Sensor Netw Data Commun 2015, 3:2
http://dx.doi.org/10.4172/2090-4886.C1.003

OMICS International
conferenceseries.com

International Conference and Business Expo on
Wireless Communication & Network
September 21-23, 2015 Baltimore, USA

An online-based approach for detecting connectivity anomaly in 802.11 networks

Dossa M Massa
The Institute of Finance Management (IFM), Tanzania

Wireless 802.11 networks are a popular technology that offers inexpensive ubiquitous access to the Internet in campuses, enterprises, homes, coffee shops, airports, and other public places. Their wide-scale adoption has brought great convenience to many people, giving them anytime and anywhere access to the Internet. As a result, people are becoming more and more dependent on these networks and are increasingly demanding reliability and high performance when connecting to the Internet through them. The task of diagnosing and fixing connectivity problems using online analysis of 802.11 network usage data is one of the key challenges that campus and corporate 802.11 network administrator's confront. This paper proposes an online method for detection of 802.11 Access Point (AP) abrupt ending of connections that happen when a large number of sessions in the same Access Point (AP) end within the same second window. Complex event processing techniques are employed to detect abrupt ending events and their associated anomaly-related patterns in real-time based on the collected 802.11 network usage data. Patterns such as AP interferences, across AP vicinity interferences, AP persistent interferences, AP overload, and AP crash are adequately detected and characterized.

mmohamed@inesctec.pt

RCIDSs for wireless mesh networks

K Ganesh Reddy
Shri Vishnu Engineering College for Women, India

Single-layer intrusion detection systems (SIDSs) consider only layer-independent parameters to isolate the various attacks in wireless mesh networks (WMNs). SIDSs generally use predefined measures such as maximum distance, hop count or round-trip time (RTT) etc, of any two communication nodes to isolate the attacks. The predefined measures of SIDSs lead to more false alarms being triggered, since these measures are not considering the behavior of the path/node when actual data packets are being forwarded. To overcome this problem, researchers have come up with behavior-based SIDSs. Behavior-based SIDSs consider layer-independent parameters to analyze the node/path behavior in WMNs, which is volatile in nature. Hence, SIDSs need layer-dependent parameters to reduce false alarms. Cross-layer intrusion detection systems (CIDSs) consider multilayer interactions to analyze the anomalies. CIDSs receive more attention because of their comprehensive ability to judge the anomalies in WMNs. However, CIDSs also suffer from false alarms due to misdetection of failure of a node/path as a malicious node/path. Reputation mechanisms empower the CIDSs by varying the reputation value of a node/path in the network. Existing reputation based IDSs do not consider the cross-layer parameters; instead they only consider the single layer parameters. Thus, researches have wide scope to develop the reputation based cross-layer intrusion detection systems (RCIDSs) in WMNs.

guncity11@gmail.com