Meaningful Attack Graph Reconstruction Through Stochastic Marking Analysis

Peppino Fazio[1], Mauro Tropea[1], Salvatore Marano[1], Miroslav Voznak[2]
[1]D.I.M.E.S. Department, University of Calabria, [2]VSB Technical University of Ostrava
[1]87036, Rende, Italy, [2]Poruba, Czech Republic
e-mail: [1]{pfazio, mtropea, marano}@dimes.unical.it, [2]miroslav.voznak@vsb.cz

Abstract— **Nowadays, the defense against Denial of Service (DoS) attacks is receiving particular interest. Different techniques have been proposed and, in particular, the Packet Marking (PM) and TraceBack (TB) procedures demonstrated a good capacity of facing the different malicious attacks. While host-based DoS attacks are more easily traced and managed, network-based DoS attacks are a more challenging threat. The powerful point of IP TB approach is the possibility given to routers to mark and add some information on attack packets, on the basis of a fixed probability value. In this paper, we propose a possible approach for modeling the classical probabilistic PM algorithms as Markov chains, giving the possibility to obtain a closed form for the evaluation of the right number of received marked packets, in order to build a meaningful attack graph.**

Index Terms— Probabilistic Packet Marking; IP TraceBack; Stochastic Process; DoS attack; Network Security.

I. INTRODUCTION

In recent years, the security has become one of the most significant issue of information technology, given its enormous practical implications and Internet, as a tool of research to universities and researchers, becomes a new medium of more pervasive communication. One of the major problem in information and communications field is the protection of confidentiality and privacy of the data. Normally, a network cannot be considered safe: in general it is possible to intercept the data in transit. All attacks that exploit a bug in the operating system or in the applications running on a network node are called “logical attacks”. These attacks are usually due to errors in programming and/or in designing of the involved programs. From a network point of view, a first remedy can be the use of an Intrusion Detection System (IDS), that is able to detect unwanted manipulations to a system [1], [2]. Regarding Distributed DoS (DDoS) attacks, two counter-measures are hardly used: one consists in mitigating the detrimental impact of the attacks on the victim, while the second one consists in trying to find out the position of the source by tracing back to the offending paths, then stopping the attacks at the source. The so-called TB approach consists into the deployment of the IP tracing technology. The studied algorithm can reduce the number of packets to be collected for reconstructing the attack path, in particular in the situation where an enormous number of counterfeit attack packets exist. In addition, it is able to identify the correct attack path and the tracing scheme uses a probability labeling approach [3].

In this paper, we propose a possible approach for modeling the classical probabilistic PM algorithms as Markov chains, giving the possibility to obtain a probabilistic closed form for the evaluation of the right number of received marked packets, in order to build a meaningful attack graph. So, the main contribution of this paper consists in giving an indication to the reader on how the minimum number of needed marked packets can be evaluated. In the next section, some important related works are surveyed and, then, different attacks are classified in detail. The structure of the following part of the paper is as follows: section II gives an overview of some of the existing works on network security issues and countermeasures, section III proposes the main TB approach based on Markov chains, while conclusions are summarized in section IV.

II. RELATED WORK

Today, the availability of hacking tool makes everyone able to improvise as hacker. Network attacks generally adopt computer networks as transportation media to convey the intrusion, or even attack the communication system itself. The attacks are based on a number of serious security flaws, inherent in the protocol design/implementation. All network attacks exploit one or more security vulnerabilities or weakness present in the TCP/IP architecture. Data security is of primary importance, both in wired and wireless networks, as demonstrated by [4], [5], [6], [7], in which the authors propose different approaches, at different ISO/OSI layers. There are many works in literature about DoS mitigation based on unconventional approaches. In [8] the authors face with the DDoS flooding attacks that try to disrupt the access to services of the users exploiting the vulnerabilities of computers inside the networks. In their paper the authors present a survey on DDoS attacks, showing attacks problems and attempting to find the right countermeasures to these issues. They highlight the needing of a comprehensive distributed and collaborative defense mechanism able to prevent and anticipate DDoS attacks. The main goal is to provide the research community a good basis for developing opportune defense mechanisms in order to prevent and detect these malicious attacks. As introduced in the previous section, another topic deeply studied by researchers is the IP Traceback technology. In [9], the authors mainly focus on security mechanisms and attacks analysis. The task of their paper is a queuing model proposal, able to perform several evaluation of DoS attacks in a computer network,

