Entropy Based Detection of DDoS Attacks in Packet Switching Network Models

Anna T. Lawniczak[1], Hao Wu[1], and Bruno Di Stefano[2]

[1] Department of Mathematics and Statistics, University of Guelph,
Guelph, Ontario N1G 2W1, Canada
alawnicz@uoguelph.ca, wuh@uoguelph.ca
[2] Nuptek Systems Ltd.,
Toronto, Ontario M5R 3M6, Canada
nuptek@sympatico.ca, b.distefano@ieee.org

Abstract. Distributed denial-of-service (DDoS) attacks are network-wide attacks that cannot be detected or stopped easily. They affect "natural" spatio-temporal packet traffic patterns, i.e. "natural distributions" of packets passing through the routers. Thus, they affect "natural" information entropy profiles, a sort of "fingerprints", of normal packet traffic. We study if by monitoring information entropy of packet traffic through selected routers one may detect DDoS attacks or anomalous packet traffic in packet switching network (PSN) models. Our simulations show that the considered DDoS attacks of "ping" type cause shifts in information entropy profiles of packet traffic monitored even at small sets of routers and that it is easier to detect these shifts if static routing is used instead of dynamic routing. Thus, network-wide monitoring of information entropy of packet traffic at properly selected routers may provide means for detecting DDoS attacks and other anomalous packet traffics.

Keywords: distributed denial of service attack, packet switching network, entropy.

1 Introduction

The packet switching technology was conceived by Paul Baran as a way to communicate in the aftermath of a nuclear attack, as a sort of resilient command and control network [1]. Fortunately, no implementation of packet switching network has ever had to undergo the test of its ability to withstand a nuclear attack. However, the Internet, one of the best known applications of packet switching technology, is constantly under attacks of different types, e.g.: intrusion, packet tapping, phishing, computer worms, computer viruses, denial of service (DoS) attack, and many others. Purpose and scope of these attacks are different, ranging from the commercial to the political domain, and often they serve only the self actualization of the perpetrators.

The most common implementation of DoS is the distributed DoS (DDoS) attack. The attack is "distributed" because the attacker carries on his/her actions by means of multiple computers, located at various network nodes, and called "zombies", almost

J. Zhou (Ed.): Complex 2009, Part II, LNICST 5, pp. 1810 – 1822, 2009.

always controlled in a covert and surreptitious way without any knowledge of their legitimate owners. We focus on the type of DDoS attack directing a huge number of "ping" requests to the target victim of the attack, [2] and [3]. In this type of attack, the target (victim) machine becomes saturated with external communications requests, being pounded by spurious packets, so that it becomes effectively unavailable to legitimate traffic. The Mafiaboy attacks of February 2000 against Amazon, eBay and other big sites are an example of this type of attacks. They caused millions of dollars damage and they are often quoted by computer experts, [4] and [5].

DDoS attacks are network-wide attacks. Thus, they cannot be detected or stopped easily. To detect them packets headers, packets aggregate flows, and/or correlations are analysed with the aim of distinguishing normal traffic from the attack traffic. Often packet traffic is analysed near the victim or near the attack sources [6]. However, in many DDoS attacks packets are "normal-looking" and the existing methods are not accurate enough to distinguish between normal and attack packets. For early detection of DDoS flooding attacks Yuan and Mills [6] proposed to study spatio-temporal correlations of packet traffic monitored at a number of observation points in a network for the purpose of detecting shifts in spatio-temporal patterns of packet traffic. They have demonstrated that given a sufficient number of observation points one can infer a shift in packet traffic patterns for larger areas outside the observation routers, [6]. Thus, by monitoring macroscopic network-wide shifts in spatio-temporal patterns of packet traffic one may discover when a more detailed analysis is needed to detect potential DDoS attack.

DDoS attacks are purposely created by humans. Thus, they must affect the natural "randomness" and "natural structure and order" of packet traffic under normal conditions [7]. In turn they must affect the "natural" information entropy profiles of "normal" packet traffic and cause shifts in these profiles, [7] and [8]. We study if these shifts may be detected by calculating entropy of packet traffic monitored at a small number of selected routers. For each set of monitored routers we establish first a baseline i.e. a profile of entropy of packet traffic under normal conditions, called a "fingerprint", and study how it is affected by DDoS attacks. If the values of entropy of packet traffic sharply decrease from the "fingerprint" profile shortly after a start of DDoS attack, this means with certainty presence of an infrequent event, i.e. an emerging anomaly in packet traffic [8]. In our simulations these anomalies are caused by "ping" DDoS attacks. Our simulations show that for small sets of properly selected monitoring routers the entropy profiles of packet traffic passing through them detect onsets of "ping" DDoS attacks in our virtual experiments and that these profiles are qualitatively similar to the network-wide entropy profiles. Also, that it is easier to detect DDoS attacks when a static routing is used instead of dynamic routing. Our study shows that information entropy provides promising tool to detect DDoS attacks.

