Computer Networks 182 (2020) 107464

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

On packet marking and Markov modeling for IP Traceback: A deep probabilistic and stochastic analysis

Peppino Fazio [a,b,*], Mauro Tropea [b], Miroslav Voznak [a], Floriano De Rango [b]

[a] VSB – Technical University of Ostrava, 17. listopadu 2172/15, 708 00 Ostrava, Czechia

[b] Department of Informatics, Modeling, Electronics and Systems Engineering (DIMES), University of Calabria, via P. Bucci, 87036 Rende (CS), Italy

ARTICLE INFO

Keywords:
Probabilistic packet marking
IP traceback
Stochastic process
DoS attack
Network security
Marking probability

ABSTRACT

From many years, the methods to defend against Denial of Service attacks have been very attractive from different point of views, although network security is a large and very complex topic. Different techniques have been proposed and so-called packet marking and IP tracing procedures have especially demonstrated a good capacity to face different malicious attacks. While host-based DoS attacks are more easily traced and managed, network-based DoS attacks are a more challenging threat. In this paper, we discuss a powerful aspect of the IP traceback method, which allows a router to mark and add information to attack packets on the basis of a fixed probability value. We propose a potential method for modeling the classic probabilistic packet marking algorithm as Markov chains, allowing a closed form to be obtained for evaluating the correct number of received marked packets in order to build a meaningful attack graph and analyze how marking routers must behave to minimize the overall overhead.

1. Introduction

Network security has been one of the most significant issues in information technology for decades, also because the demand for connections between remote nodes have grown hand in hand with the quality and speed of broadband connections. Given this enormous amount of information exchange, a major problem in the information and communications field is protecting the confidentiality and privacy of data. This work focuses on a particular type of malicious attack that may occur in IP networks, called Denial-of-Service (DoS). As we know, the term "attack" means, in general, any action aimed at adversely affecting a particular system. The impairment may only be unwanted disclosure of information (the attacker can detect the running operating system), but it may also stop the delivery of services provided by the system or block it. In the worst case, the attacker can take complete control of the system (with administrative privileges) and can use it as a "bridgehead" to conduct new attacks. A distributed-DoS (DDoS) attack is a malicious attempt to block/damage normal traffic of a selected node (or an entire network) by shattering the selected node/network with a flood of IP packets. The probability of appearing a malicious attack is very high nowadays, given that we move to a complete IoT reality, in which each node may have a connection to the Internet, hence can be compromised by an attacker and used as a source for malicious packets [1]. The literature describes two counter-measures: one consists in mitigating the detrimental impact of attacks on the victim, while the second consists in attempting to discover the position of the source by tracing back the offending paths, then stopping the attacks at the source (this method is discussed in detail in this paper). In fact, the TraceBack (TB) method consists in deploying IP tracing technology: the source address in the packet header can be forged, and it therefore needs a security mechanism to determine the attack sources and attack paths when a DDoS attack occurs. The discussed algorithm can reduce the number of packets collected to reconstruct the attack path, especially in situations when an enormous number of counterfeit attack packets exist. It can also identify the correct attack path, and the tracing scheme uses a probability labeling method. In this paper, we propose a potential method for modeling the classic probabilistic PM algorithms as Markov chains, allowing a probabilistic closed form to be obtained for evaluating of the correct number of received marked packets in order to build a meaningful attack graph. The main contribution of this paper is therefore in providing an indication to the reader how the minimum number of required marked packets can be evaluated.

The structure of the following sections of the paper is as follows: Section 2 gives an overview of some of the existing works on network security issues and countermeasures, Section 3 proposes the main TB approach based on Markov chains, while conclusions are summarized in Section 4.

* Corresponding author at: Department of Informatics, Modeling, Electronics and Systems Engineering (DIMES), University of Calabria, via P. Bucci, 87036 Rende (CS), Italy.

E-mail address: peppino.fazio@vsb.cz (P. Fazio).

https://doi.org/10.1016/j.comnet.2020.107464
Received 10 November 2019; Received in revised form 28 July 2020; Accepted 30 July 2020
Available online 7 August 2020

2. Related work

Because of its widespread distribution and range of use, the Internet offers endless business opportunities for companies and consumers by making information available in a simple and straightforward manner, especially when remote and distributed applications are exploited. Unfortunately, it is also a powerful vehicle in the hands of hackers to launch attacks on almost anyone [2]. Today, the availability of hacking tools allows anyone to improvise as a hacker. Network attacks generally adopt computer networks as transportation media to convey the intrusion or even attack the communication system itself. The TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite, which is the most widely used communication protocol and the de-facto standard in the Internet society, is the vector used to launch an attack. These attacks are based on a number of serious security flaws inherent in the protocol design and implementation. By exploiting these security holes, different types of network attack can be launched. All network attacks exploit one or more security vulnerabilities or weaknesses present in the TCP/IP architecture. In the following section, we present some articles in the literature concerning typical network attacks that exploit (D)DoS operations.

2.1. DoS attack and mitigation

There are many works in literature about DoS mitigation, and most of them exploit several alternative approaches (such as neural networks, Markov chains, Kalman filtering, machine learning, etc. In [1] the authors study the effects of DoS attacks by establishing an attacker/defender game and analyzing the evolution based on game theory. They observed that managing all the expired state-entries can give more utility to the defender. The proposed scheme is the enhanced Distributed Low-rate Attack Mitigating (eDLAM), based on the concept of the Malicious Request Table (MRT), which allows to reduce the forwarded data, if a packet match is found inside. Simulation results shown that eDLAM outperforms some of the existing schemes (DPE, Rate-Limit). In [3], the authors mainly focus on security mechanisms and attacks analysis. The authors propose a queuing model that can perform several evaluations of DoS attacks in a computer network, characterized by a two-dimensional embedded Markov chain model used to develop an algorithm able to find the stationary probability distribution and other interesting performance metrics for analyzing traffic attacks. These analytical methods for security and studying networks under DoS attacks could open new lines of research in computer networks. Another work on DoS attacks is presented in [4]. In this paper, the authors provide a survey of the current attacks and possible defense solutions from both theoretical and practical points of view. These studies can help us understand rapid and increasingly sophisticated attacks and aid us in designing and implementing suitable countermeasures for security purposes. DDoS flooding attacks are also one of the biggest concerns for security professionals. In [5], the authors examine DDoS flooding attacks that try to disrupt access to user services by exploiting the vulnerabilities of computers inside the networks. In their paper, the authors present a survey on DDoS attacks, describing the problems of the attacks, and attempt to find the right countermeasures to these issues. They highlight the need for a comprehensive, distributed and collaborative defense mechanism able to prevent and anticipate DDoS attacks. The main goal was to provide the research community with a good basis for developing opportune defense mechanisms in order to prevent and detect these malicious attacks. In [6] the authors propose a completely different approach (detecting delay) to deal with the, so-called, interest flooding attack in Information-Centric Networks (ICNs). Instead of caring about the detecting accuracy, the authors propose a new scheme for minimizing it, while guaranteeing an acceptable detecting delay, by the use of an m-list table (mT), which maintains the entries related to the malicious Interests, based on the proposed algorithm. Simulation results demonstrate that the detection delay is minimized, with a negligible loss of the false negative/positive rate. The work in [7] underlines the importance of traffic security in vehicular environments, where the risk of an information leakage can influence the overall driving (car and personal) safety. To this aim, the authors propose the SINET architecture, as an instance of smart collaborative networking. SINET is vertically composed by three layers and horizontally contains two domains. A very good and deep description of the provided functions, services and protocols is given into the paper, giving to the reader the possibility to well understand all the advantages of the proposed architecture for different vehicular scenarios.

2.2. IP traceback and packet marking for security tracking

As introduced in the previous section, another topic deeply studied by researchers is IP Traceback technology. In [8], the authors propose a new and very light approach that is simple to implement and does not introduce processing overhead into the system. The mechanism proposed by the authors is innovative in being able to trace back possible attacks even if they are composed of only a few packets. The method also previews the possibility of implementing a service provider that implements the proposed scheme without revealing its internal network topology. In [9] the authors considered the issue of DDoS attacks launched from P2P systems. The paper demonstrates that, generally, the attacks derive from the violation of three key aspects: (a) the validation of membership information is necessary before use, (b) unaware nodes must forward only validated information, (c) the network must be able to protect nodes against multiple references to the victim. The authors validated their consideration in the context of P2P deployments. The authors of [10] analyze existing methods of IP Traceback systems. They discuss the active research in this topic and also consider possible attacks sent from infected hosts. Many existing works are based on efficient packet logging. They conclude their work affirming that an active security system utilizing IP Traceback technology could contribute to a safer and more reliable Internet environment by effectively protecting against intentional Internet hacking. The IP Traceback issues are examined in [11]. The authors compare the different Traceback techniques present in the literature. Their analysis shows that a best solution does not exist. Each proposed method has good qualities and its own advantages and disadvantages, but none of them can resolve all issues. The functionalities of each method are discussed in detail and then evaluated. They conclude their article with a discussion on the legal implications of IP Traceback. The work in [12] focuses on a particular type of attack called a reflector attack, which a serious DoS threat. The authors propose a new scheme based on reflective algebraic marking. This scheme comprises three different algorithms: marking, reflection and reconstruction. The proposal has been tested through simulations that have demonstrated it achieves high results in being able to trace the sources of potential attack packets. The merit of the proposal is also confirmed by the ability to produce a very low and consequently negligible number of false positives. In addition, in [13] an enhanced marking algorithm is proposed, based essentially on hash functions, able to mitigate the effects of false positives. By their proposal, the authors are able to reduce the number of needed packets to reconstruct the reverse path, and to authenticate the marking that enables a victim to detect the attackers attempts. In [14] the authors propose a solution for DDoS attacks. A traceback technique to support the detection of attackers by Deterministic Packet Marking (DPM) is investigated. The DPM marks the multiple bots engaged in tackling the victims IP address and once the DDoS attack is confirmed, the victim procure an identified DDoS attack on to his IP address through marks refining. Their results show a better performance of DPM compared to other approaches. In [15] a novel and practical SDN-based traceback technique to confirm the communication relationship between the suspicious server and the user is proposed. They validate the feasibility and effectiveness of the proposed technique through an

extensive real-world experiments showing a significantly low false positive rates. In [16] the authors review an ICMP traceback method, called SPITRI, and suggest few changes in the way the packets are marked and traced back in order to reduce the number of clock cycles needed for marking and tracking back. Their experiments demonstrate that the refinements reduce the time for marking and tracing back with high accuracy. In [17] A logging based IP traceback mechanism, referred to as Singleton Flow Traceback (SFT) is proposed and analyzed. The authors provide a mathematical description of the technique showing how SFT reaches zero false negative. Their results are also proved by experiments on a real Internet topology.

2.3. Traffic monitoring and DoS detection

The authors of [18] present a new application-level DoS detection approach, validating the proposed approach in the context of web servers. In particular, the idea is based on a non-parametric cumulative sum control chart algorithm (CUSUM), by which through the exploitation of a sequential analysis approach, it is possible to recognize DoS attacks. The authors, in addition, investigated also the effects of sampling the traffic to be analyzed. In [19], the authors propose a new mechanism that can identify and group together traces on machines in the same botnets (a number of Internet-connected nodes that communicate with other similar peers, in which components located on networked hosts communicate and coordinate their actions by "command and control" or by passing messages between them). They provide a solution for detecting new botnets using very cheap and easily deployable solutions, and the method has been validated through many months of collected data. They have also provided a solution for distinguishing relevant from not relevant traces. They have also shown that these botnets can remain active for very long periods of time. Through numerous experiments, the authors highlighted the benefit of considering more point of views in each attack process. The defense against DoS attacks has been receiving particular interest in recent years. While different techniques have been proposed, the Packet Marking (PM) and Traceback (TB) [20–24] procedures have especially demonstrated good results in facing different malicious attacks. Although host-based DoS attacks are more easily traced and managed, network-based DoS attacks (which employ spoofing in order to alter the source address of DoS packets and hide the source address) are a more challenging threat [25,26]. The work in [27] takes into account the current Internet shortcomings, as its poor data security. The authors propose a new architecture and describe the different proposed functions/services, able to allow the collaboration among users, so the transmission path for a certain service can be actively changed to protect one node from being attacked continuously (collaborative service). From this point of view, the authors show how the probability of a given service, to be affected by a DDoS attack, is inversely proportional to the grade of nodes collaboration. So, it will be more difficult for an attacker to guess the accurate transmission path and target server. Our paper differs from the literature by the implementation of the following features:

- First of all, a dynamic probabilistic approach has been proposed, instead of a static one in which each router of the network has the same marking probability; we based our approach on the theory proposed in [23,28] and a new expression of the left-over probability is proposed;
- A new Markovian model, based on the marking probability expression is defined and analyzed by varying the available parameters;
- The probabilistic and Markovian models are compared with some marking algorithms proposed in the literature.

3. Network attacks in IP networks and recent countermeasures

Network security is a large and very complex topic. As stated in [29], the weakness in Internet Protocol is that the source host itself fills the IP source host ID, and there is no means in TCP/IP to discover the true origin of a packet. Then, it is important to study techniques against protocol stack weaknesses potentially exploiting by attackers. Categorization of potential network attacks can possibly be done by considering transport or network layer attacks.

3.1. Attacks on the transport layer

The Session Hijacking attack exploits a web session to gain unauthorized access to data [30]. It can be categorized as follows: Man-in-the-middle (MITM), the attacker is able to intercept packets passing between two victims [31]; Blind hijacking, a malicious attacker injects data into the captured communications between two nodes [32]. In a Local Area Network Denial (LAND) attack, the attacker sends a TCP SYN packet with the victim's IP address and an open port for source and destination address, causing a system loop whose counter measure concerns control on IP addresses: suspicious packets are those with a source address that is not in the local subnet [33]. A UDP flooding attack is a DoS mechanism that sends a large number of UDP packets to random ports on a remote host, causing the attacked system to be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients. This attack can be managed by deploying firewalls at key points in a network to filter unwanted network traffic [34,35]. E-mail attacks have become common crimes in cyberspace. An attacker exploits default port (25), because packets entering this port are not filtered, sending malicious content [36].

3.2. Attacks on the network layer

IP spoofing is one type of network attack in which an attacker assumes the IP address of another host and uses it as source address to communicate with the targeted unaware hosts. This technique is used mainly during a (D)DoS attack. The main defense against IP spoofing is the packet filtering method [37,38]. Packet Sniffing is a software or hardware technique in which the malicious attacker captures packets from a network and takes advantage of known traffic content unethically. By reviewing the different headers in the data link, network, transport and application, sniffers can retrieve all kinds of information about the communication between two or more nodes [39]. An attacker can exploit also of IP packet fragmentation by create overlapping fragments. In this way he may be able to evade firewall packet inspection activity and still force packets to a target host. If the malicious attacker makes any changes in a data packet, then the entire data will change [40,41].

3.3. Defense against DoS attacks, general description of PM and IP TB

From the above, we can observe that PM suffers from two weaknesses: (a) it is a reactive scheme, and the attack must therefore occur before corrective actions can be taken; (b) it does not scale well under DDoS attacks, i.e., in terms of attacked hosts and effort needed to identify the attack sites. So, the powerful aspect of the IP TB method is in giving routers the possibility to mark and add information to attack packets, considering a certain value of probability. The destination victim can analyze the marked data in order to build-up a structured graph, whose meaningfulness depends on the quantity of information obtained by the victim, so an index should be considered (as suggested in the literature) a Savage's equation [21]. As shown later, the obtained expression is valid for a single attacker, while for several simultaneous attacks it is assumed or claimed that the number of packets required to reconstruct each path is a linear function of the number of simultaneous attacks. But, unfortunately, the main problem

is represented by network topologies, because linearity is not a general property (where for linear topology we refer to an acyclic graph with a connection degree higher or equal to two [42]). For this reason, Savage's equation underestimates the number of packets required for reconstructing the attack graph. Our proposal is based on the notion in [43], which attracted the attention of several researches in this area (in fact Savage's work was the first one able to give an expression for the number of packets needed to "build back" an attack path). From that point, many studies have been proposed, because the Traceback method allows "marking enabled" routers to mark attack packets. When the number of received packets on the victim/receiver's side is enough (what "enough" means, in this case, should be analyzed), the attack graph can be constructed and the path where the attack started from can be traced.

4. Basic principles and considerations for the new packet marking approach

4.1. Preliminaries on IP traceback

If we want to argue exactly about the origins of IP TB, we can refer to the ICMP Traceback method proposed in [44] in which each router, with a very low probability value (such as 1/25000), creates an ICMP message containing the information extracted from a received packet, including information about the adjacent nodes. ICMP traffic, unfortunately, is however highly differentiated or filtered, therefore its packets could be forwarded with lower rates than normal traffic. Malicious attacks can also create false ICMP packets. In the same year, the authors of [45] introduced for the first time the concept of packet marking for tracing back the attacker by using the collected packets. Savage in [21,43] analyzed this method in detail, arriving at a main conclusion about the minimum number of packets needed to reconstruct the attacker's path. The author underlined that all marking algorithms are composed of two components: *marking* (executed by enabled routers in the network) and *reconstruction* (executed by the attacked victim) and concluded that the convergence time of an algorithm is related to the number of packets that the victim must observe in order to reconstruct the attack path. A basic marking procedure (node append) provides that each enabled router marks the packets by appending its identity to the IP packet fields, arriving, however, with a high overhead level. Differently from deterministic approaches [28], this method can be enhanced by setting a certain marking probability m_p for each router and reserving the space for only one router identity in IP packets (node sampling) so that each packet can be marked by appending the router's identity only once. In this way, if N is a set of network routers, the probability of receiving a marked packet from router $r_i \in N$ that is k hops away from the victim (left-over probability) is:

$$p_{mark_i}(k) = m_{pi} \prod_{j=1}^{k-1} (1 - m_{pj}), \tag{1}$$

assuming that m_{pi} is the marking probability of $r_i \in N$ and the marking events are, obviously, i.i.d. If $m_{pi} = m_p \forall r_i \in N$, then the expression in Eq. (1) becomes:

$$p_{mark}(k) = m_p \cdot (1 - m_p)^{k-1}. \tag{2}$$

The main issue of this method consists in the fact that the victim should receive a huge number of marked packets for knowing the identity of "distant" routers (packets can be marked only once). In order to moderate the number of required packets, Savage [21,43] considered edges for marking (edge sampling) instead of single nodes. Three fields are used: the first (*start* field) adds the identity of the first marking router, the second (*distance* field) is set to zero by the first marking router and is then incremented by one by each no-marking router, and the third (*end* field) is used by the next marking routers to set their identity. The marking probability is the same for each marking-enabled router. Under these conditions and based on the model of *the coupon collector* problem [46], Savage showed that the expected number $E[P]$ of received packets by the victim in order to have a meaningful manner of reconstructing the attacking path of length k is bounded by:

$$E[P] < \frac{\ln(k)}{m_p \cdot (1 - m_p)^{k-1}} = g(k, m_p). \tag{3}$$

If we analyze the Eq. (3), the derivative function of the second term in respect of m_p is:

$$\begin{aligned} \frac{\partial g(k, m_p)}{\partial m_p} &= \ln(k) \cdot [m_p^{-2} \cdot (1 - m_p)^{1-k} + \cdots \\ &\quad \cdots - m_p^{-1} \cdot (k-1) \cdot (1 - m_p)^{-k}], \end{aligned} \tag{4}$$

which is equal to zero for $m_p^* = 1/k$.

Referring to Figs. 1 and 2, we can observe how the trend of $g(k, m_p)$ is minimized for m_p^*. In these charts, some values have been removed in order to show only comparable variables. The leftover probability in the case of edge-marking, assuming constant marking probability, can be easily determined as follows:

$$p_{mark_i}(k) = m_p \cdot (1 - m_p)^{k-i}. \tag{5}$$

where i is considered as the distance of the marking router from the source. The main issue of this approach consists in the distance k between attacker and victim being an *a priori* unknown, therefore it is difficult to determine which is the best value of the marking probability. Another consideration about marking probability is in assigning low values to m_p, but if we derive and illustrate (Fig. 3) the expression of the probability of receiving an unmarked packet as:

$$p_{unmark}(k) = (1 - m_p)^k, \tag{6}$$

we can observe that if we set m_p to values lower than 0.3 and the network is not large (in terms of hops), then the marking field can be improperly changed by an attacker, arriving undetected at the victim and compromising the traceback algorithm.

A first enhancement was proposed in [47] in which the authors suggested using a dynamic value of m_p, outperforming the previous idea of edge marking introduced by Savage in terms of left-over probability.

4.2. Our proposed marking probability expression

Starting from the contents of the previous subsection, we propose a more general approach in order to validate the potential of obtaining better results both from a probabilistic and a stochastic point of view. To this aim, we set the dynamic value of m_p to:

$$m_p(i) = i^{-n}, \tag{7}$$

where n is a positive value. For $n = 1$, the authors of [47] showed that a constant value of leftover probability can be obtained (as introduced for Eq. (1)). If we consider a path from source S (as a potential attacker A) to a destination D (as a potential victim V), then a packet sent from S/A to D/V will traverse k intermediate routers $\{r_1, \ldots, r_k\} \in N$, as illustrated in Fig. 4.

If we recall the expression of the leftover probability (that is to say the probability of a packet being marked by r_i and not by any other router on a path of length k), then for the dynamic case with $n = 1$ we have:

$$\begin{aligned} p_{mark_i}(k) &= m_{pi} \prod_{j=i+1}^{k} (1 - m_{pj}) = m_{pi} \prod_{j=i+1}^{k} (1 - \frac{1}{j}) = \\ &= \frac{1}{i} \cdot (1 - \frac{1}{i+1}) \cdot (1 - \frac{1}{i+2}) \cdot \cdots \cdot (\frac{1}{k}) = \\ &= \frac{1}{i} \cdot (\frac{i}{i+1}) \cdot (\frac{i+1}{i+2}) \cdot \cdots \cdot (\frac{k-1}{k}) = \frac{1}{k}, \end{aligned} \tag{8}$$

which is a constant leftover probability $\forall r_i \in N$.

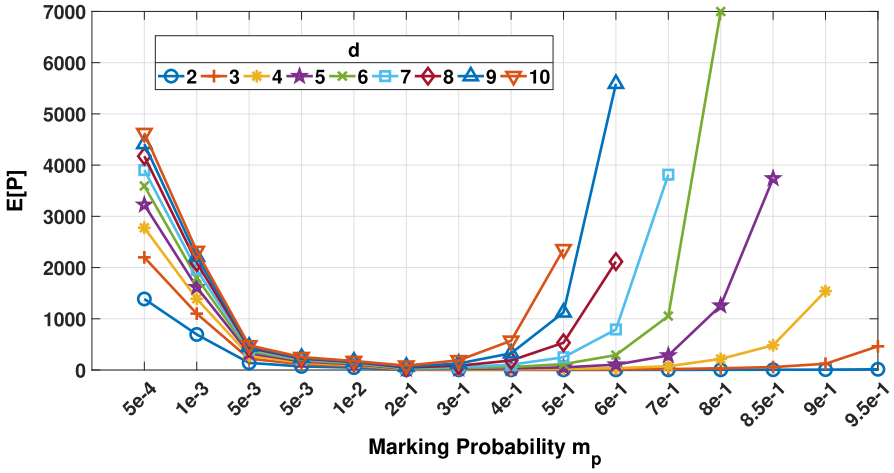

Fig. 1. Typical trend of $E[P]$ vs m_p in the case of edge marking.

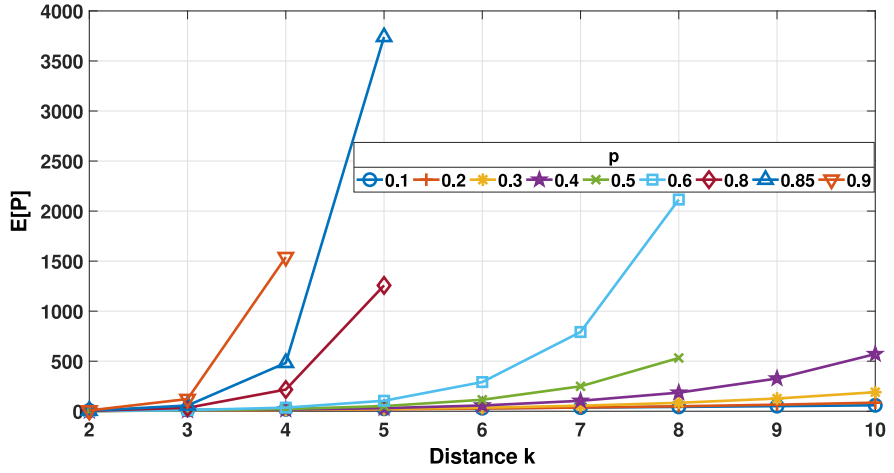

Fig. 2. Typical trend of $E[P]$ vs k in the case of edge marking.

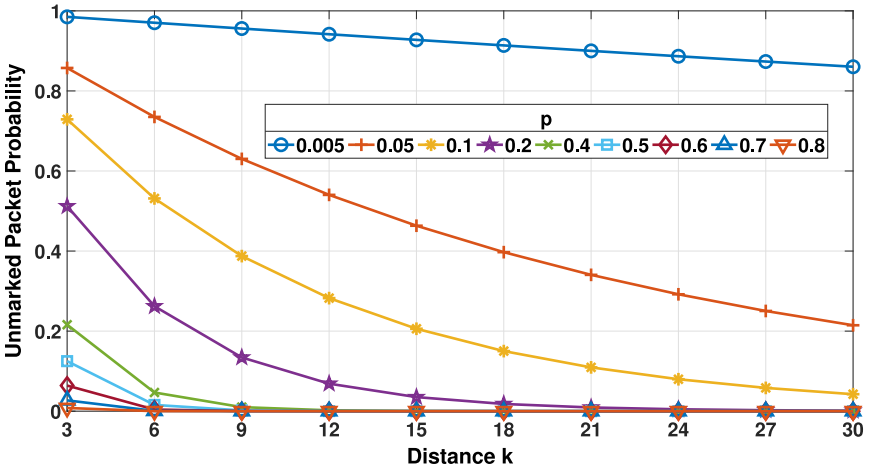

Fig. 3. Trend of the probability of receiving an unmarked packet vs k in the case of edge marking.

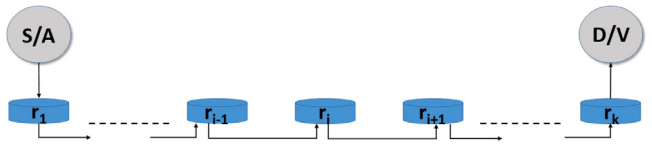

Fig. 4. Illustration of the path between S/A and D/V, with k intermediate routers.

Comparing this result to the one obtained in Eq. (5), then for larger k, the leftover probability is very low in the case of dynamic marking, while for Savage's PM method it increases polynomially (Fig. 5). Furthermore, for the proposed expression of marking probability, the leftover probability decreases when the path length increases, outperforming the other methods. In order to derive the number of packets needed to reconstruct a meaningful attack graph, we need to obtain an expression for its expectation value. Following the method in [21,43], we know that the probability of receiving a packet marked by the most distant router r_k is the lowest, and that the convergence time of the marking procedure is dominated by the time to receive a sample from r_k (distance k). In this way, in order to find an upper bound, we can assume that the victim receives a marked packet by any router with the same likelihood as r_k (these events are, however, not related), with probability:

$$m_p(k) = k^{-n} \cdot (1 - k^{-n})^{k-k} = k^{-n}. \tag{9}$$

Therefore, the probability that a given packet will be marked by a router is at least $k \cdot m_p(k)$. Recalling the theory of the *coupon collector* problem, the number of events needed to obtain one of each k items is $k \cdot (\ln(k) + O(c))$, where c is a constant value. In this way, we can conclude that an upper bound for the expected number of required packets $E[P]$ for building a meaningful attack graph is the second term of the following inequality:

$$E[P] < \ln(k) \cdot k^n. \tag{10}$$

Fig. 6 shows a comparison between the trend of the expected value of the number of required packets for reconstructing a meaningful attack graph. In the static case, the optimal value for p was selected as $1/k$. It can be seen how the static approach is overcome by the dynamic and the proposed methods. In particular, the range of the n parameter was set as [0.8, 1.2]: in this way, the rule "at least one marking per router" is satisfied. For different path lengths k, the proposed scheme outperforms both static and dynamic methods for $n < 1$, while for higher values of n the dynamic scheme demonstrates better results.

At this point, the proposed Markovian model is presented, based on the discussion above.

5. The Markovian model for IP TB related to the PM

The main aim of this work consists in modeling the PM approach as a Finite State Discrete Markov Chain (PM-FSDMC) in order to demonstrate how a stochastic approach can be deployed for network security and combating malicious attacks based on the PM procedure, as previously explained. Clearly, the assumption of marking capability by network routers must be made (so that routers are said to be PM-aware). Let us briefly recall the concept of stochastic processes and Markov chains.

5.1. Markov chains basics

A stochastic process is a family of random variables, all defined over the same sample space Ω and indexed through a t parameter that varies in the index set T:

$$\{X_t(\omega), t \in T, \omega \in \Omega\}. \tag{11}$$

The difference between two stochastic processes is the type of dependence existing between the random variables that compose them. From the definition and from Eq. (11), a stochastic process can be also considered a temporal evolution of a non-deterministic system. A process is said to be "discrete" if the random variables can assume a finite set of discrete values. A stochastic process is said to be "Markovian" when, for a fixed observation time instant t_l, the process evolution beginning from t_l depends only on t_k and not on the previous time instants:

$$\begin{aligned} &P[X(t_{l+1}) = x_{l+1} | X(t_l) = x_l \cap X(t_{l-1}) = x_{l-1} \cap \cdots \\ &\cdots \cap X(t_1) = x_1] = P[X(t_{l+1}) = x_{l+1} | X(t_l) = x_l]. \end{aligned} \tag{12}$$

Eq. (12) shows the so-called chain dependence property. In this paper, the discrete-time, discrete-values and finite-state Markov processes (also called Markov chains, where $X(t_l) = X_l$) are employed in order to analyze the behavior of the marking algorithm. Let $\Omega = \{\omega_0, \omega_1, \ldots, \omega_{K-1}\}$ denote a finite set of states and $\{X_j\}, j = 0, 1, 2, \ldots$ be a constant Markov process. Since the constant Markov process has the property of stationary transitions, the transition probability M between two states is independent of the time index j, thus:

$$M_{u,v} = P(X_{l+1} = \omega_v | X_l = \omega_u) \tag{13}$$

for all $l = 0, 1, 2, \ldots$ and $u, v \in \{0, 1, 2, \ldots, K-1\}$. Now, we can define a $K * K$ state transition probability matrix M with its elements $M_{u,v}$, as in Eq. (13). Note that a state transition probability matrix has the property that the sum of elements on each row is equal to 1:

$$\sum_{m=0}^{K-1} M_{l,m} = 1, \forall m \in \{0, 1, 2, \ldots, K-1\}. \tag{14}$$

Furthermore, with the stationary transition property, the probability of state j at any permissible time index l without any state information at other time indexes can be defined as:

$$p_j = P(X_l = \omega_j), j \in \{0, 1, 2, \ldots, K-1\}. \tag{15}$$

A $Kx1$ steady state probability vector $\vec{p}$ can be defined with its elements p_j, as in Eq. (15). In many cases, this vector can provide the set of initial state probabilities. Note that Eqs. (13) and (15) must satisfy the equilibrium condition, which states that for any given state j, the incoming flow and outgoing flow must be equal. That is:

$$\sum_{m=0}^{K-1} p_m \cdot M_{m,j} = p_j, \forall m \in \{0, 1, 2, \ldots, K-1\}, \tag{16}$$

and, in compact form, $\vec{p}' \cdot M = \vec{p}'$, where $\vec{p}'$ is the transpose of $\vec{p}$.

5.2. The Markovian marking model (PM-FSDMC)

As illustrated in previous sections, let us now consider a network composed of end-nodes and a set N of forwarding routers. Each $r_i \in N$ is "edge-marking capable", exploiting the *start*, *end* and *distance* fields: when a packet arrives at $r_i \in N$, a random number $x_i \in [0, 1)$ is extracted. On the basis of the x_i value, the marking procedure is executed. Then, the packet is forwarded to the next hop, according to the routing table. In this way, the marked packet represents an edge that will arrive at the victim only if next hops do not encode it again. The distance field is always increased in order to give to the victim knowledge of the distance of the received edge (packet). The marking process can terminate when $\exists$ a marked packet $\forall\ r_i \in N$: that is to say that the entire attack path (from the attacker to the victim) can be completely built when all the routers on the attack path chosen to mark a packet, which has been received by the victim side, are satisfying the Savage's equation. In order to define the discrete Markovian model, the state space Ω must first be defined. Let us again consider the set N, with $\|N\| = q$. If a Markov state represents a possible combination

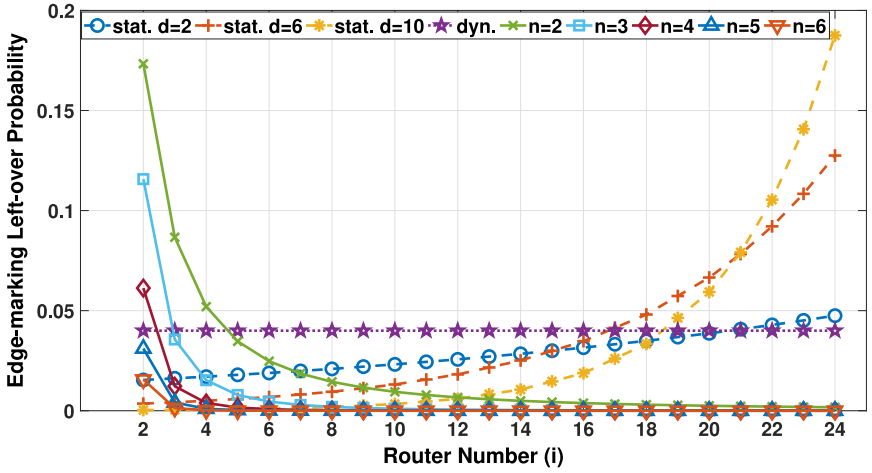

Fig. 5. Comparison of the edge-marking leftover probability for static, dynamic and proposed m_p values.

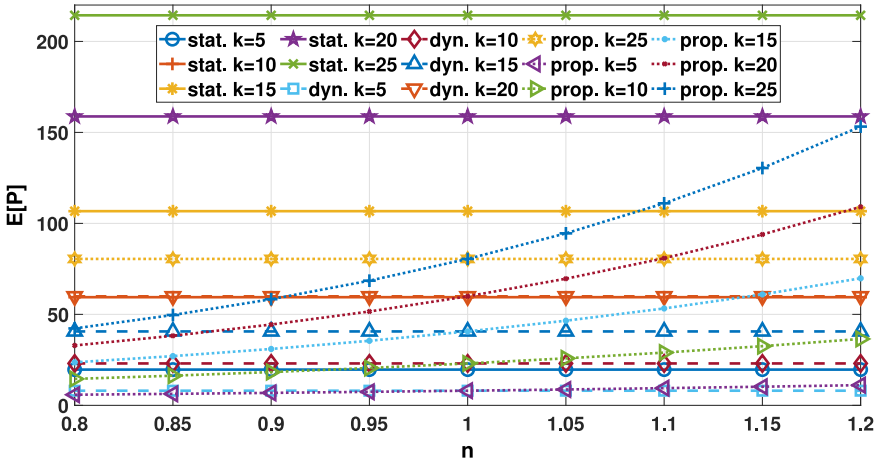

Fig. 6. Trend of E[P] vs n for static (*stat.*), dynamic (*dyn.*) and proposed (*prop.*) PM methods.

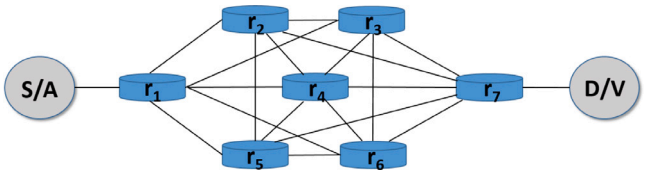

Fig. 7. Example of forwarding network, with q = 7..

of the collected marked packets, then the number of states $\|\Omega\|$ can be easily evaluated as follows:

$$\|\Omega\| = 1 + \sum_{k=1}^{q} C_{q,k}, \tag{17}$$

where $C_{q,k}$ represents the combination of q elements of class k, and an additional value is considered to take into account the case of no marking (starting state).

Fig. 7 shows a sample mesh topology in which malicious packets can flow from source S/A to destination D/V. In this case, $N = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7\}$, q = 7, $\Omega = \{\emptyset, r_1, r_2, r_3, r_4, r_5, r_6, r_7, (r_1r_2), (r_1r_3), \ldots, (r_1r_7), (r_2r_3), (r_2r_4), \ldots, (r_2r_7), (r_3r_4), \ldots, (r_3r_7), (r_4r_5), (r_4r_6), (r_4r_7), (r_5r_6), (r_5r_7), (r_1r_2r_3), (r_1r_2r_4), \ldots, (r_1r_2r_7), \ldots, \ldots, (r_1r_2r_3r_4), \ldots, \ldots, (r_1r_2r_3r_4r_5), \ldots, \ldots, (r_1r_2r_3r_4r_5r_6), \ldots, \ldots, (r_1r_2r_3r_4r_5r_6r_7)\}$, *with* $\|\Omega\| = C_{7,1}+C_{7,2}+C_{7,3}+C_{7,4}+C_{7,5}+C_{7,6}+C_{7,7}+1 = 7+21+35+35+21+7+1+1 = 128$. The state $s_1 = \emptyset$ is called the beginning state (the victim starts its algorithm without marked packets), while the state $s_{\|\Omega\|}$ is called the ending (or absorbing, as explained later) state (in the example $s\|\Omega\| = s_{128} = (r_1r_2r_3r_4r_5r_6r_7)$). The other states represent a transient condition for the algorithm. As described in previous sections, a Markovian chain is completely described by the state set and the transition probability matrix M. We must consider that a transition occurs only when the victim collects new information. For example, when the chain is in state $s_2 = r_1$ and the victim receives a packet marked by r_2, then a transition occurs, and the new state will be $s_9 = (r_1r_2)$. In order to define the transition probabilities matrix, the packet marking probability should be derived. Now, let $p(Marked\_by\_r_i)$ be the probability of a packet to be marked by $r_i \in N$, while $q - i$ is assumed to be the distance from r_i to the victim (in terms of number of hops), then:

$$p(Marked\_by\_r_i) = \frac{S_k}{S} \cdot m_{pi} \prod_{j=i+1}^{q} (1 - m_{pj}), \tag{18}$$

where S_k is the number of malicious sources that can reach r_i through attacking packets and S is the total number of sources. The marking event of r_i is independent of the marking event of r_j. Clearly, the probability of a packet to be not marked is:

$$p(!Marked) = 1 - \sum_{j=1}^{q} p(Marked\_by\_r_j). \tag{19}$$

Considering the example in Fig. 7, we have only one source S, therefore in this case, the ratio S_i/S is always 1. Since a transition between the Markovian states occurs only if new edges are discovered

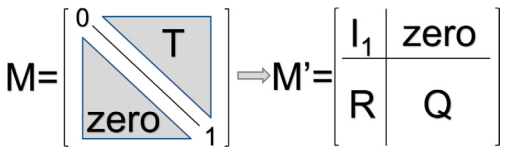

Fig. 8. General structure of matrix M and its structure M' after row and column permutations.

by the victim, the probability of receiving unmarked packets should be not taken into account, so the expression in Eq. (18) should be rewritten as:

$$p^*(Marked\_by\_r_i) = \frac{p(Marked\_by\_r_i)}{\sum_{k=1}^{q} p(Marked\_by\_r_k)}. \quad (20)$$

Here, the elements of M, indicated by M_{s_i,s_j}, can be defined. The exact expressions are as follows: $M_{\emptyset,\emptyset} = 0$, $M_{\emptyset,r_1} = p^*(Marked\_by\_r_1)$, $M_{r_1,(r_1r_2)} = p^*(Marked\_by\_r_2), \dots, M_{(r_1r_2\dots r_l),(r_1r_2\dots r_lr_{l+1})} = p^*(Marked\_by\_r_{l+1}), \dots, M_{(r_1r_2\dots r_l),(r_1r_2\dots r_l)} = \sum_{j=1}^{l} p^*(marked\_by\_r_j)$, $M_{(r_1\dots r_q),(r_1\dots r_q)} = 1$.

As known from Markov chains theory, M^r (with r a positive integer) represents the system state after r evolutions; in our case, r is the number of arrived packets, and the element $M^r(1, \|\Omega\|)$ is the probability of completing graph construction after the victim receives r packets:

$$M^r(1, \|\Omega\|) = \sum_{l=0}^{r} P[Pkt = l]. \quad (21)$$

It is therefore easy to verify that the term in Eq. (21) represents the probability that the considered system transits from state s_1 to state $s_{\|\Omega\|}$ after r packets are received. This value also represents the probability that r marked packets are enough to construct a consistent attack graph. From the derived Markov model, we can now obtain a theoretical evaluation of the upper bound $E[P]$ by considering the absorbing property of Markov chains [48,49]. A Markov process is said to be "absorbing" if at least one state $s_i \in \Omega$ exists that once reached, the evolution of the process never leaves. The state s_i is called the absorbing state, while all the others are called transient states. In general, a Markov chain is therefore an absorbing chain if and only if the following two conditions are satisfied: (a) the chain has at least one absorbing state, (b) it is possible to go from any non-absorbing state to an absorbing state (perhaps in more than one step). The considered PM-FSDMC is surely absorbing, given that the process no longer evolves once the state $s\|\Omega\|$ is reached. When the considered system evolves (the victim receives more packets), considering the M^r structure, and when M is raised to higher and higher powers, the system will tend towards an absorbing state. Regardless of the original state, the chain will therefore enter an absorbing state in a finite number of steps. Clearly, in general, if there are more absorbing states, the long-term trend depends on the initial state (changing the initial state can change the final result). In our case, only one absorbing state exists. In fact, regardless of the marking probability values (static, dynamic, proposed), the obtained structure of M is always composed of several components: a lower triangle of zero (*zero*) below the main diagonal, an upper triangle of transient probabilities (T), a diagonal of probabilities values with a zero in the upper left corner and a one in the lower right corner, as illustrated at the left of Fig. 8.

We can evaluate the composition of M^r in order to determine the final probabilities of entering an absorbing state, however, depending on the required value of r, the computation can be quite long. In order to obtain the same information without evaluating all the powers of M, the concept of "fundamental matrix" should be taken into account. By acting a permutation of the states, the matrix M can be rewritten as M', as illustrated at the right of 8, where I_1 is the 1×1 identity matrix, *zero* is the sub-matrix of zero at the upper-right, R is the sub-matrix at the lower left and related to the transition probabilities from transient to absorbing states, and Q is the sub-matrix at the lower right related to the transition probabilities between transient states. From Markovian theory, it is known that $Q^r \to 0$ for $r \to \infty$, because the probability that the chain cannot reach an absorbing state from a transient state s_j is the sum of the corresponding row of Q, indicated as Q_j. The values of Q_j are less than 1, and for this reason, $Q_j \to 0$. In our case and given that we have only one absorbing state, we can re-write M so that the rows and columns corresponding to the absorbing state come first. In this way, the fundamental matrix of M is defined as [50,51]:

$$F = (I_{\|\Omega\|-1} - Q)^{-1} \quad (22)$$

or, equivalently:

$$F = I + Q + Q^2 + Q^3 + Q^4 + \cdots \quad (23)$$

Each element $F(i, j)$ is intended as the expected number of times the process is in state s_j if it started in state s_i. In the case of PM-FSDMC, the starting state is always s_1 (the potential victim starts without having received any marked packets), so the expected number of received packets $E[P]$ can be also evaluated as the expected number of visits from s_1 to any transient state (each visit represents a received packet) before reaching the absorbing condition (state $s\|\Omega\|$):

$$E[P] = F(1, 1) + F(1, 2) + \cdots + F(1, \|\Omega\| - 1). \quad (24)$$

In this way, once the network structure and the value of q and the marking algorithm (static, dynamic or proposed) are determined, the expected number of marked packets to be received for meaningful attack graph reconstruction can be easily evaluated using Eq. (24).

6. Numerical analysis

In this section, we introduce some concrete examples of the theoretical approaches proposed in the previous sections so that the reader can better understand how these concepts can be applied.

First, let us use an example to clarify how the parameters can be determined numerically, considering the topology of Fig. 9, where $q = 9$ and $N = \{r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9\}$. We have $\Omega = \{s_1, s_2, \dots, s_{512}\} = \{\emptyset, r_1, r_2, r_3, r_4, r_5, r_6, r_7, r_8, r_9, (r_1r_2), \dots, (r_1r_9), (r_2r_3), \dots, (r_2r_9), (r_3r_4), \dots, (r_3r_9), (r_4r_5), \dots, (r_4r_9), (r_5r_6), \dots, (r_5r_9), (r_6r_7), \dots, (r_6r_9), \dots, (r_7r_8), (r_7r_9), (r_8r_9), (r_1r_2r_3), (r_1r_2r_4), \dots, (r_1r_2r_9), (r_2r_3r_4), \dots, (r_2r_3r_9), \dots, (r_7r_8r_9), (r_1r_2r_3r_4), (r_1r_2r_3r_5), \dots, (r_1r_2r_3r_9), \dots, (r_6r_7r_8r_9), (r_1r_2r_3r_4r_5), (r_1r_2r_3r_4r_9), (r_2r_3r_4r_5r_6), \dots, (r_2r_3r_4r_5r_9), \dots, (r_5r_6r_7r_8r_9), (r_1r_2r_3r_4r_5r_6), \dots, (r_1r_2r_3r_4r_5r_9), \dots, (r_4r_5r_6r_7r_8r_9), (r_1r_2r_3r_4r_5r_6r_7), \dots, (r_1r_2r_3r_4r_5r_6r_9), \dots, (r_3r_4r_5r_6r_7r_8r_9), (r_1r_2r_3r_4r_5r_6r_7r_8), \dots, (r_1r_2r_3r_4r_5r_6r_7r_8r_9)\}$, where $\|\Omega\| = 1 + C_{9,1} + C_{9,2} + C_{9,3} + C_{9,4} + C_{9,5} + C_{9,6} + C_{9,7} + C_{9,8} + C_{9,9} = 512$. We consider what happens when the probability is set to $1/q$ (static, ST), i^{-1} (dynamic, DY) and i^{-n} (our proposal, PR based on PM-FSDMC). Without the loss of generality, we assume only one source, therefore in Eq. (18) the ratio Si/S is always equal to 1. Another assumption regards the forwarding protocol: we assume that the best path from S to D is always evaluated as the shortest one, that is in Fig. 9 neither vertical forwardings (for example from R_4 to R_5 or from R_7 to R_8) nor backward forwardings (for example from R_5 to R_2 or from R_8 to R_6) are allowed. Red dotted lines in the figure separate routers on the basis of their distance from the source.

Fig. 10 represents the values of Eq. (20) for different values of n for ST, DY and PR schemes, with $q = 9$ and $m_p = 1/q$, while Table 1 lists the values of Eq. (20) for the topology of Fig. 9, with $n = 1.2$.

Recalling that, for the forwarding network of Fig. 9, we have $\|\Omega\| = 512$, then the associated Markov model, as defined in the previous section, can be illustrated as in Fig. 11.

The transition matrix (as defined in Eq. (13) and in Eq. (20)) can now be evaluated by considering the starting state and the transition probabilities.

For readability issues, we illustrate only a portion of M, as indicated in Fig. 12. It can be seen how the first column is equal to zero (it is

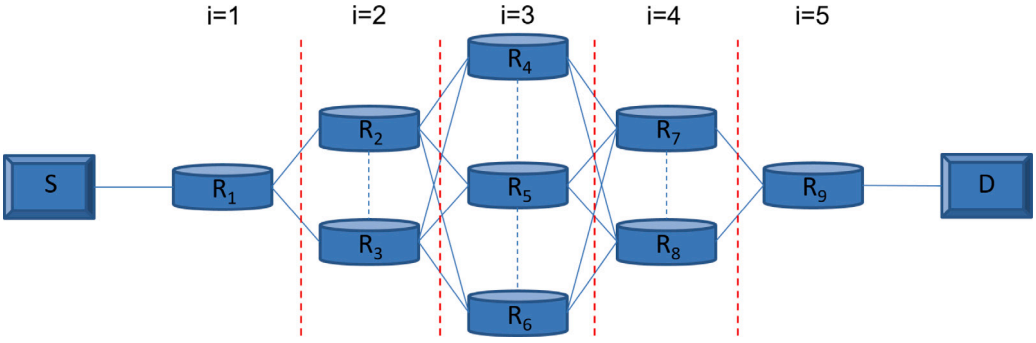

Fig. 9. Sample topology, with q=9.

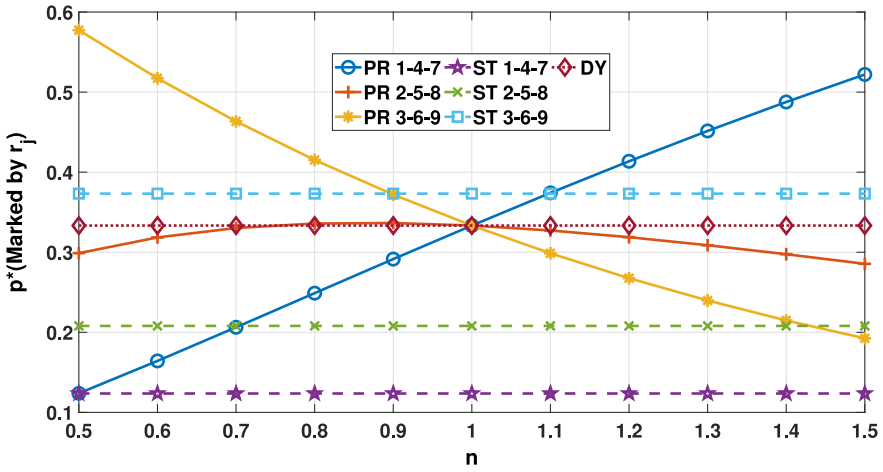

Fig. 10. p* trends (Eq. (20)) for different values of n.

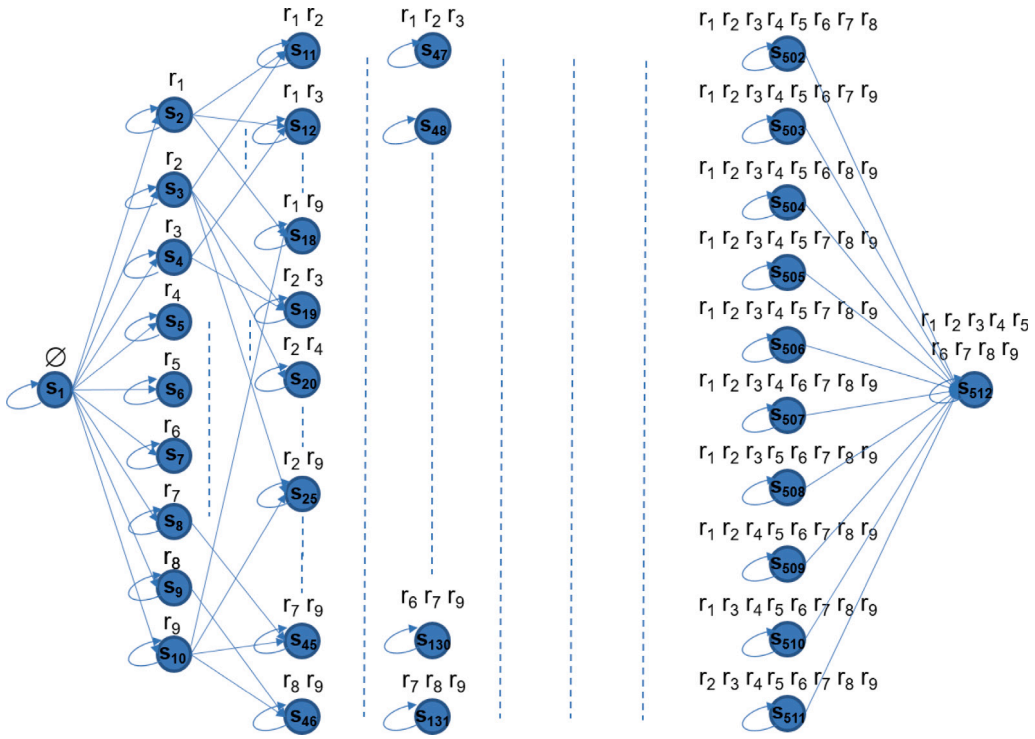

Fig. 11. Markov chain model associated with the topology of Fig. 9, with $q = 5$.

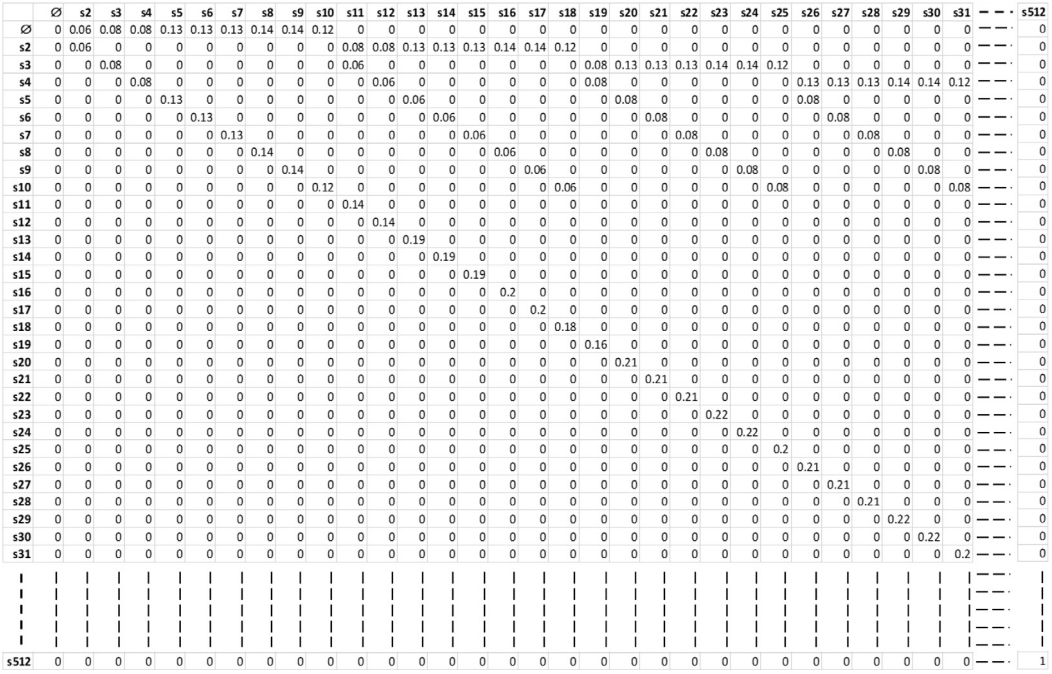

Fig. 12. A portion of the Transition Probabilities Matrix M associated with the model in Fig. 11 for the PR scheme, with $q = 9$, $n = 1.2$, $\|\Omega\| = 32$.

Table 1
$p^*(Marked\_by\_r_i)$ values for $ST, DY, PR(n = 1.2)$ algorithms, related to the topology of Fig. 9.

ALG	r_1	r_2	r_3	r_4	r_5	r_6	r_7	r_8	r_9
ST	0.066	0.074	0.084	0.094	0.106	0.119	0.134	0.151	0.170
DY	0.033	0.033	0.066	0.066	0.100	0.150	0.150	0.200	0.200
PR	0.060	0.081	0.081	0.127	0.127	0.127	0.137	0.137	0.122

related to the initial state) and its composition respects the structure illustrated in Fig. 8 on the left side. Because of space limitations, we only illustrate the portion of the matrix structure only for PR, but the results are also evaluated for the ST and DY schemes. In addition, scalability is not an issue, because of M is a $\Omega \cdot \Omega$ sparse upper triangular matrix, which can be easily stored and/or compressed by considering only non-zero values [52] and, for example, one of the Compressed Sparse Row (CSR), Compressed Sparse Column (CSC), or COordinate Format (COF) algorithm.

Before comparing the main results obtained by Savage [21,43] and the Markov model (under PR), we show the trend of some $M(i, j)$ values, as illustrated in Fig. 13. Four sub-figures are shown, and all of them illustrate the trend of some (i, j) elements of M: the indexes i and j represent the set of routers which have marked the packet received by the destination (victim). That is, $M(\emptyset, 3)$ represents the probability of receiving a packet marked by router 3, given that the receiver has not received any marked packet before, so a transition from the state $\emptyset$ to the state r_3; similarly, $M(1234, 1234)$ represents the probability of receiving a packet marked by r_1, or by r_2, or by r_3, or by r_4 given that all these markings have already been received before, so the probability of remaining in the state $r_1r_2r_3r_4$, and so on. Each curve is plotted in function of n, that is the parameter chosen in our proposed marking scheme PR. The sub-figures b, c and d represent diagonal elements of M. It can be seen how, there is a variable trend in function of n, recalling that the sum of all elements on a row of M should be 1.

At this point, in order to verify the effectiveness of the proposed scheme, we first examine the analysis of the $M^r(1, \|\Omega\|)$ element, which is the probability of attack graph reconstruction after r packets received by the victim (Eq. (21)). In other words, Figs. 14–16 represent the trend of the probability that r marked packets are enough in order to construct a meaningful attack graph. Values exists only in correspondence of each point on the x-axis, connecting lines are illustrated only to represent the trend (pdf and cdf are discrete functions in this case). Fig. 14 shows how increasing the number of received packets will also increase the cumulative probability of r packets, although the static scheme offers slightly lower values. The same information can be determined from the pdf (Fig. 15) simply by evaluating the following quantity:

$$M^r(1, \|\Omega\|) - M^{r-1}(1, \|\Omega\|) = M^r(1, 512) - M^{r-1}(1, 512), \tag{25}$$

in other words, by deriving the pdf from the cumulative values, we have the punctual information about the probability of having enough packets for a meaningful attack graph.

Fig. 16 shows the exact values illustrated in Figs. 14 and 15, but additional comments need to be made. First, it can be seen that with ST and PR (n=1.2), the victim needs to receive at least fifteen packets to reconstruct the attack graph completely, while with PR (and n values from 0.8 to 1.1), thirteen marked packets are enough. It should be also highlighted that the values in Fig. 16 respect precisely the upper bounds illustrated in Fig. 6.

The same analysis can be done by considering the fundamental matrix related to M. By applying Eq. (22), the matrix F with size $511x511$ has been obtained. From F, the upper bound for $E[P]$ can be evaluated by applying Eq. (24), and repeating the experiment for different values of n, the chart in Fig. 17 is obtained, which shows a comparison of the different ways of obtaining the expected value of required packets for meaningful graph reconstruction.

The curve trends verify the probabilistic method and fundamental matrix: it can be seen that the obtained theoretical bounds are very close, independently on the particular approach (pdf/cdf, probabilistic or Markovian). The maximum evaluation error is around 3 packets (for n=1.1).

7. Conclusions

In this paper, we studied and proposed potential method for combating malicious attacks in telecommunications networks. The aim was to

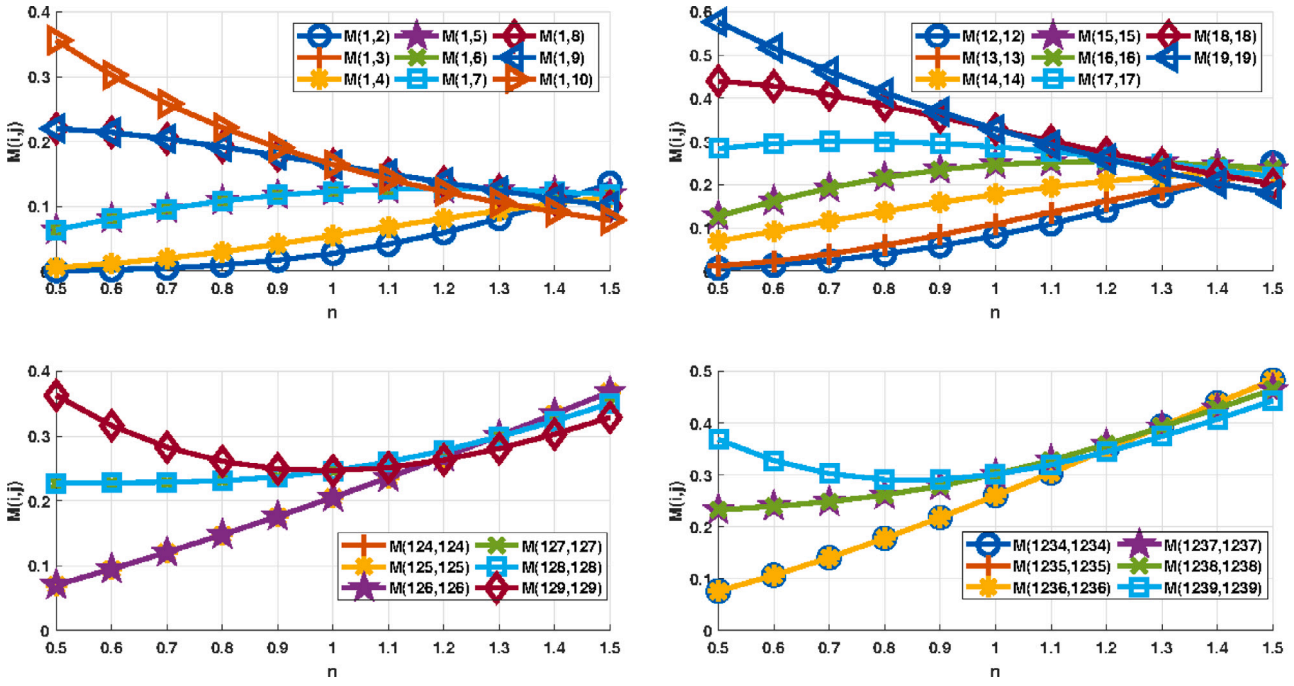

Fig. 13. The trend of some M(i, (j) values.

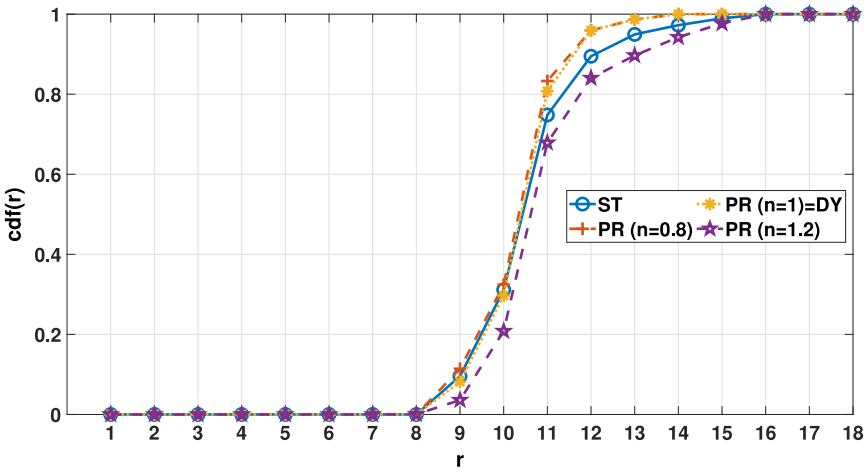

Fig. 14. Cumulative probability of having a meaningful attack graph after receiving r marked packets ($q = 9$).

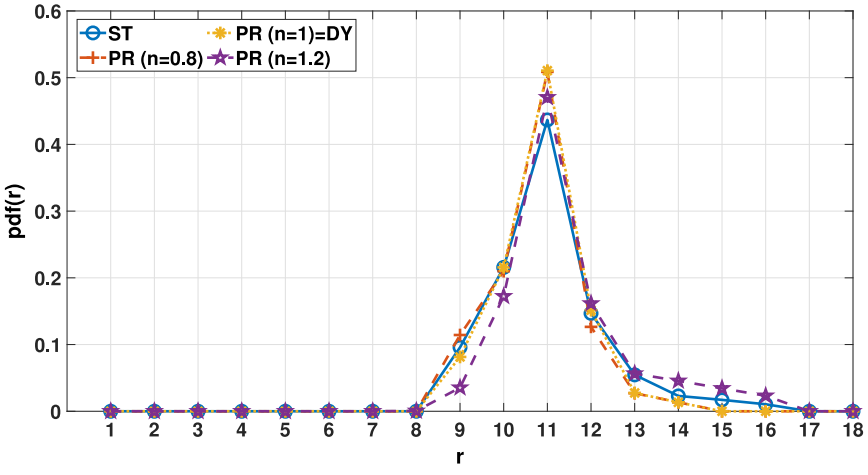

Fig. 15. Probability of having a meaningful attack graph after receiving r marked packets ($q = 9$).

r	ST	PR (n=0.8)	PR (n=1) = ST	PR (n=1.2)	ST	PR (n=0.8)	PR (n=1) = ST	PR (n=1.2)
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0.0006	0	0	0	0.0006
9	0.0958	0.1143	0.0814	0.0354	0.0958	0.1143	0.0814	0.0359
10	0.2157	0.2099	0.2157	0.1723	0.3114	0.3242	0.2971	0.2083
11	0.4367	0.5088	0.5106	0.4705	0.7481	0.8330	0.8076	0.6788
12	0.1468	0.1265	0.1515	0.1615	0.8949	0.9595	0.9592	0.8403
13	0.0545	0.0270	0.0275	0.0565	0.9494	0.9865	0.9866	0.8968
14	0.0230	0.0135	0.0134	0.0456	0.9724	1	1	0.9424
15	0.0171	0	0	0.0344	0.9895	1	1	0.9768
16	0.0105	0	0	0.0232	1	1	1	1
17	0	0	0	0	1	1	1	1
18	0	0	0	0	1	1	1	1
	pdf				*cdf*			

Fig. 16. Tabular values of pdf and cdf probability of having a meaningful attack graph after receiving r marked packets ($q = 9$).

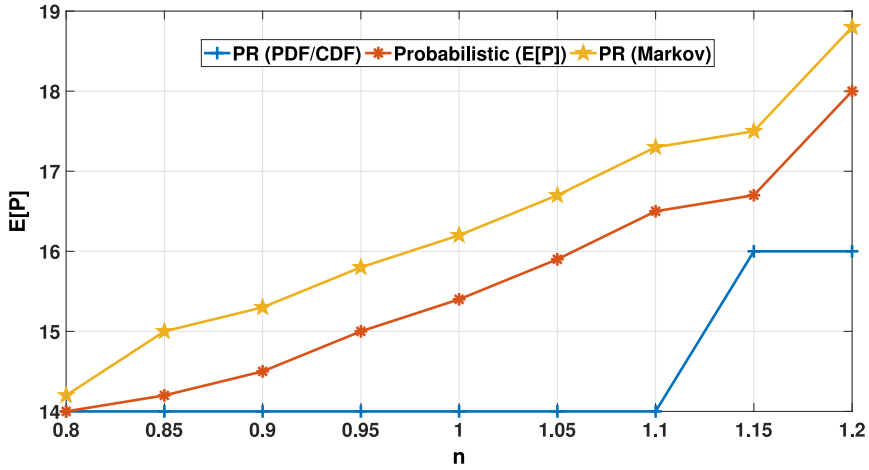

Fig. 17. Trend of E[P] for different values of n.

study the statistics that can be obtained from a packet marking Markovian approach, taking into account different methods of assigning marking probabilities values. For this kind of approach, one of the main issue consists in obtaining information about the minimum number of marked packets to be collected in order to derive a meaningful attack graph. The victim should avoid waiting to receive additional marking information after the necessary number of marked packets have been received. We started from Savage's fundamental relationship, which provides an indication of the upper limit of the expected number of packets, and then modeled the marking algorithm as a Markov chain, investigating the fundamental matrix and relating the kernel of the transition probabilities matrix to the number of packets required to start the graph reconstruction. A closed form was derived in order to provide a more precise indication of the number of required packets. We also provided a deep description of the main numerical results, which show that the proposed approach is reliable and comparable with the main existing works in literature.

CRediT authorship contribution statement

Peppino Fazio: Conceptualization, Methodology, Investigation, Writing - original draft, Preparation. **Mauro Tropea:** Data curation, Software, Visualization. **Miroslav Voznak:** Supervision, Writing - review & editing. **Floriano De Rango:** Validation, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by The Czech Ministry of Education, Youth and Sports from the Large Infrastructures for Research, Experimental Development and Innovations project "IT4Innovations National Supercomputing Center – LM2015070" and partially received a financial support also from a grant No. SGS SP2019/41 conducted by the VSB-Technical University of Ostrava, Czech Republic.

References

[1] G. Liu, W. Quan, N. Cheng, H. Zhang, S. Yu, Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things, J. Netw. Comput. Appl. 130 (2019) 1–13.

[2] O. Osanaiye, K.-K.R. Choo, M. Dlodlo, Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework, J. Netw. Comput. Appl. 67 (2016) 147–165.

[3] Y. Wang, C. Lin, Q.-L. Li, Y. Fang, A queueing analysis for the denial of service (DoS) attacks in computer networks, Comput. Netw. 51 (12) (2007) 3564–3573.

[4] V. Zlomislić, K. Fertalj, V. Sruk, Denial of service attacks: an overview, in: 2014 9th Iberian Conference on Information Systems and Technologies, CISTI, IEEE, 2014, pp. 1–6.

[5] S.T. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Commun. Surv. Tutor. 15 (4) (2013) 2046–2069.

[6] G. Liu, et al., Accuracy or delay? A game in detecting interest flooding attacks, Internet Technol. Lett. 1 (2018).

[7] W. Quan, et al., Enhancing crowd collaborations for software defined vehicular networks, IEEE Commun. Mag. 55 (2017) 80–86.

[8] L. Cheng, D.M. Divakaran, W.Y. Lim, V.L. Thing, Opportunistic piggyback marking for IP traceback, IEEE Trans. Inf. Forensics Secur. 11 (2) (2015) 273–288.

[9] S. Xin Sun, R. Torres, Preventing DDoS attacks on internet servers exploiting P2P systems, Comput. Netw. 54 (15) (2010) 2756–2774.

[10] N. Srilakshmi, K. Rani, An improved IP traceback mechanism for network security, Int. J. Res. Eng. Technol. 2 (08) (2013).

[11] A. Belenky, N. Ansari, On IP traceback, IEEE Commun. Mag. 41 (7) (2003) 142–153.

[12] Z. Chen, M.-C. Lee, An IP traceback technique against denial-of-service attacks, in: 19th Annual Computer Security Applications Conference, 2003. Proceedings, IEEE, 2003, pp. 96–104.

[13] D.C.J. Hasmukh Patel, LPM: A lightweight authenticated packet marking approach for IP traceback, Comput. Netw. 140 (2018) 41–50.

[14] S. Suresh, N. Ram, M. Mohan, An optimistic approach to interpret the DDoS attacks by wielding deterministic packet marking, in: 2019 International Conference on Smart Structures and Systems, ICSSS, IEEE, 2019, pp. 1–4.

[15] Z. Ling, J. Luo, D. Xu, M. Yang, X. Fu, Novel and practical SDN-based traceback technique for malicious traffic over anonymous networks, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 1180–1188.

[16] S. Malliga, S. Kogilavani, P. Nandhini, A low traceback and zero logging overhead IP traceback approach for communication networks, in: 2018 International Conference on Intelligent Computing and Communication for Smart World, I2C2SW, IEEE, 2018, pp. 100–105.

[17] R.C. Baishya, D. Bhattacharyya, Singleton flow traceback (SFT) mechanism, in: 2020 Third ISEA Conference on Security and Privacy, ISEA-ISAP, IEEE, pp. 139–148.

[18] H.H. Jazi, et al., Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling, Comput. Netw. 121 (2017) 25–36.

[19] D. Rajwal, D. Band, A. Yadav, Study of different attacks on network & transport layer, Int. J. Eng. Comput. Sci. 2 (3) (2013) 692–695.

[20] S. Bellovin, M. Leech, T. Taylor, Internet Draft: ICMP Traceback Messages, technical report, Network working Group, 2000.

[21] S. Savage, D. Wetherall, A. Karlin, T. Anderson, Practical network support for IP traceback, ACM SIGCOMM Comput. Commun. Rev. 30 (4) (2000) 295–306.

[22] D.X. Song, A. Perrig, Advanced and authenticated marking schemes for IP traceback, in: Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213), volume 2, IEEE, 2001, pp. 878–886.

[23] K. Park, H. Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, in: Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213), volume 1, IEEE, 2001, pp. 338–347.

[24] M. Adler, Trade-offs in probabilistic packet marking for IP traceback, J. ACM 52 (2) (2005) 217–244.

[25] L. Golubchik, J.C. Lui, Bounding of performance measures for threshold-based queuing systems: Theory and application to dynamic resource management in video-on-demand servers, IEEE Trans. Comput. 51 (4) (2002) 353–372.

[26] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker, Controlling high bandwidth aggregates in the network, ACM SIGCOMM Comput. Commun. Rev. 32 (3) (2002) 62–73.

[27] H. Zhang, et al., Smart identifier network: a collaborative architecture for the future internet, IEEE Netw. 30 (2016) 46–51.

[28] V.A. Siris, I. Stavrakis, Provider-based deterministic packet marking against distributed DoS attacks, J. Netw. Comput. Appl. 30 (3) (2007) 858–876.

[29] R.T. Morris, A Weakness in the 4.2 BSD Unix TCP/IP Software, Tech. Rep. Comput. Sci. 117, AT&T Bell Labs, 1985.

[30] Y. