic should achieve high availability, with fast failover in case of a link failure.
Geofencing (G4): Traffic should only traverse trusted networks.
Authentication (G5): Traffic should be source authenticated and end-to-end encrypted.

Brownfield-compatibility (G1) is achieved by designing Linc as a SCION-IP gateway. This allows Linc to bridge multiple IP deployments over a SCION network in a way that is transparent to the hosts in the IP deployment. This is illustrated in Figure 2, which shows an example Linc deployment that bridges a SCADA network to an enterprise network for remote management.

Linc achieves path optimality (G2) by allowing path preferences based on network metrics to be specified in a configuration file, and by continuously measuring path properties. A path selection module then selects the most appropriate path(s) for each packet.

In order to provide high availability (G3), Linc supports three failover and redundancy modes: single-path, redundant multi-path and adaptive multi-path. In single-path mode, when a path fails the Linc gateway switches to an alternative path as soon as the failure is detected. This mode is most suitable for applications that can tolerate a momentary interruption in connectivity. Since failover decisions are made by the gateway, recovery times after a link failure will be of the same order of magnitude as the traffic's RTT. This stands in contrast to the BGP Internet, where recovery times are measured in minutes [3]. In redundant multi-path mode, traffic is duplicated at the IP level and continuously transmitted over two or more paths. If one path fails, traffic keeps flowing along the other path(s), minimizing the impact on the application. This mode is most suitable for applications that require absolute availability or have very low traffic volumes. The adaptive multi-path mode follows a *make-before-break* approach, in which the Linc gateway starts duplicating traffic on an additional path as soon as the performance of the primary path drops below a specified threshold. If the primary path recovers, the redundant transmission is stopped. If the primary path deteriorates further, the traffic is fully routed over the additional path. This approach provides a trade off between the single-path and redundant multi-path modes. Moreover, it allows Linc to quickly react to changing network conditions (*e.g.*, sudden increase in latency or jitter) while minimizing the impact of false-positives (*e.g.*, if the adverse condition was only transient).

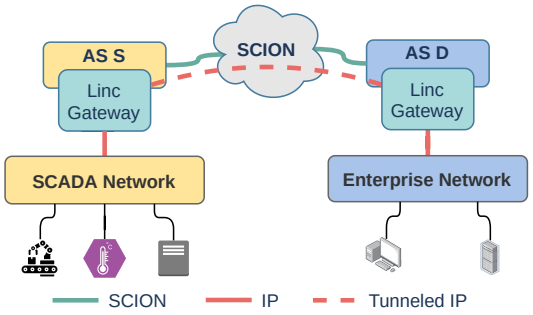


Figure 2: An example Linc deployment

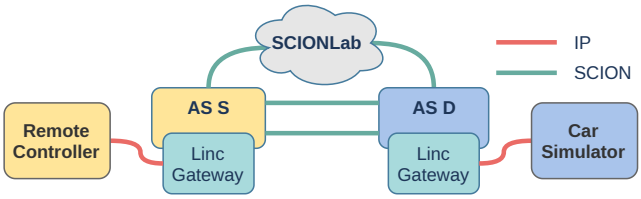


Figure 3: Network layout of the demo

Since SCION ASes have a high level of control over the paths used for their traffic, geofencing (G4) can be implemented entirely in the Linc gateway. Concretely, the gateway exposes a routing policy file that allows administrators to black- or whitelist specific ASes, thereby ensuring that traffic only traverses trusted networks. Because SCION routing information is carried in each packet header, routing attacks (*e.g.*, BGP hijacking) are not possible.

SCION's DRKey subsystem [6] enables Linc to efficiently derive keys for each gateway pair. These keys are used to authenticate and encrypt all inter-gateway traffic. This mechanism prevents espionage and man-in-the-middle attacks against the application traffic.

4 REMOTE DRIVING DEMO

We demonstrate the capabilities of Linc using a simulated remote driving demonstration. Similar to industrial control systems, remote driving requires a highly reliable communication channel: any interruption can have severe consequences in a real-world scenario. Figure 3 illustrates the demo setup. The remote controller sends control messages to the car simulator, and the simulator sends back a video feed from the front view camera of the car. Both the controller and the simulator are connected to a Linc gateway. There are three paths available between the two gateways, one of which is routed over SCIONLab [4].

The three operating modes and path selection preference features of Linc are demonstrated in the demo by disconnecting the paths one by one and by changing the paths' metrics using Linux's NetEm [1].

REFERENCES

[1] 2011. *tc-netem(8) — Linux manual page.*

[2] Cristina Alcaraz and Sherali Zeadally. 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection* 8 (2015), 53–66.

[3] Ricardo Bennesby da Silva and Edjard Souza Mota. 2017. A survey on approaches to reduce BGP interdomain routing convergence delay on the Internet. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 2949–2984.

[4] Jonghoon Kwon, Juan A. García-Pardo, Markus Legner, François Wirz, Matthias Frei, David Hausheer, and Adrian Perrig. 2020. SCIONLab: A Next-Generation Internet Testbed. In *Proceedings of the IEEE International Conference on Network Protocols (ICNP).*

[5] Adrian Perrig, Pawel Szalachowski, Raphael M Reischuk, and Laurent Chuat. 2017. *SCION: a secure Internet architecture.* Springer.

[6] Benjamin Rothenberger, Dominik Roos, Markus Legner, and Adrian Perrig. 2020. PISKES: Pragmatic Internet-Scale Key-Establishment System. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (ASIACCS).* https://doi.org/10.1145/3320269.3384743

[7] Marco Sanchez. 2021. Five Reasons Remote Technology Makes Sense Even If You Never Plan to Operate Your Power Plant Remotely. (21 Jan 2021). Retrieved June 1, 2021 from https://www.powermag.com/five-reasons-remote-technology-makes-sense-even-if-you-never-plan-to-operate-your-power-plant-remotely/

[8] Li Da Xu, Eric L Xu, and Ling Li. 2018. Industry 4.0: state of the art and future trends. *International Journal of Production Research* 56, 8 (2018), 2941–2962.