characterized by a two-dimensional embedded Markov chain model, used for developing an algorithm able to find the stationary probability distribution and other interesting performance metrics for analyzing traffic attacks. They provide an analytical approach for security, studying of networks under DoS attacks that could open new research lines in computer networks. The authors of [10] make an analysis of existing approaches to IP TB systems. They have shown the active research on this kind of topic, considering also possible attacks sent from infected hosts. Many existing works are based on efficient packet logging. They conclude their work affirming that the active security system utilizing IP TB technology could be contributed for safer and better reliable Internet environment, by effectively protecting the intentional Internet hacking. In [11] the authors propose a new mechanism able to identify and group together trace on machines in the same botnets (a number of Internet-connected nodes, communicating with other similar peers, in which components located on networked hosts communicate and coordinate their actions by "command and control" or by passing messages among them). They provide a solution to detect new botnets, thanks to very cheap and easily deployable solutions. The method has been validated through many months of collected data. Moreover, they have provided a solution for distinguishing relevant from not relevant traces. They have also shown that these botnets are able to remain active during very long periods of time. Through many experiments the authors have highlighted the goodness of considering more point of view into each process of attack. The work in [12] focuses its attention on a particular type of attack, the reflector attack, a serious kind of DoS threat. The authors propose a new scheme based on reflective algebraic marking. This scheme is composed of three different algorithms: marking, reflection and reconstruction. The proposal has been tested through simulation campaigns that have shown the high results reached by proposed approach able to trace the sources of the potential attack packets. Moreover, the goodness of proposal is confirmed by the ability of producing a very low and, then, negligible amount of false positives. In the next section, our contribution is described in detail. Given the migration to IP paradigm of many applications, e.g. IP telephony, security treats become dangerous also in digital phone networks [13-15].

III. Stochastic Processes for Traceback Modeling

As early described, the defense against the DoS attacks is receiving particular interest in recent years. Different techniques have been proposed for combating DoS attacks and, in particular, the PM and TB [16-20] procedures demonstrated a good capacity of facing those threats in an acceptable way. The powerful point of IP TB approach is the possibility, given to the network routers, to mark and add some information on attack packets, on the basis of a fixed value of probability. Assuming that we are dealing with TCP/IP stack, the information for packet marking, generally, is inserted in the Options field of the IP packets. After the receipt of a given amount of packets, the destination victim can analyze the marked data in order to build-up a structured graph, representing a way for identifying the source of the attack. Figure 1 just gives an idea of the considered scenario. The meaningfulness of the obtained graph depends on the quantity of information that is obtained by the victim, so an index should be considered (as suggested in literature, known as Savage equation [17]).

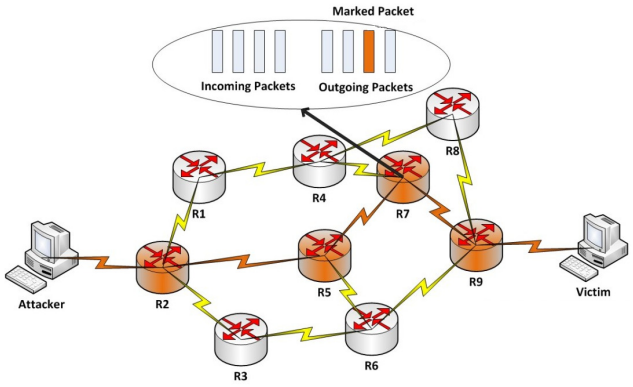

Fig. 1. An example of data exchanging with an ongoing attack (from the attacker to the victim) and packet marking approach.

