UNIVERSITÀ DI PISA

Relazione progetto Gestione di Rete 2018/19

Marco Mazzei 546816
Hamza Karoui 543916

Estensione bubble charts

Si è eseguita un'estensione dello script *bubble.lua*, aggiungendo dei nuovi bubble chart utili per identificare anomalie nella rete andando a vedere gli outlier dei vari grafici.
In particolare sono stati aggiunti 4 nuovi bubble chart.
I primi 2 analizzano l'andamento della rete tramite la distribuzione di alcuni flag TCP:

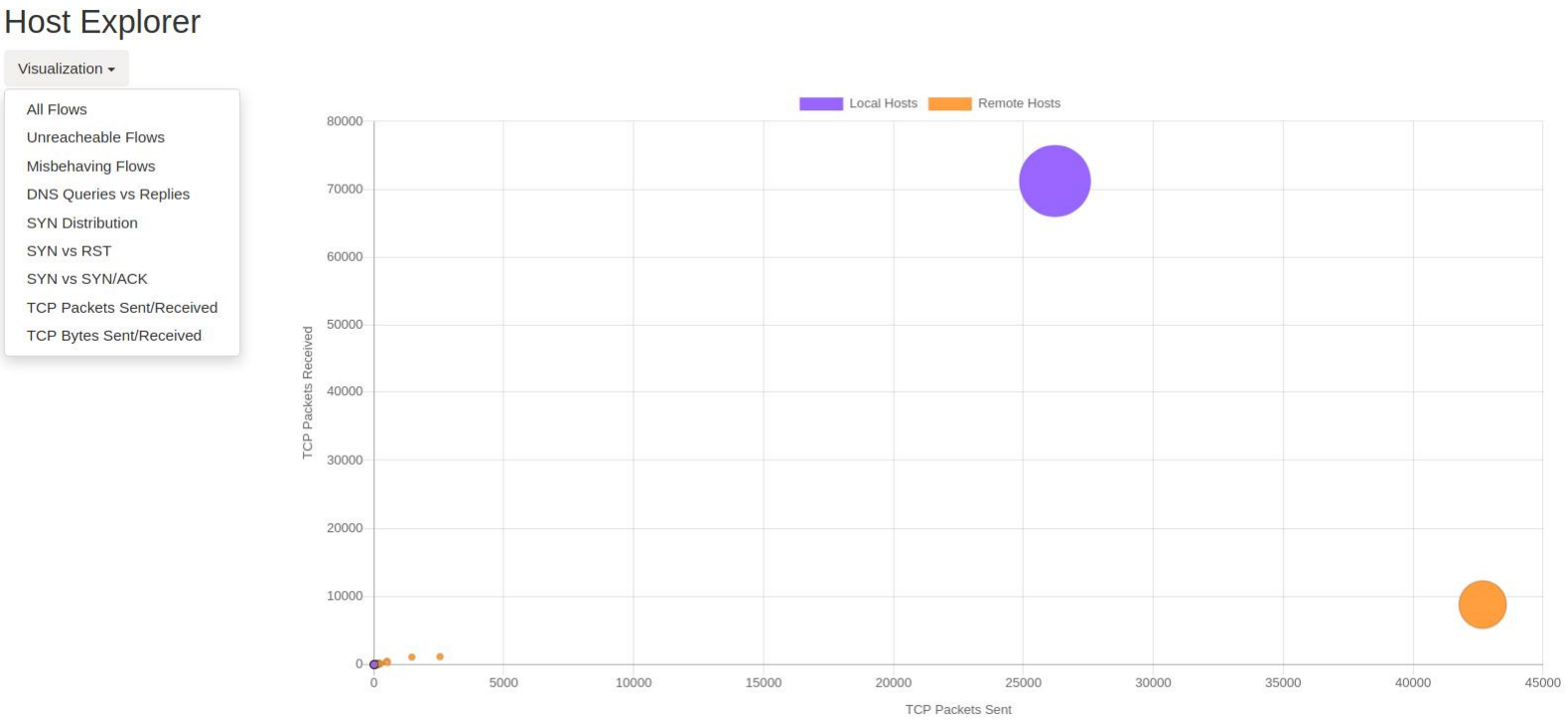
1) Mette in relazione, per ogni host, i SYN inviati con i RST ricevuti, utilizzando come raggio il numero di flussi attivi.
   Permette di identificare, tra gli outlier, comportamenti anomali e in particolare gli host che ricevono più RST dei SYN inviati. Molto spesso i RST non sono molto inferiori ai SYN, perché attualmente molte applicazioni di largo uso chiudono sistematicamente le connessioni TCP con il flag RST, perché la classica procedura di chiusura della connessione TCP (FIN, FIN-ACK) è particolarmente costosa per server di queste dimensioni.

2) Ha sull'asse delle ascisse i SYN inviati e sulle ordinate i SYN/ACK ricevuti (utilizzando ancora come raggio il numero di flussi attivi). In situazioni

normali le bolle sono centrate sulla diagonale degli assi (SYN = SYN/ACK) o molto vicine ad essa. Permette di identificare, fra gli outlier, le bolle che hanno i SYN/ACK molto inferiori rispetto ai SYN.

Gli altri 2 invece confrontano, per ogni host, il numero di pacchetti TCP inviati con quelli ricevuti e il totale dei bytes inviati con TCP con i ricevuti. In particolare:

1) Mette in relazione il numero di pacchetti TCP inviati (asse x) con il numero di pacchetti TCP ricevuti (asse y), utilizzando come raggio della bolla il traffico totale TCP in bytes (totale bytes inviati + totale bytes ricevuti), come nella seguente immagine.



2) Questo bubble chart, invece, ha sull'asse delle ascisse il totale dei bytes inviati (con TCP) e su quello delle ordinate il totale dei bytes ricevuti. Questo ovviamente permette, rispetto al precedente, di vedere più nel dettaglio le dimensioni dei pacchetti inviati e ricevuti, perché ad esempio un host potrebbe avere un numero di pacchetti inviati molto alto ma una dimensione media per pacchetto molto piccola o viceversa, e lo stesso per i ricevuti.