DoS attach on UM and impact on pings

There were SYN flood attacks on UM around March 11,2915

There is significantly higher packet loss on 6th March but I do not think it is related to the DoS attack Or at least ICT centre was not aware of it.

On other days there were periodic 7% losses every 3-3 hoursOn March 11th there were attacks for 2 hours every 6 hours, i.e. noon-2pm, 5:30-7:30pm, midnight - 3am. This went on for 3 days. At times it resulted in 80% losses and the RTT increasing up to 400-500ms.

Another point is, there are not much losses after 12th March. I checked from UM to SLAC. There are higher losses than average of 9% every 3-4 hours but again.

Data confirms something was not ok between 8th to 12th March but a little more digging into data and info is required to find out what happened afterwards. It can be a good case study. Few more things that come to my mind are:

1- May be smaller packets of ping were getting through while larger packets were being dropped? (we could not access the Internet at all)

2-Because we know it was TCP sync flood attack, can we draw more meaningful correlation between such attack and the PingER data or in general ping response?

May be Ibrahim can look into it and see if it can turn out to be a publishable work. One would need to describe the nature of the attack, the times it was observed, and how it correlates with the ping measurements.

um-dos-attack.xlsx