A. General PM approach

The problem of that approach is represented by the validity for a single attacker, while for different simultaneous attacks it is claimed that the number of needed packets for reconstructing each path is a linear function of the number of simultaneous attacks. Not all networks have a linear topology (classic acyclic graph with a connection degree higher or equal to two), and if the linearity condition is not verified, Savage's relation tends to under-estimate the number of needed packets for the construction of the needed graph [21]. The idea proposed in [21] attracted the most attention of the whole research in this area and all the recent schemes started from it, because TB approach, as said before, allows enabled routers to mark attack packets on the basis of a predetermined probability. When the number of received packets, on the victim/receiver side, is enough, the attack graph can be determined, so the path from which the attack started can be "easily" discovered. The main issues in this field of research are: 1) The evaluation of how many packets are enough to have a concrete knowledge of the attack graph, 2) The time at which the victim can assume to have enough meaningful packets. The main aim of this work consists in modeling the PM algorithm behavior as a Discrete Markov Chain (DMC), in order to demonstrate how an alternative approach can be deployed for network security and for combating malicious attacks. Clearly, the assumption of marking capability by network routers has to be made (so, the routers are said to be PM-aware). The marking procedure has been deeply described in literature [16], [17], [22], [23], as a powerful approach for determining the source of a malicious attack. Let us consider a network *NET* composed by sending/receiving nodes and a set of routers $RS=\{R_1,...,R_m\}$, with $\|RS\|=m$. The marking information which is put inside a packet by a router represents an edge of the future graph that should be considered by the victim. The marking information is composed by three

components: *START*, *END* and *DISTANCE* [17], in addition to a pre-defined marking probability p_{mark}. When a packet *pkt* arrives into a router R_i, on the basis of p_{mark}, R_i could decide to mark "positively" the packet: in this case the *START* field is set to the IP address of R_i's interface, while the *DISTANCE* field is set to zero. If R_i decides to mark "negatively" the packet, the *END* field is set to R_i's address (if the *DISTANCE* field contains a zero value) or the *DISTANCE* field is increased by 1. Then, *pkt* is forwarded to the next hop, according to the routing table. In this way, the marked packet represents an edge of the attack graph, which will arrive to the possible victim, only if next hops will not encode it again. The *DISTANCE* field is always increased, in order to give to the victim the knowledge about the distance of the received "edge". Clearly, a received packet could not be marked, if no routers of the network decide to mark it. The marking process can terminate when there exists one marked packet for each router of the network.

B. *Markovian PM and TB Model (MPMTBM)*

We start defining the MPMTBM by giving a definition of the possible states of a Markov chain, as representing all the possible combinations of the collected marked packets by the victim, that is to say the states space $\boldsymbol{S}$ will have a cardinality of $\|\boldsymbol{S}\|=C_{m,1}+C_{m,2}+C_{m,3}+...+C_{m,m}+1$, where $C_{m,k}$ are the combinations of m elements of class k, and an additional value is considered for taking into account the case of no marked packet received (starting state). State $s_1=\varnothing$ is called beginning state (the victim starts its algorithm without the reception of any marked packet), while the state $s_{\|S\|}$ is called ending state (or absorbing state, as explained later). A markovian chain is completely described by the state set $\boldsymbol{S}$ and the transition probability matrix $\boldsymbol{M}$. For the MPMTBM, we can consider that only when the victim collects new information a transition occurs. For example, when the chain is in state $s_i=R_1$ and the victim receives a packet marked by R_2, then a transition occurs and the new state will be $s_j=R_1$-R_2. In order to define the transition probabilities matrix, the effective packet marking probability should be derived. At this point, let $p(Mark\_by\_R_i)$ be the probability of a packet to be marked by $R_i \in RS$, while $\|R_i, \text{victim}\|=d_i$ is assumed to be the minimum distance from R_i to the victim (in terms of number of hops), then:

$$p(Mark\ \_by\_R_i) = \frac{Sreach_i}{S} \cdot p_{mark}(1-p_{mark})^{d_i-1}, \quad (1)$$

where $Sreach_i$ represents the number of malicious sources which can reach R_i through attacking packets and S is the total number of sources. The marking event of R_i is independent from the marking event of R_j. Since a transition among the Markovian states occurs only if new edges are discovered by the victim, the probability of receiving unmarked packets should be not taken into account, so the expression in eq. (1) should be rewritten as:

$$p^*(Mark\_by\_R_i) = \frac{p(Mark\_by\_R_i)}{\sum_{k=1}^{m} p(Mark\_by\_R_k)}. \quad (2)$$