The paper is organized as follows. First, we briefly describe our existing abstraction of PSN ([9], [10]), its C++ simulator, Netzwerk ([11], [12]), and explain how they have been customized to model a "ping" type DDoS attacks. Next, we introduce definition of entropy functions used by us in detection of DDoS attacks in our virtual experiments. We present selected simulation results and our conclusions.

2 PSN Model and Its DDoS Attack Customization

Our PSN model ([9] and [10]) is an abstraction of the Network Layer of the 7-Layer OSI Reference Model [13] and like in real networks is concerned primarily with packets and their routings; it is scalable, distributed in space, and time discrete. It avoids the overhead of protocol details present in many PSN simulators designed with different aims in mind than study of macroscopic network-wide dynamics of packet traffic flow and congestion. We view a PSN connection topology as a weighted directed multigraph $\boldsymbol{L}$ where each node corresponds to a vertex and each communication link is represented by a pair of parallel edges oriented in opposite directions. In each PSN model setup all edge costs are computed using the same type of *edge cost function* (*ecf*) that is either the *ecf* called *ONE* (ONE), or *QueueSize* (QS), or *QueueSizePlusOne* (QSPO). The *ecf* ONE assigns a value of "one" to all edges in the lattice $\boldsymbol{L}$. Since this value does not change during the course of a simulation this results in a *static routing*. The *ecf* QS assigns to each edge in the lattice $\boldsymbol{L}$ a value equal to the length of the outgoing queue at the node from which the edge originates. The *ecf* QSPO assigns a value that is the sum of a constant "one" plus the length of the outgoing queue at the node from which the edge originates. The routing decisions made using *ecf* QS or QSPO rely on the current state of the network simulation. They imply *adaptive* or *dynamic routing* where packets have the ability to avoid congested nodes during the PSN model simulation. In our PSN model, each packet is transmitted via routers from its source to its destination according to the routing decisions made independently at each router and based on a *minimum least-cost criterion* of selecting a *shortest path* from a packet current node to its destination. This results in the *minimum hop routing* (*minimum route distance*) if the PSN model is setup with *ecf* ONE and the *minimum route length* if it is setup with *ecf* QS or QSPO. Since *ecf* QS and QSOP are dynamic functions, it is important to notice, that in the case of PSN model setup with *ecf* QS or QSPO each packet is forwarded from its current node to the next one belonging to a least cost shortest path from a packet current node to its destination at this time. The PSN model uses *full-table routing*, that is, each node maintains a routing table of least path cost estimates from itself to every other node in the network. The routing tables are updated at each time step when the *ecf* QS or QSPO is used, see [9], [10]. They do not need to be updated for the static *ecf* ONE, because the values of this *ecf* do not change over time, see [9] and [10]. We update the routing tables using distributed routing table updates algorithm [10].

In our simulations to study DDoS attacks we use a version of PSN model in which each node performs the functions of *host* and *router* and maintains one incoming and one outgoing queue which is of unlimited length and operates according to a first-in, first-out policy, see [10] for other options. At each node, independently of the other nodes, packets are created randomly with probability λ called *source load*. In our PSN model all messages are restricted to one packet carrying time of creation, destination address, and number of hops taken.

In the PSN model time is discrete and we observe its state at the discrete times $k = 0, 1, 2, \ldots, T$, where T is the final simulation time. At time $k = 0$, the setup of the PSN model is initialized with empty queues and the routing tables are computed. The time discrete, synchronous and spatially distributed PSN model algorithm consists of the sequence of five operations advancing the simulation time from k to $k + 1$. These

operations are: (1) *Update routing tables*, (2) *Create and route packets*, (3) *Process incoming queue*, (4) *Evaluate network state*, (5) *Update simulation time*. The detailed description of this algorithm is provided in [10].

To study DDoS attacks we modified the above described PSN model to allow modeling a PSN containing one victim computer and a user defined number of zombies either located at specified nodes or located at random. Start and end of attack time can be specified separately for each zombie. As in most real life cases, zombies continue to carry on their normal jobs during the attack, i.e. they act also as sources, destinations, and routers of legitimate data transfers. However, each zombie also sends a packet to the victim at each time step of the simulation.

3 Entropy Functions

We calculate entropy of packet traffic passing through monitored routers/nodes of PSN model as follows [8]. Let M be a set of N monitored routers. The set M may include all network routers except zombies and the victim. We index all routers in the set M by the parameter i (i.e., i = 1, …, N). We denote by q(i,k) a number of packets at the outgoing queue of a router i at time k. At each time k we calculate probability density function p(i,k) of packets queuing at a router i of the set M as follows

$$p(i,k) = q(i,k)/ \sum_{i=1}^{N} q(i,k).$$

We calculate entropy function of packet traffic monitored at routers of the set M as

$$H(M, k) = - \sum_{i=1}^{N} p(i,k)\log p(i,k),$$

using convention that if p(i,k) = 0, then p(i,k)logp(i,k) = 0.

