Network Anomaly Detection using Sensor Devices

1710239 Shogo Asaba

Network failure causes a serious impact on social life. It is important to detect rapid and accurate network anomalies. In large-scale networks, the cause of network failures diversifies and becomes complicated. Consequently, The network administrator who operates a large-scale network has to measure their network environment periodically.

It is essential to measure the change of the network state in order to detect the malfunction of equipment constituting the network an indication of failures. In contrast, too many telemetric queries to network facilities cause wasting computing and network resource in these devices. Therefore, it gives a non-ignorable impact to the network system.

In this research, I conducted to network anomaly detection using sensor devices. I periodically measured the network condition from the sensor devices which measures a network condition developed by SINDAN Project. From their measurement results, We examined the method of network anomaly detection using several anomaly detection algorithms. Using the sensor devices, the measurement can be performed without imposing a high load on the resources of the network devices. In addition, network measurement data have different characteristics such as periodicity and correlation that depending on the type of data. Focusing on these characteristics, we achieved realized difficult anomaly detection which cannot be detected by existing detecting mechanisms.

For the network condition measurement of this research, I used the network condition measurement method of SINDAN Project, which is previous research. In the previous method, the network state is hierarchically measured across the data link layer, the interface setting layer, local network layer, global network layer, name resolution layer, and web application layer.

I evaluated my proposed method using an assumed case where a load of wireless Becomes high. I carried out the network measurement at a 1-minute interval. I tried to anomaly detection by using multiple algorithms to the measurement results and considered from the results. I used unsupervised learning algorithms such as Local Outlier Factor which detects outliers from correlated data collection and Change Finder which is change point detection. Since unsupervised learning algorithms do not require tagging of normal data and abnormal data, anomaly detection can be performed without defining normal values and abnormal values from the result of network measurement.

I used several measured values on the network layer measurement for decision. I measured the average value of 10 times ping from IPv4 default

router (hereinafter, this is called v4rtt_router_ave) and the standard deviation value of 10 times ping from IPv4 default router (hereinafter, this is called v4rtt_router_dev) was selected as the measurement results.

A correlation was found between v4rtt_router_ave and v4rtt_router_dev, but no anomaly could be detected in Local Outlier Factor. For Change Finder, an anomaly detection was successful in both v4rtt_router_ave and v4rtt_router_dev. However, Change Finder is not good at data with large jitter, in this case, the precision of anomaly detection was improved by performing preprocessing. In addition, the result of anomaly detection was evaluation using F-measure.

In this paper, I have demonstrated my proposed network anomaly detection using sensor devices, setting sensor devices on the user side, abnormality due to load change point in the wireless LAN environment was detected by preprocessing v4rtt_router_ave and v4rtt_router_dev from Change Finder.