At this point, the elements of $\boldsymbol{M}$, indicated with $\boldsymbol{M}(s_i,s_j)$, can be defined. The exact expressions will be the following one:

$\boldsymbol{M}(\varnothing,\varnothing)=0$; $\boldsymbol{M}(\varnothing,R_1)$=p*(Marked_by_$R_1$); $\boldsymbol{M}(R_1,R_1$-$R_2)=p^*(Mark\_by\_R_2)$, ..., $\boldsymbol{M}(R_1$-R_2-...-R_k, R_1-R_2-...-$R_k,R_{k+1})$=p*($Mark\_by\_R_{k+1}$), ..., $\boldsymbol{M}(R_1$-R_2-...-R_k, R_1-R_2-...-$R_k)=\sum_{j=1}^{k} p^*(Mark\_by\_R_j)$, ..., $\boldsymbol{M}(R_1$-...-R_m,R_1-...-$R_m)$=1.

Just for clarifying the expressions of the obtained values, an example is now illustrated.

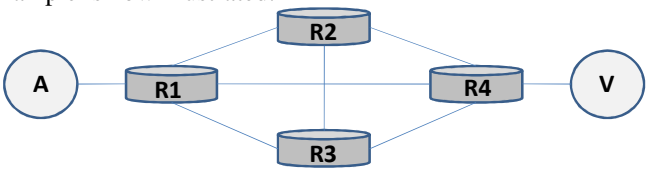

Fig. 2. A network topology with m=4.

For the network topology illustrated in figure 2, we have $RS=\{R_1, R_2, R_3, R_4\}$, m=4, $\boldsymbol{S}=\{s_1, s_2,..., s_{16}\}=\{\varnothing, R_1, R_2, R_3, R_4, R_1$-$R_2, R_1$-$R_3, R_1$-$R_4, R_2$-$R_3, R_2$-$R_4, R_3$-$R_4, R_1$-$R_2$-$R_3, R_1$-$R_3$-$R4, R_1$-$R_2$-$R_4, R2-R3-R4, R1-R2-R3-R4\}$ and $\|S\|=C4,1+C4,2+C4,3+C4,4=16$. As in the traditional schemes [17], [24], the p_{mark} value can be set to 1/m, (with m the maximum number of forwarding nodes, assuming that the shortest path is always evaluated), as in [21]. The obtained Markov chain is illustrated in figure 3. Following the definitions given in eq. (1), (2), it is easy to evaluate the elements of the transition probabilities matrix $\boldsymbol{M}$ related to the Markov chain, fixed a p_{mark}=0.33: $p(Mark\_by\_R_1)$=0.14378, $p(Mark\_by\_R_2)$=0.2178, $p(Mark\_by\_R_3)$=0.2178, $p(Mark\_by\_R_4)$=0.33. The final values are: $p^*(Mark\_by\_R_1)$=0.1581, $p^*(Mark\_by\_R_2)$=0.2395, $p^*(Mark\_by\_R_3)$=0.2395, $p^*(Mark\_by\_R_4)$=0.362881.

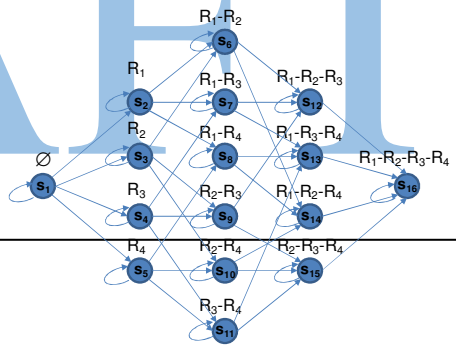

Fig. 3. The MPMTBM associated to the network in figure 2.

As known from Markov chains theory, in our case $\boldsymbol{M}^k$ ($k\geq 0$) represents the system state after the arrival of k packets and the element $\boldsymbol{M}^k(1,\|\Omega\|)$ represents the probability of the completion of the graph construction after k packets received at the victim side:

$$M^k(1,\|S\|) = \sum_{i=0}^{k} P[Pkt=i] \quad (3)$$

It can be also considered as the cumulative probability that k marked and received packets are enough to build up a meaningful attack graph. So it is easy to verify that the term in eq. (3) represents the probability that the considered system transits from state 1 to state $\|\Omega\|$ after the reception of k packets. This value represents, also, the probability that k

marked packets are enough to have a consistent attack graph. At this point, the last step to obtain a theoretical approach in evaluating the number of needed packets is to consider the absorbing property of Markov chains [25], [26]. A Markov process is said to be "absorbing" if there is at least one state s_i such that once reached, the evolution of the process never leaves it. The state s_i is called absorbing state, while all the other ones are called transient states. The proposed model is surely absorbing, given that the process does not evolve anymore, once the state $s_{|\Omega|}$ is reached. From [27], it is known that by acting a permutation of the states, the matrix $\boldsymbol{M}$ can be structured as:

$$M = \begin{bmatrix} TR & AB \\ 0 & ID \end{bmatrix} \tag{4}$$

where the sub-matrix $\boldsymbol{TR}$ is associated to the transition probabilities among transient states, $\boldsymbol{AB}$ is associated to the transition probabilities from transient to absorbing states, and $\boldsymbol{ID}$ is the identity matrix. From the markovian theory it is known that $\boldsymbol{TR}^k \to 0$ for $k \to \infty$, because the probability that the chain is not able to reach an absorbing state from a transient state s_j is the sum of the corresponding row of $\boldsymbol{TR}$, indicated as $\boldsymbol{TR}_j$. The value of $\boldsymbol{TR}_j$ is less than 1 and, for this reason, $\boldsymbol{TR}^k_j \to 0$. The direct consequence is that the individual entries of $\boldsymbol{TR}^k$ converge to 0. In the literature, the fundamental matrix is defined as:

$$F = I + TR + TR^2 + TR^3 + \ldots \tag{5}$$

and each element $\boldsymbol{F}(i,j)$ is to be intended as the expected number of times the process is in state s_j if it started in state s_i [27]. As said before, in the case of the proposed MPMTBM, the starting state is always s_1 (the potential victim starts without having received any marked packet), so the expected number of received packets for having a meaningful attack graph can be evaluated as the expected number of visits from s_1 to any transient state (each visit represents the reception of a packet), before reaching the absorbing condition, $\boldsymbol{F}(1,1)+\boldsymbol{F}(1,2)+\ldots+\boldsymbol{F}(1,|\Omega|-1)$.

IV. A Numerical Analysis

In order to show some numerical results that are derived from the proposed theoretical approach, in this section we show some trends of the main parameters which have been considered in the studied model. First of all, the transitions matrix is illustrated. We implemented a Java network simulator, by considering the main dynamics of the DoS/flooding attack. The network topology can be defined graphically. As example, we replicated the topology already depicted in figure 2. The following figures show how the values expressed in eq. (1) and eq. (2) varies for different p_{mark} values. Figure 4 shows the trend of the Independent Marking Probability (IMP) as expressed in eq. (2), that is to say the probability that an unmarked packet is received and marked by R_i, taking into account its distance from the victim.

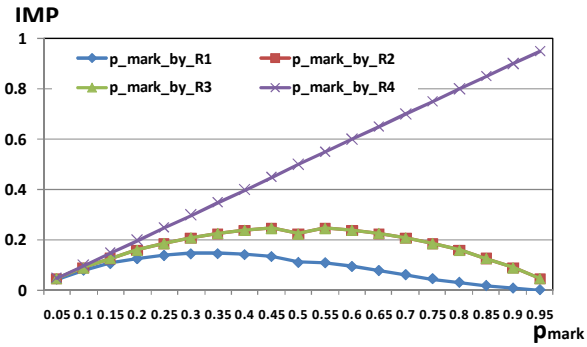

Fig. 4. The Independent Marking Probability (IPM) evaluated as in eq. (1).

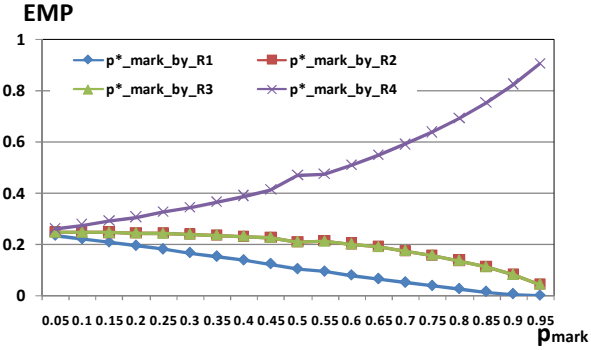

Fig. 4. The Effective Marking Probability (EPM) evaluated as in eq. (2).

It could be seen how, given a lower distance the values are higher, due to the absence (or lower probability) of other intermediate nodes which could, eventually, mark the packet. The curves for R_2 and R_3 are the same, because their distance from the victim is the same. Figure 5 (eq. (2)), instead, takes into account also the global marking probability of the other nodes, neglecting the probability of receiving unmarked packets. At this point, given the definitions of the elements $M(s_i,s_j)$ and the topology of figure 2, setting p_{mark}=0.33 (approximated to 0.35), the following $\|S\|x\|S\|$=16x16 transition probabilities matrix M is obtained (for the graphical representation, all the values are truncated to the second decimal number):

$M =$

0.00	0.16	0.24	0.24	0.37	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.00	0.16	0.00	0.00	0.00	0.24	0.24	0.37	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
0.00	0.00	0.24	0.00	0.00	0.16	0.00	0.00	0.24	0.37	0.00	0.00	0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.24	0.00	0.00	0.16	0.00	0.24	0.00	0.37	0.00	0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.00	0.37	0.00	0.00	0.16	0.00	0.24	0.24	0.00	0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.39	0.00	0.00	0.00	0.00	0.00	0.24	0.37	0.00	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.39	0.00	0.00	0.00	0.00	0.24	0.00	0.37	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.52	0.00	0.00	0.00	0.00	0.24	0.24	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.48	0.00	0.00	0.16	0.00	0.00	0.37	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.61	0.00	0.00	0.16	0.00	0.24	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.61	0.00	0.00	0.16	0.24	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.63	0.00	0.00	0.00	0.37
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.76	0.00	0.00	0.24
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.76	0.00	0.24
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.84	0.16
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00

Fig. 5. Transition Probability Matrix for the topology in figure 2 and the MTMPBM in figure 3.

It is easy to see that, in only one step, the probability of a complete attack graph construction is zero. Our simulator is

able to evaluate the element $M^k(s_1,s_{|S|})=M^k(s_1,s_{16})$ for different values of k. The next figure represents the trend of that elements, which indicates the probability that k marked packets are enough to have a meaningful attack graph. Figure 6 shows how increasing the number of received packets, the cumulative probability of k will increase too, but the trend is strictly dependent on the value of p_{mark}: higher values of p_{mark} (>0.60) lead to a sensible decrease in the obtained values of $M(s_1,s_{16})$. This effect could be thought as undesired, but for high values of p_{mark}, all the intermediate nodes tends to mark the packets more frequently, so the victim, in the same time, will receive packets marked by the same nodes, without reaching the completeness of the received information. The main works in literature about this phenomenon [17], [21] suggest to choose a value of marking probability near to $1/d_{max}$, where d_{max} is the maximum distance from the victim of all the intermediate nodes.