4 Virtual Experiment Setups of DDoS Attacks

To study entropy based detection of DDoS attacks we carried out simulations for PSN model setups with network connection topology isomorphic to $\boldsymbol{L}^p_{\square}(37)$ (i.e., periodic square lattice with 37 nodes in the horizontal and vertical directions) and each of the *ecf* ONE, QS and QSPO. Thus, we considered PSN model setups $\boldsymbol{L}^p_{\square}(37, ecf, \lambda)$, where *ecf* = ONE, or QS, or QSPO, and λ is a value of *source load* that the network is operating under normal conditions. We studied DDoS attacks when *source load* value λ = 0.040. At this value each PSN model setup is free of any congestion, i.e. is in its free flow state. The *critical source load* value λ_c , i.e. the phase transition point from free flow to congested network state, for each of the considered PSN model setups is as follows: $\lambda_c = 0.053$ for $\boldsymbol{L}^p_{\square}(37, ONE)$, and $\lambda_c = 0.054$ for $\boldsymbol{L}^p_{\square}(37, QS)$ and $\boldsymbol{L}^p_{\square}(37, QSPO)$. Since each simulation of a PSN model setup starts always with empty queues, all DDoS attacks started after the initial transient time, i.e. when the network was operating already in its normal steady state for some time. All DDoS attacks started at time $k_0 = 20480$ that was much larger than the transient times and lasted until the final simulation time, $T = 131072$ (the same for all PSN model setups).

We considered a series of separate DDoS attacks each characterized by a number of active attackers/zombies. In this series of attacks, while increasing number of

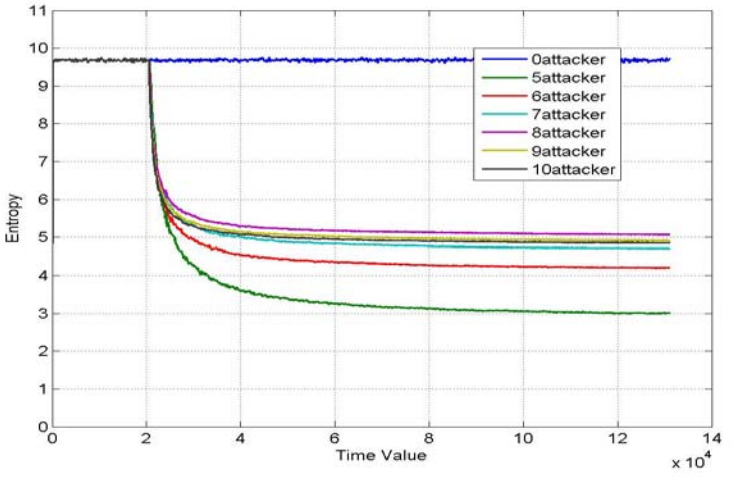
zombies we maintained always the same locations of the zombies from the DDoS attacks with their lower numbers, i.e. each time we added only new zombies to the set of the zombies from the previous attack. Additionally, in all the experiments we always maintained the same location of a victim. In this paper we present the results for the DDoS attacks with number of active attackers/zombies varying from 5 to 10, i.e. with the number of zombies varying from about 0.37% to 0.73% of the total number of nodes/routers in the network. The results of the DDoS attacks experiments with number of zombies less than 5 are discussed in [8].

For each PSN model setup operating under normal conditions (i.e., in the absence of any attack) and for each considered set M of monitored routers/nodes we calculated first entropy function $H(M,k)$. Thus, we built first a "natural" entropy function, a sort of "fingerprint" profile of the given PSN setup, characterizing normal PSN operation, i.e. normal traffic passing through the routers of the set M. Next, we calculated the entropy function $H(M,k)$ for each PSN model setup being under a DDoS attack. We calculated entropy functions $H(M,k)$ for sets M of different sizes (i.e., having different numbers of monitored routers) and for each set size we considered sets M that differ only in locations of the monitored routers. We selected locations of monitored routers randomly using different seeds of random number generator. Since we are interested in the dynamics of packet traffic passing through the routers/nodes that are not the victim or the zombies under DDoS attacks we selected the sets M in such a way that they did not include the victim and the zombies. The routers/nodes that are not the victim or the zombies/attackers are called "normal" router/nodes.

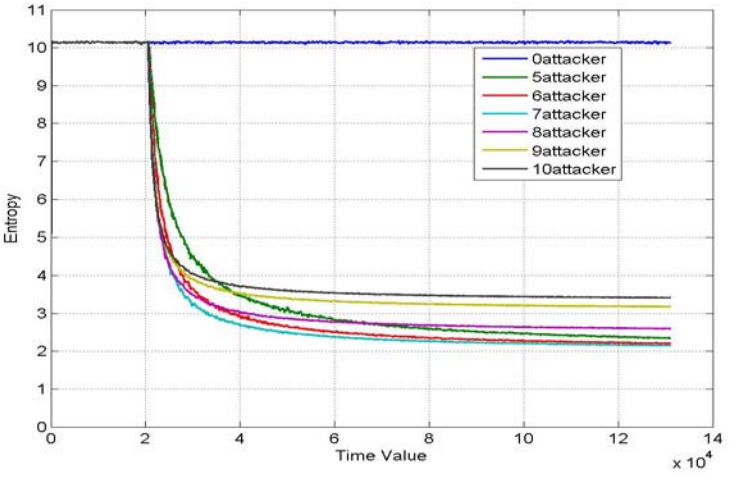
5 Entropy Based Detection of DDoS Attacks in PSN Models

