An entropy based analysis method of network delays for a discriminating DoS attack detection

Yann Labit, Philippe Owezarski

University of Toulouuse
LAAS-CNRS
7 avenue du Colonel Roche, 31077 Toulouse cedex 4 FRANCE
Email: {ylabit, owe}@laas.fr

***Abstract*—DoS attacks represent a big threat for the Internet. While most of attack detection techniques are based on passive monitoring of traffic, we propose a detection method based on active measurements, the objective being to make possible the real-time detection of DoS attacks, without intrusive probing. The originality of our contribution relies on the use of the entropy function computed from the time series of measured ICMP request/echo delays. However, the evaluation of the method exhibits a dramatic number of false positives. It has then been enriched by the use of the Hausdorff distance on the entropy function, which significantly improves it. In addition, a short improvement is presented to discriminate ICMP attacks from others (TCP/UDP attacks) using *icmp_seq*. Experiments for evaluating the effectiveness of the approach have been run on the French operational RENATER network, on which artificial attacks have been generated using TFN2K. Results exhibit that TCP, UDP and ICMP DoS attacks have been accurately detected in less than 1 second.**

Keywords: DoS attack detection, active measurements, entropy, Hausdorff distance.

I. Motivation

DoS attacks represent a big threat for the Internet, and their detection and mitigation is a key research issue. Most of previous work on attack detection has been concentrating on monitoring traffic using passive measurement techniques, as in Intrusion Detection Systems. This paper proposes an alternative approach based on active measurements, the objective being to make possible the real-time detection of DoS flooding attacks, without intrusive probing. It relies on the assumption that delays will be impacted in case of attack. The advantage of active measurement is its user oriented nature which allows anybody to cope with DoS attack detection (whereas it is usually devoted to network administrators). The end to end approach of active measurements also makes possible to detect attacks anywhere in the Internet from any source. Active measurements would then significantly ease the design of a global attack detection system for the Internet.

Active measurements are very popular in the Internet for measuring delays, loss rates, inferring network topologies, etc. They are also used for estimating available bandwidth (see tools as Abing, Spruce, Pathload, IGI-PTR, Pathchirp, etc). As for our attack detection method, these tools aims at interpreting delay variations on pairs or trains of packets as changes in the link or path load [1]. Our method then relies on analyzing time series of measured ICMP request/echo delays. The originality of this method relies on how this time series are computed in order to exhibit anomalous values corresponding to DoS flooding attacks. For this purpose, and taking advantage of previous work on anomaly (passive) detection which demonstrated the benefits of spectral [2] or entropy [3] analysis, our detection method also computes the entropy from the RTT time series. However, first results when working on the entropy function only were not convincing, because of a high rate of false positives. The methodology has been extended by the use of the Hausdorff distance on the entropy function, which proved to significantly reduce this level of false positives.

Section 2 describes and motivates this methodology. Section 3 presents how our detection method has been assessed. Especially, it indicates how RTT time series in the presence of attacks have been built. Then, experimenting our detection method on this RTT time series repository, it has been possible to show that thanks to the Hausdorff distance estimations on entropy functions, DoS attacks have been accurately detected in less than 1 second. Section 4 presents the meaning of discriminating ICMP attacks from others. Finally, section 5 concludes the paper by describing ongoing and future work for improving and validating this method.

II. Entropy based detection system

Before presenting the detection method, let's introduce the entropy and Hausdorff distance.

- **Entropy:** Entropy aims at measuring the randomness degree of various random experiments. The use of entropy concept is motivated in this work by the need to estimate the disorder level in RTT time series.
- **Hausdorff distance:** The Hausdorff distance measures how far two compact non-empty subsets of a metric space are from each other, in topology. In this work, this distance is used to determine the degree of resemblance between two probe sequences. The use of Hausdorff distance is also motivated by its capability of describing fractal or self-similar objects [4], as it has been exhibited that traffic as well as other Internet objects have multi-fractal and self-similar properties ([5], [6], [7]).

Let's now present the entropy based detection algorithm.

• **Step 1: ICMP probing:** RTT is measured as the ICMP request/echo delays. Different packet lengths can be selected, as well as the period between the sending of two successive probes (between 200 and 1000ms).

• **Step 2: Entropy Calculus**: Computing the entropy function on the delay time series in our method requires to fix two parameters: the sliding window W_s and the overlapping parameter O_p.

– The sliding window W_s is the granularity for analyzing the RTT time series. The longer the sliding window, the more precise the results, the less reactive the intrusion detection.

