System Detecting Border Gateway Protocol Anomalies Using Local and Remote Data

Authors : Alicja Starczewska, Aleksander Nawrat, Krzysztof Daniec, Jarosław Homa, Kacper Hołda

Abstract : Border Gateway Protocol is the main routing protocol that enables routing establishment between all autonomous systems, which are the basic administrative units of the internet. Due to the poor protection of BGP, it is important to use additional BGP security systems. Many solutions to this problem have been proposed over the years, but none of them have been implemented on a global scale. This article describes a system capable of building images of real-time BGP network topology in order to detect BGP anomalies. Our proposal performs a detailed analysis of BGP messages that come into local network cards supplemented by information collected by remote collectors in different localizations.