Fig. 1 displays time dependent plots of "natural entropy" profiles (i.e., with 0 attackers) and of the entropy functions of packet traffic monitored at 100% of "normal" routers during DDoS attacks on PSN model with $\boldsymbol{L}^p_{\square}$(37, ONE, 0.040) setup in Fig. 1 (a) and $\boldsymbol{L}^p_{\square}$(37, QSPO, 0.040) setup in Fig. 1 (b). The colours of the plots correspond to the number of attackers, 0, and 5 to 10, and they are explained in the figure legends. We observe that the "natural entropy" profiles are almost constant functions and their values are very similar for both PSN model setups. Thus, the probability distributions of packets among the "normal" routers are similar ones when networks operate under normal conditions. As soon as each DDoS attack starts the entropy functions decrease very fast until they reach new levels at which they remain almost constant. Thus, using the entropy functions one may detect almost immediately anomalies in packet traffic because when their values sharply decrease from the "fingerprint" profiles shortly after the DDoS attacks begin this means that these functions detect with certainty the presence of an infrequent event, i.e. an emerging anomaly in packet traffic, and in our case "ping" type DDoS attacks.

The new levels that entropy functions reach are higher when the number of attackers is larger, see Fig. 1. This is because with the increase of the number of attackers the numbers of routers that become locally congested increase and their locations form patterns that are more spatially distributed in the network, in particular when the network uses *ecf* ONE. Our simulations show that the pattern of local congestion formation for the PSN model with $\boldsymbol{L}^p_{\square}$(37, ONE, 0.040) setup is different



(a)



(b)

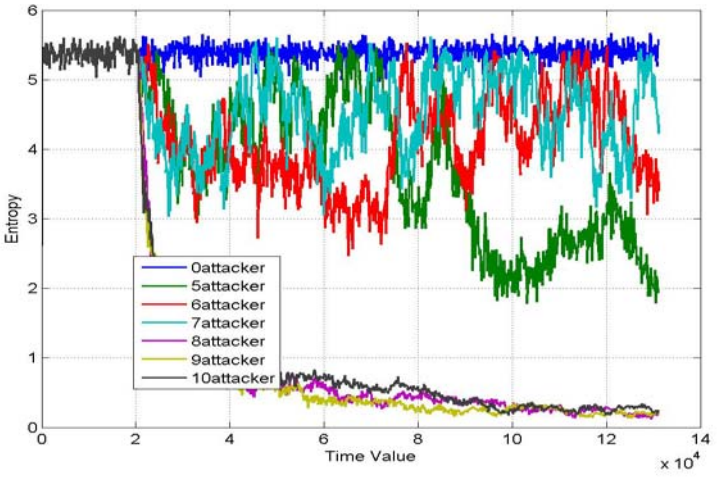
Fig. 1. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 100% of "normal routers" (i.e., all routers/nodes except the victim and the "zombies") during DDoS attacks in PSN model with $\boldsymbol{L}p_{\square}(37, \text{ONE}, 0.040)$ setup in (a) and $\boldsymbol{L}^{p}_{\square}(37, \text{QSPO}, 0.040)$ setup in (b). The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

from the one of the PSN model with setup $\boldsymbol{L}^{p}_{\square}(37, \text{QSPO}, 0.040)$ or $\boldsymbol{L}^{p}_{\square}(37, \text{QS}, 0.040)$. For the PSN model with setup $\boldsymbol{L}^{p}_{\square}(37, \text{ONE}, 0.040)$ the local congestion builds up along the shortest paths from zombies to the victim, while for the PSN model with setup $\boldsymbol{L}^{p}_{\square}(37, \text{QSPO}, 0.040)$ or $\boldsymbol{L}^{p}_{\square}(37, \text{QS}, 0.040)$ it builds up mostly around the victim. This may explain why the values of the new levels of entropy functions, i.e. when networks are under DDoS attacks, are higher for the PSN model