– The overlapping parameter O_p allows shifting the sliding window W_s from part or the full studied interval. It allows an overlapping between to consecutive sliding windows $W_s(k-1)$ and $W_s(k)$, $k \in \mathbb{N}$.

• **Step 3: Hausdorff distance estimation:** The Hausdorff metric is applied to a subset of delay time series according to (W_s, O_p). The level of intrusion is "filtered" thanks to the combination between entropy and Hausdorff distance.

III. A discriminating DoS attack process: ICMP vs TCP/UDP attacks

The second original pattern of this work is based on discriminating of the Dos attack. Attacks are generated by tools which used one or several protocols: ICMP, TCP or UDP. As it is previously said, RTT is measured as the ICMP request/echo delays. We observed that an attack based on ICMP protocol uses a high level of *icmp_seq*. From the other side, TCP and UDP protocol based attacks use a low level of *icmp_seq*. Thanks to the ICMP probing techniques, one can discriminate ICMP attacks from others.

IV. Traces for the methodology assessment

Assessing the accuracy and performance of our detection method requires RTT time series measured while attacks arise. Unfortunately, hackers do not warn us when they launch an attack, and as far as we know, such public repository of RTT times series in the presence of attacks does not exist. We then decided to generate ourselves our own attacks on the French operational Renater network.

The Denial of Service attacks were launched using the TFN2K attacking tool. The attacker in Mont-de-Marsan sent different DoS attacks to LAAS in Toulouse. DoS attacks have been sent with different profiles ("ramp burst", "flat burst" and "mixed burst") and different protocols (UDP, TCP, ICMP). In parallel of the attacks, an ICMP ping probing was sent out periodically.

A set of these different kinds of attacks with different intensities were launched: it allows the assessment of our detection method for cases ranging from high intensity attacks increasing seriously delays, to low intensity ones, which have more limited impact. Detecting low intensity attacks which could be part of large distributed DoS is one of the challenges for any attack detection methods, and has been the core of our assessment work.

V. Results and Analysis

A. Detection

Because of space limitation, only two sorts of attack scenarios are presented: the "ramp" and "flat" burst attacks. Figures 1.(a) (resp.(c)) and 2 .(b) (resp. (d)) present the results on a "ramp" (resp. "flat") example when analyzed with two different sets of parameters (W_s, O_p):= $\{(10s, 16\%), (10s, 50\%)\}$ respectively. For each Figure **??**.(x) $(x = a, b, c, d)$, top curve represents the ICMP RTT measured (which by the way confirms our starting hypothesis on the impact of attacks on delays), middle curve the detection alarms when applying the entropy function only on RTT time series, and bottom curve the detection alarms when combining Hausdorff distance and entropy.

In all cases, the use of the entropy functions only leads to several false alarms: 6 and 1 respectively for figures **??**.(a) and (b) corresponding to "ramp" bursts. The number of false alarms in case of "flat" burst is significantly high, exhibiting a serious lack of the entropy only detection method. Note also that increasing the overlapping factor makes the false positive rate significantly better. At the opposite, in the four cases (as well as in all tested cases), combining the Hausdorff distance with the entropy function on RTT time series leads to perfect detection results without false alarms.

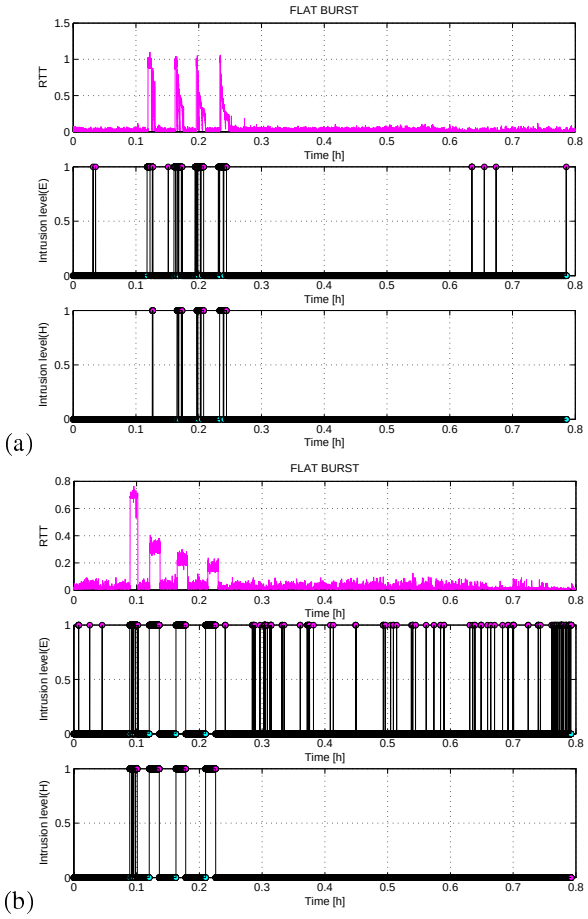

Figure 1. Ramp bursts: Intrusion levels for (W_s, O_p):= $\{(10s, 16\%)$ (a), $(10s, 50\%)$ (b).

