ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΑΡΟΥΣΙΑΣΗ / ΕΞΕΤΑΣΗ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Μηλολιδάκης Αλέξανδρος
Μεταπτυχιακός Φοιτητής

Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
Επόπτης Μεταπτ. Εργασίας: Επικ. Καθηγητής, Χ. Δημητρόπουλος

Τρίτη, 27/03/2018, 14:00
Αίθουσα B108,Τμήμα Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης

“ Ανίχνευση Ανωμαλιών Κίνησης Δεδομένων σε Εγκαταστάσεις Σύζευξης ”

ΠΕΡΙΛΗΨΗ

Τα Internet eXchange Points (IXPs) είναι ζωτικά μέρη της υποδομής του Internet, που στεγάζονται σε εγκαταστάσεις σύζευξης, και διευκολύνουν την ανταλλαγή τεράστιου όγκου κίνησης σε ημερήσια βάση ανάμεσα στους μεγαλύτερους παρόχους Internet. Παρέχοντας ευελιξία, προνόμια δρομολόγησης και ασφαλή χώρο στους παρόχους να εγκαταστήσουν τον εξοπλισμό τους, οι εγκαταστάσεις σύζευξης αποτελούν το ιδανικό μέρος για την ανάπτυξη νέων σχέσεων ανταλλαγής δεδομένων μεταξύ των παρευρισκόμενων Αυτόνομων Συστημάτων (ASes). Παρά την συνήθη καλή συντήρηση του εξοπλισμού, υπάρχει ο κίνδυνος για την εμφάνιση σοβαρών ανωμαλιών κίνησης μεταξύ αυτών των Συστημάτων κατά την ανταλλαγή δεδομένων μέσω των εγκαταστάσεων.

Η παρούσα μεταπτυχιακή εργασία στοχεύει στην ανίχνευση ανωμαλιών μεταξύ των εγκαταστάσεων σύζευξης και μελετάει τον αντίκτυπο στην κίνηση που διασχίζει τις εμπλεκόμενες οντότητες. Για να γίνει αυτό εφικτό, 1) χρησιμοποιούμε δεδομένα από τις εγκαταστάσεις όπου φιλοξενούνται IXPs (για παράδειγμα διευθύνσεις IP) και καθημερινές μετρήσεις traceroute μέσω της πλατφόρμας μετρήσεων του RIPE Atlas για να αναγνωρίσουμε τις εγκαταστάσεις που διασχίζει η κίνηση και 2) κάνουμε χρήση μεθόδων στατιστικής ανάλυσης για την ανίχνευση ασυνήθιστων αποκλίσεων στην καθυστέρηση και ανωμαλιών δρομολόγησης μέσω των ζεύξεων ανάμεσα στις εγκαταστάσεις αυτές.

Μέσω του συστήματός μας, αναλύσαμε το χρονικό πλαίσιο μεταξύ Μαΐου και Δεκεμβρίου 2015, ιεραρχώντας τις παρατηρούμενες ενδείξεις ανωμαλιών ώστε να εντοπίσουμε σημαντικές παρεκκλίσεις. Για περαιτέρω επικύρωση της λειτουργίας του συστήματός μας, παρουσιάζουμε τις ακόλουθες περιπτώσεις χρήσης: μια περίπτωση διακοπής λειτουργίας ενός IXP, μια περίπτωση επίθεσης DDoS και μια περίπτωση διακοπής ρεύματος σε μια εγκατάσταση σύζευξης, όπου το σύστημά μας ανίχνευσε επιτυχώς. Επιπροσθέτως, αντιστοιχήσαμε τις εγκαταστάσεις αυτές στην μητροπολιτική τους περιοχή και αποτιμήσαμε τον αντίκτυπο κάθε ένδειξης ανωμαλίας στις γειτονικές εγκαταστάσεις της ίδιας περιοχής. Τα αποτελέσματα μας επίσης υποδεικνύουν ένα χρονικό πλαίσιο μεταμεσονύκτιων ωρών όπου υπάρχει μεγάλη πιθανότητα ένδειξης ανωμαλίας, πιθανώς λόγω προγραμματισμένης συντήρησης..

Milolidakis Alexandros
M.Sc. Thesis

Computer Science Department
University of Crete
Master's Thesis Supervisor: Assistant Professor, X. Dimitropoulos

Tuesday, 27/03/2018, 14:00
Room B108, Computer Science Dept., University of Crete

“Detecting Traffic Anomalies At Colocation Facilities”

ABSTRACT

Internet eXchange Points (IXPs) as core parts of the Internet infrastructure, hosted at Colocation Facilities (Colos), facilitate the exchange of Terabytes of traffic on a daily basis by big Internet Service Providers (ISPs). Offering flexibilities, routing benefits and a safe place for operators to install their equipment, Colos provide the ideal location where new peering relations are formed. Although the equipment is usually well preserved, major traffic anomalies between Autonomous Systems (ASes) over facility peering links can take place.
This thesis aims to detect anomalies at Colos and measure the impact on traffic traversing the affected entity. To achieve this, i) we use data plane information from the facilities where IXPs are located (e.g., IP addresses), ii) we utilize daily traceroute snapshots from the RIPE Atlas measurement platform to identify the facilities the traffic goes through and iii) we use statistical

methods to detect unusual delay discrepancies and routing anomalies over the facility peering links.

Using our system, we analyzed a timeframe between May and December 2015 ranking the observed alarms to infer significant disruptions. To demonstrate our system, we present and validate three cases: an IXP outage, a DDoS attack and a power failure in a colocation facility indicating that our proposed methods are able to detect real world outages. Furthermore, we map Colos to their metropolitan area and assess the impact of each alarm in neighboring facilities of the same area. Our results also show a time window ('the hours' around midnight) that has a higher probability of triggering an alarm, possible due to planned maintenance.