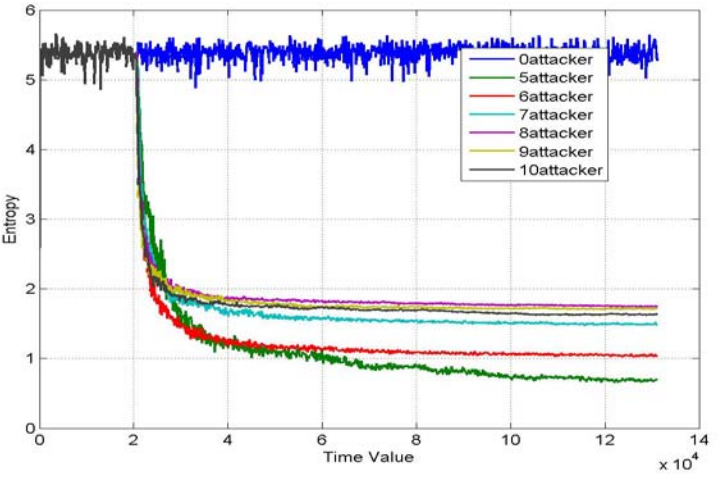
with setup $\boldsymbol{L}^{p}_{\square}$(37, ONE, 0.040) than with $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040), see Fig. 1. Additionally, when adaptive routing is used instead of the static one, packet traffic self-organizes to avoid local congestions, thus, smaller number of routers outside the closest neighbourhood of the victim experience higher local congestion in comparison with the other routers. Let us mention that the "natural entropy" profile and the corresponding entropy functions of PSN model with setup $\boldsymbol{L}^{p}_{\square}$(37, QS, 0.040) under the DDoS attacks (not shown here) are very similar to those of the PSN model with setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040). Thus, under the DDoS attacks the behaviours of packet traffics of PSN model using *ecf* QS are similar to those of the PSN model using *ecf* QSPO. From Fig. 1 we observe that the entropy functions of packet traffic monitored at 100% of all "normal" routers drop almost immediately after start of each attack. Thus, the entropy functions almost immediately detect the considered DDoS attacks. Two questions arise naturally. Will the entropy functions of packet traffic monitored at a smaller number of "normal" routers detect the DDoS attacks? Will these functions retain qualitatively the same "information" about packet traffic dynamics as the entropy functions calculated for 100% of all "normal" routers? Some answers to these questions are provided by Fig. 2 to Fig. 6.

In Fig. 2 and Fig. 3 the horizontal plots, fluctuating around constant values, correspond to the "natural entropy" profiles of packet traffic passing through 5% of all "normal" routers selected randomly with seed 1 in Fig. 2 (a) and Fig. 3 (a), and with seed 2 in Fig. 2 (b) and Fig. 3 (b). For each *ecf* type (i.e., ONE or QSPO) the behaviours of the entropy "fingerprints" are very similar to each other regardless of which seed value was used to select the set of monitoring routers. Thus, for each *ecf* type the probability distributions of packets among the routers of these two sets of monitoring routers are similar ones. Our simulations show that the entropy functions of packet traffic monitored at only 5% of all "normal" routers (i.e., at 68 routers out of 1369 routers in our model) may significantly deviate downward from their "natural profiles" almost immediately after DDoS attacks start on the networks, as can be seen from Fig. 2 (a) and (b), and Fig. 3 (b). However, from Fig. 3 (a) and (b) we see that the behaviours of the entropy functions may be influenced by the selection of the locations of the monitoring routers. On Fig. 3 (a) we see that the entropy functions corresponding to all DDoS attacks (i.e., with 5 to 10 attackers) on the PSN model with setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040) are superimposed with the respective entropy "fingerprint" plot, i.e. when number of attackers is "0". We notice on Fig. 3 (a) only some increase in the entropy functions' fluctuations during the DDoS attacks and we do not observe the sudden drop in values of the entropy functions displayed on Fig. 3 (b) that happens just after the start of the DDoS attacks.

For the PSN model setup with *ecf* QS we observed behaviours of entropy functions (not shown here) very similar to those of the PSN model setup with *ecf* QSPO. The results displayed on Fig. 2 and Fig. 3 may imply that it is easier to detect anomalous packet traffic employing the entropy functions calculated for small set of monitoring routers if the PSN model is using static routing instead of the dynamic ones. Thus, the question arises by how much one needs to enlarge the set of monitoring routers of Fig. 3 (a) to detect anomalous packet traffic. For the PSN model with the setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040) we obtained entropy functions' plots looking still similarly to those on Fig. 3 (a) when we used as a set of monitoring routers 10% of all "normal"



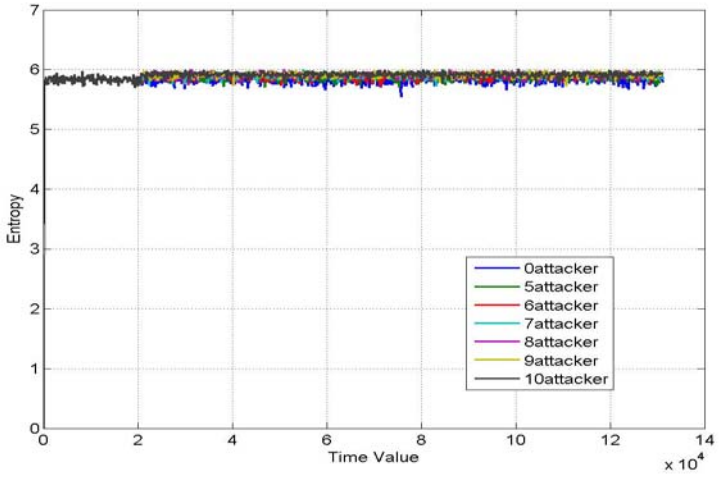
(a)



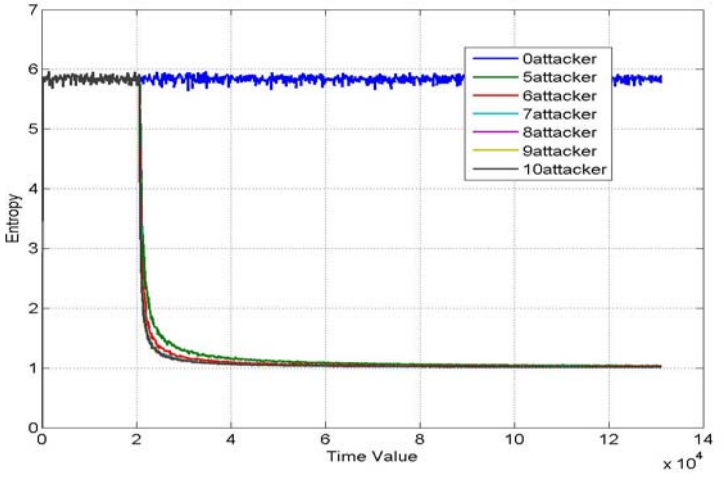
(b)

Fig. 2. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 5% of all "normal" routers randomly selected, with seed 1 in (a) and with seed 2 in (b), during DDoS attacks in PSN model with $\boldsymbol{L}^{p}_{\square}$(37, ONE, 0.040) setup. The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

routers selected randomly with seed 1. However, when we increased further the set of monitoring routers, i.e. when we used 20% of all "normal" routers selected randomly with seed 1 (in our case 274 out of 1369 routers) the values of entropy functions of packet traffic passing through these routers dropped almost immediately after start of each DDoS attack, see Fig. 4. Thus, the entropy functions detected almost immediately DDoS attacks on our PSN model with the setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040). The graphs of the entropy functions displayed on Fig. 4 are qualitatively similar to the



(a)



(b)

Fig. 3. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 5% of all "normal" routers randomly selected, with seed 1 in (a) and with seed 2 in (b), during DDoS attacks in PSN model with $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040) setup. The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

graphs of entropy functions shown on Fig. 3 (b). We see on Fig. 3 (b) that the graphs become almost constant after very short transient times. These transient times are a bit longer on Fig. 4. Furthermore, on Fig. 3 (b) the constant values are almost identical while on Fig. 4 they are slightly different. This may mean that in the case of the monitoring set of routers of Fig. 3 (b) the probability distributions of packets among

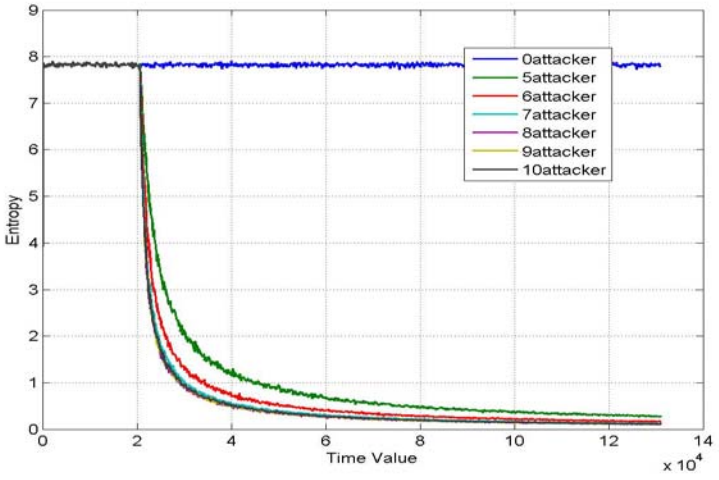
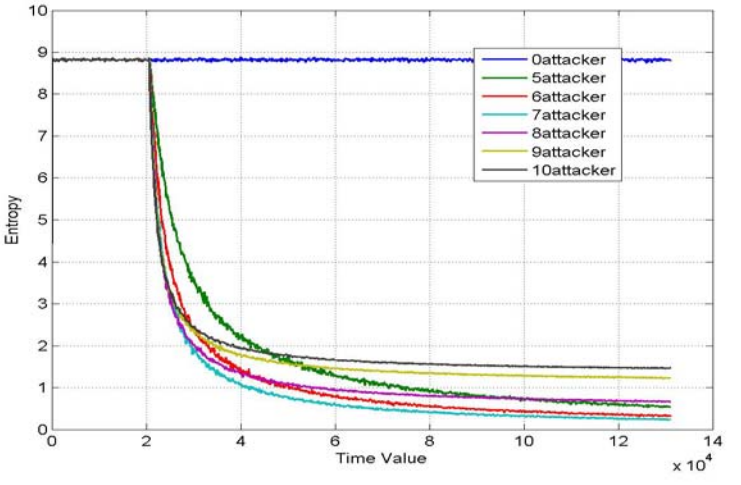
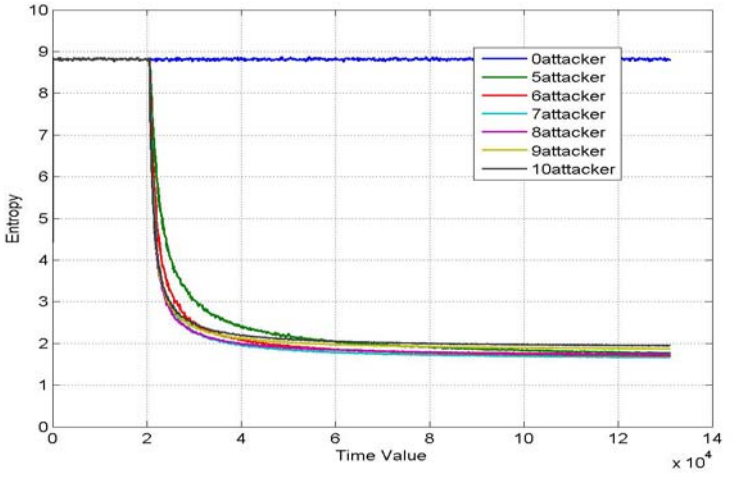


Fig. 4. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 20% of all "normal" routers randomly selected, with seed 1, during DDoS attacks in PSN model with $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040) setup. The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

these monitoring routers are very similar for all the DDoS attacks while in the case of the set of monitoring routers of Fig. 4 the probability distributions of packets among the monitoring routers slightly differ among DDoS attacks. In other words, in the first case (i.e., Fig. 3 (b) case) the monitoring routers are similarly locally congested during all DDoS attacks, while in the second case (i.e., Fig. 4 case) the local congestions of the monitoring routers slightly differ among the DDoS attacks. The differences among levels of local congestions of the monitoring routers during different DDoS attacks become more noticeable if each monitoring set consists of 40% of all "normal" routers selected randomly with seed 1 or seed 2, as can be seen from Fig. 5 (a) and (b). The graphs of entropy functions displayed on Fig. 5 (a) are qualitatively very similar to those shown of Fig. 1 (b). The entropy functions of packet traffic monitored at 100% of all "normal" routers (i.e., those displayed on Fig. 1 (b)) and those of packet traffic monitored at 40% of all "normal" routers selected randomly with seed 1 (i.e., those displayed on Fig. 5 (a)) convey very similar information about how the distributions of local congestions differ among different DDoS attacks on the PSN model with setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040). Thus, the entropy functions of packet traffic calculated for a significantly smaller set of the monitoring routers may retain qualitatively the same "information" about packet traffic dynamics as the entropy functions calculated for 100% of all "normal" routers. We obtained very similar results for the DDoS attacks on the PSN model with the setup $\boldsymbol{L}^{p}_{\square}$(37, QS, 0.040) to those with the setup $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040). In the case of DDoS attacks on the PSN model with the setup $\boldsymbol{L}^{p}_{\square}$(37, ONE, 0.040) our simulations show that the entropy functions of packet traffics monitored at 100% of all "normal" routers



(a)



(b)

Fig. 5. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 40% of all "normal" routers randomly selected, with seed 1 in (a) and with seed 2 in (b), during DDoS attacks in PSN model with $\boldsymbol{L}^{p}_{\square}$(37, QSPO, 0.040) setup. The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

(see Fig. 1 (a)) and those of packet traffic monitored at 20% of all "normal" routers selected randomly with seed 1 (see Fig. 6) are qualitatively very similar. Thus, under DDoS attacks on the PSN model using static routing the entropy functions of packet traffic monitored at smaller sets of routers than those if dynamic routings are used may retain qualitatively the same information about the packet traffic dynamics as the entropy functions calculated over 100% of all "normal" routers.

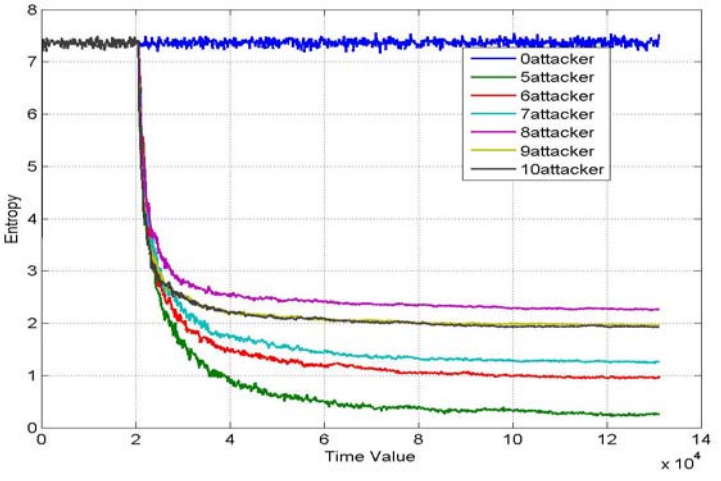


Fig. 6. Time dependent plots of "natural entropy" profile (i.e., with 0 attackers) and of entropy functions of packet traffic monitored at 20% of randomly selected, with seed 1, "normal" routers during DDoS attacks in PSN model with $\boldsymbol{L}^{p}_{\square}(37, \text{ONE}, 0.040)$ setup. The colours of the plots correspond to the number of attackers, 0, and 5 to 10 and they are explained in the figure legends. Each DDoS attack starts at $k_0 = 20480$.

6 Conclusions

Our simulations show that information entropy may detect anomalous packet traffic in data networks since such traffic changes "natural" spatio-temporal packet traffic pattern, i.e. "natural" distribution of packets among routers. We observe that the considered "ping" type DDoS attacks change "natural entropy" profiles of packet traffic monitored at properly selected small set of "normal" routers (i.e., excluding the victim and zombies). The values of entropy functions of packet traffic monitored at these sets of routers sharply decrease from the "natural entropy" profiles shortly after the beginning of each DDoS attack. This means that the entropy functions detect with certainty presence of an infrequent event, i.e. an emerging anomaly in packet traffic and in our case a DDoS attack. Our simulations show that for each set of monitored routers the plots of entropy functions of packet traffic for the PSN model setup using *ecf* QSPO and the one using *ecf* QS are qualitatively and quantitatively similar but they are different from those of the PSN model setup using *ecf* ONE. We observe that using entropy functions it is much easier to detect DDoS attacks on the PSN model using static routing than dynamic routing. The static routing does not have the ability to route packets avoiding congested network routers. Thus, congestion develops very quickly along the paths from zombies to the victim and around the victim altering "natural packet traffic" distributions and the entropy "fingerprint" profiles. For networks using dynamic routings packet traffics are more evenly distributed among the routers and it takes longer for congestion to develop, most likely, first around the victim and from there to spread out into the network. Also, we noticed that entropy functions of packet traffic monitored at properly selected small sets of "normal"

routers may retain qualitatively the same information about the packet traffic dynamics as the entropy functions calculated over 100% of all "normal" routers. In conclusion, we demonstrated that information entropy and entropy functions have the ability to detect DDoS attacks. However, several questions need to be explored further, i.e. how to select the monitored routers and how many of them so that entropy functions can reliably detect anomalous packet traffic regardless of its intensity.

Acknowledgments. The authors acknowledge the prior work of A.T. Lawniczak with A. Gerisch and the use of Sharcnet computational resources. A.T.Lawniczak acknowledges partial financial support from NSERC of Canada and H. Wu from the Univ. of Guelph.

References

1. Paul Baran and the Origins of the Internet, http://www.rand.org/about/history/baran.html
2. http://en.wikipedia.org/wiki/Ping_flood
3. http://en.wikipedia.org/wiki/Ping_of_death
4. http://www.theregister.co.uk/2002/10/23/feds_investigating_largest_ever_internet/
5. http://en.wikipedia.org/wiki/Mafiaboy#cite_note-13
6. Yuan, J., Mills, K.: Monitoring the Macroscopic Effect of DDoS Flooding Attacks. IEEE Transactions on Dependable and Secure Computing 2(4), 1–12 (2005)
7. Nucci, A., Banneman, S.: Controlled Chaos. In: IEEE Spectrum, December 2007, pp. 43–48 (2007)
8. Lawniczak, A.T., Wu, H., Di Stefano, B.: DDoS attack detection using entropy of packet traffic in CA like data communication network model. In: Adamatzky, A., et al. (eds.) Automata-2008 Theory and Applications of Cellular Automata, pp. 573–584. Luniver Press, UK (2008)
9. Lawniczak, A.T., Gerisch, A., Di Stefano, B.: Development and Performance of Cellular Automaton Model of OSI Network Layer of Packet Switching Networks. In: 16th IEEE CCECE 2003 – CCGEI 2003, vol. 2, pp. 1409–1412 (2003)
10. Lawniczak, A.T., Gerisch, A., Di Stefano, B.: OSI Network-layer Abstraction: Analysis of Simulation Dynamics and Performance Indicators. In: Mendes, J.F., et al. (eds.) AIP Conference Proc., New York, vol. 776, pp. 166–200 (2005)
11. Gerisch, A., Lawniczak, A.T., Di Stefano, B.: Building Blocks of a Simulation Environment of the OSI Network Layer of Packet Switching Networks. In: 16th IEEE CCECE 2003 – CCGEI 2003, p. 4 (2003)
12. Lawniczak, A.T., Gerisch, A., Maxie, K., Di Stefano, B.: Netzwerk: Migration of a Packet Switching Network Simulation Enviroment from MS Windows PC to Linux PC and to HPC. In: 19th International Symposium no High Performance Computing Systems and Applications, pp. 280–286. IEEE Press, Los Alamitos (2005)
13. Leon-Garcia, A., Widjaja, I.: Communication Networks: Fundamental Concepts and Key Architectures. The McGraw-Hill Companies, Inc., New York (2000)