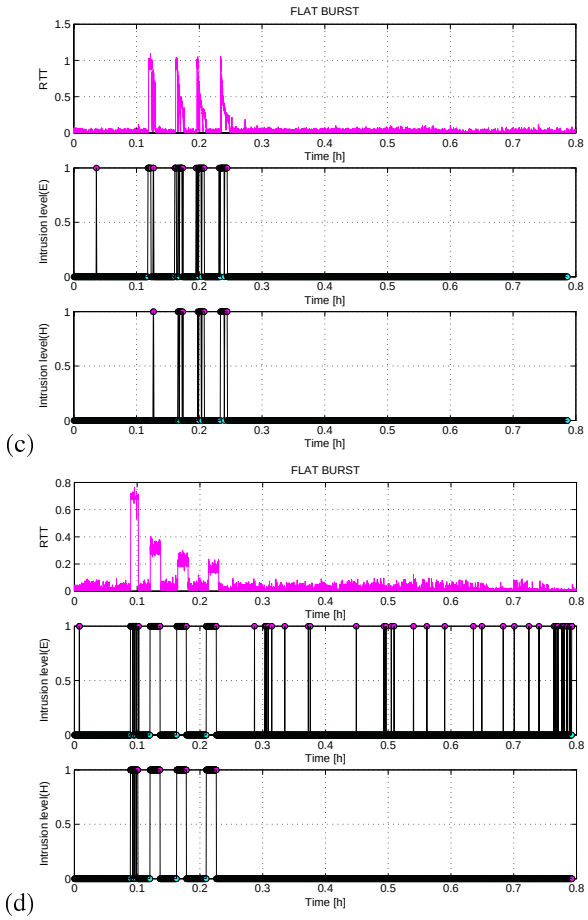

Figure 2. Flat bursts: Intrusion levels for (W_s, O_p):= $\{(5s, 16\%)$ (c), $(5s, 50\%)$ (d)$\}$.

B. ICMP vs TCP/UDP attack identification

Let's have a complete scenario of an attack: DoS attacks have been sent with different profiles ("ramp burst", "flat burst" and "mixed burst") with different protocols (UDP, TCP, ICMP). This is illustrated in the figure 3: This attack was done March 2007, 21, with TFN2K. The attacker in Mont-de-Marsan sent different DoS attacks to LAAS in Toulouse using three zombies (one zombie per protocol).

The figure 4 describes the level of *icmp_seq* utilization. The different evolution are subtracted to a normal *icmp_seq* evolution (*icmp_seq*$= 1, 2, 3, \ldots$).

by this way, it's clearly evident to discriminate the ICMP attack from the others and eliminate false positives if it is necessary.

VI. Conclusion

This paper proposed a method for detecting DoS attacks, in real time, using active measurements of ICMP RTT, and an original analysis method of the related RTT time series combining the use of entropy and Hausdorff distance. In addition, a short improvement is done to discriminate ICMP attacks from others (TCP/UDP attacks) using *icmp_seq*. The evaluation of the method demonstrated perfect detection results. Future work includes more extensive experiments with other DoS attacks,

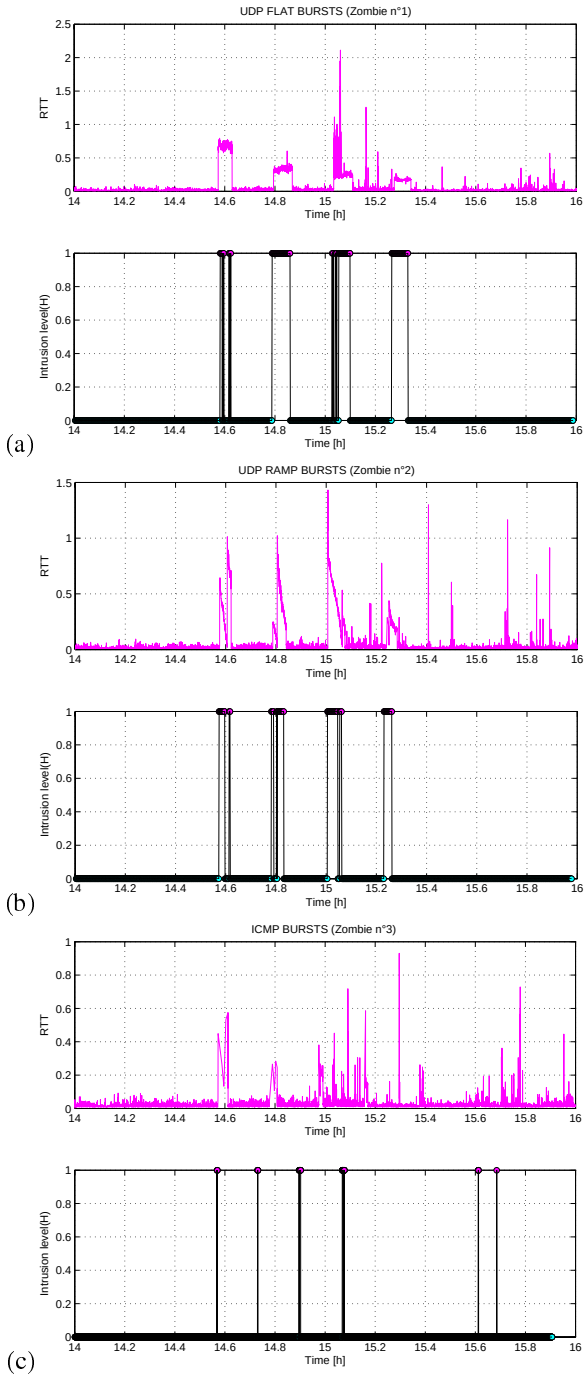

Figure 3. Intrusion levels for the 3 zombies.

but also with other kinds of anomalies. If we notice that the method detects legitimate anomalies as DoS attacks, it will be improved to make it able to differentiate legitime anomalies from DoS attacks.

References

[1] R. Prasad, C. Dovrolis, M. Murray, and K. Claffy, "Bandwidth estimation: metrics, measurement techniques, and tools," *IEEE Network*, pp. 27–35, 2003.

[2] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in *SIGCOMM'03*, Karlsruhe, Germany, August 25-29, 2003, pp. 99–110.

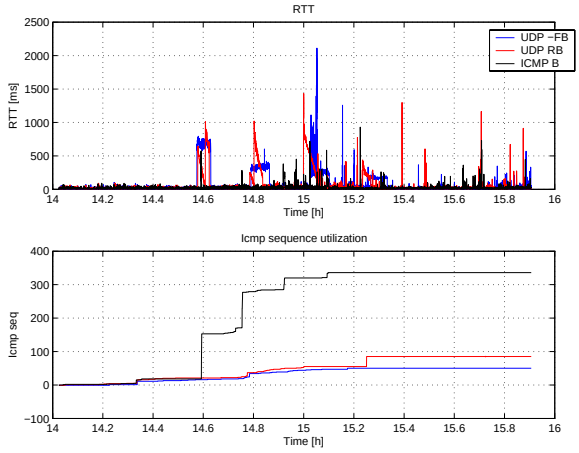

Figure 4. Identification of ICMP attack using *icmp_seq* utilization.

[3] Y. Gu, A. McCallum, and D. Towsley, "Detecting anomalies in network traffic using maximum entropy estimation," in *IM'2005*, Berkeley, CA, USA, October 19-21, 2005, pp. 345–350.

[4] T. Bedford, "Hausdorff dimension and box dimension in self-similar sets," 1988, pp. 17–26.

[5] D. Chakraborty, A. Ashir, T. Suganuma, G. M. Keeni, T. K. Roy, and N. Shiratori, "Self-similar and fractal nature of internet traffic," *Int. J. Netw. Manag.*, vol. 14, no. 2, pp. 119–129, 2004.

[6] W. W. W. E. Leland, M. S. Taqqu and D. V. Wilson, "On the self-similar nature of ethernet traffic," in *IEEE/ACM Transactions on Networking*, Feb, 1994, pp. 1–15.

[7] W. W. M. S. Taqqu, V. Teverovsky, "Is network traffic self-similar or multifractal?" in *Fractals*, vol. 5:63, 1997.