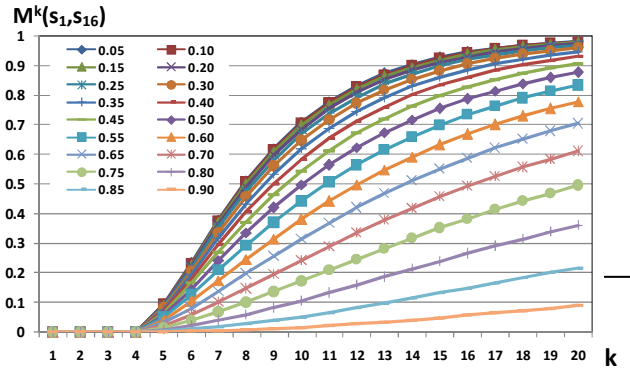

Fig. 6. Cumulative probability of having a meaningful attack graph after the reception of k marked packets (topology of fig. 2).

The same information can be analyzed by the pdf, simply evaluating the following quantity:

$$M^k(s_1,s_{16}) - M^{k-1}(s_1,s_{16}) \qquad (6)$$

that is to say, by deriving the pdf from the cumulative values, having a punctual information about the probability of having enough packets for a meaningful attack graph.

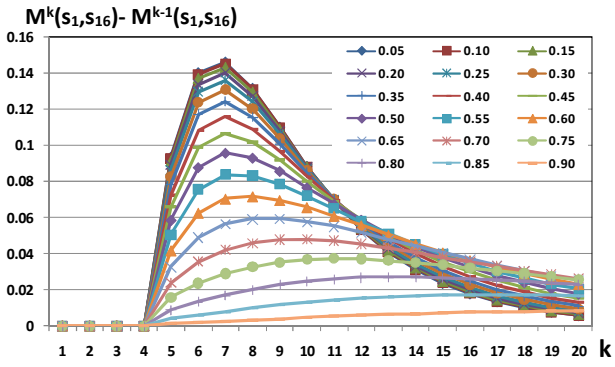

Fig. 7. Probability of having a meaningful attack graph after the reception of k marked packets (topology of fig. 2).

Figure 7 shows some obtained trends of the pdf, reflecting the same concepts of the previous figure, clearly from a punctual point of view.

V. Conclusions and Future Works

In this paper we investigated and studied a stochastic scheme for combating malicious attacks in telecommunication networks: the idea is based on the well-known traceback and packet marking approaches, with the main aim of introducing a markovian analysis about the needed packets for constructing a meaningful attack graph. The main interest is focused on the determination of the minimum number of marked packets to be collected: the victim should avoid to wait for receiving further marking information, after the necessary amount of marked packets has been received. A markovian scheme is able to give probabilistic indications about the needed number of received packets, as well as about the evolution of the model through time. Some numerical data have been provided, proving how the proposed model is able to describe the desired parameters.

References

[1] V. C. Valgenti, M. S. Kim , "Increasing Diversity in Network Intrusion Detection System Evaluation", IEEE Global Communications Conference (GLOBECOM), pp. 1-7, 2015.

[2] C. N. Kao, Y. C. Chang, N. F. Huang, I. J. Liao, R. T. Liu, H. W. Hung, C. W. Lin, "Automatic NIDS Rule Generating System for Detecting HTTP-like Malware Communication", International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), pp. 199-202, 2015.

[3] Belenky, Andrey, and Nirwan Ansari, "IP Traceback with deterministic packet marking", IEEE Communications Letters, Vol. 7, Issue 4, pp.162-164, 2003.

[4] F. De Rango, "Trust-based SAODV protocol with intrusion detection, trust management and incentive cooperation in MANETs," International Journal of Interdisciplinary Telecommunications and Networking (IJITN), vol. 1, no. 4, pp. 54–70, 2009.

[5] F. De Rango, D.C. Lentini, S. Marano, "Static and dynamic 4-way handshake solutions to avoid denial of service attack in Wi-Fi protected access and IEEE 802.11i", EURASIP Journal on Wireless Communications and Networking 2006 (1), 1-19.

[6] A. Lupia, F. De Rango, "Evaluation of the energy consumption introduced by a trust management scheme on mobile ad-hoc networks", Journal of Networks, vol. 10, no. 4, 2015.

[7] Lupia, A., De Rango, F., "Energy consumption evaluation of SAODV with trust management scheme under gray-hole attacks", (2015) Wireless Telecommunications Symposium, 2015-January, art. no. 7117288.

[8] Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks." Communications Surveys & Tutorials, IEEE15.4: 2046-2069, 2013.

[9] Wang, Yang, et al. "A queueing analysis for the Denial of Service (DoS) attacks in computer networks", Computer Networks, Vol. 51, Issue 12, pp. 3564-3573, 2007.

[10] N. Srilakshmi, K. Rani. "An Improved IP Traceback Mechanism For Network Security", IJRET: International Journal of Research in Engineering and Technology, Vol. 02, Issue 08, Aug-2013.

[11] Pham, V. H., Dacier, M., "Honeypot trace forensics: The observation viewpoint matters", Future Generation Computer Systems, 27(5), 539-546, 2011.

[12] Zhaole, C., & Lee, M., "An IP Traceback technique against Denial-of-Service attacks", In Proc. 19th Annual Computer Security Applications Conference, 2013.

[13] M. Voznak, F. Rezac and K. Tomala, "SIP penetration test system," 33rd International Conference on Telecommunications and Signal Processing (TSP 2010), pp. 504-508, 2010.

[14] J. Rozhon and M. Voznak, "SIP registration burst load test," Communications in Computer and Information Science, Volume 189 CCIS, Issue PART 2, pp. 329-336, 2011.
[15] M. Voznak and F. Rezac, "Web-based IP telephony penetration system evaluating level of protection from attacks and threats," WSEAS Transactions on Communications, Volume 10, Issue 2, pp. 66-76, 2011.
[16] E. Steven M. Bellovin, "ICMP Traceback Messages, Internet Draft", draft-bellovin-itrace-00.txt, 2000.
[17] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," in Proceedings of the ACM SIGCOMM Conference, pp. 295–306, 2000.
[18] D. X. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback," in Proceedings of IEEE INFOCOM '01, pp. 1–9, April 2001.
[19] K. Park and H. Lee., "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack", in Proceedings of IEEE INFOCOM '01, pp. 338 – 347, 2001.
[20] Micah Adler, "Trade-Offs in Probabilistic Packet Marking for IP Traceback," Journal of the ACM, vol. 52, pp. 217–244, March 2005.
[21] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback", IEEE/ACM Transactions on Networking, vol. 9, June 2001.
[22] J. Ioannidis and S. M. Bellovin, "Pushback: Router-based defense against ddos attacks", Network and Distributed System Security Symposium: NDSS '02, Reston, Va.: Internet Society, 2002.
[23] K. T. Law, J. C. S. Lui, and D. K. Y. Yau, "You Can Run, But You Can't Hide: An Effective Methodology to Traceback DDoS Attackers," IEEE Transactions on Parallel and Distributed Systems, vol. 15, no. 9, pp. 799 – 813, 2005.
[24] D. K. Y. Yau, John C. S. Lui, F. Liang, and Y. Yeung, "Defending Against Distributed Denial of-service Attacks with Max-min Fair Server-centric Router Throttles," in IEEE/ACM Transactions on Networking, vol. 13(1), February 2005.
[25] Keming Gu; M. N. O. Sadiku, "Absorbing Markov Chain solution for Possion's equation", Southeastcon, Proceedings of the IEEE, pp. 297-300, 2000.
[26] R. C. Garcia; M. N. O. Sadiku; Keming Gu , "Applying absorbing Markov chains to solve Poisson's equation in inhomogeneous regions", SoutheastCon. Proceedings. IEEE, pp. 166-168, 2001.
[27] C. M. Grinstead, J. Laurie Snell, "Introduction to probability", American Mathematical Society, 2nd edition, 2006.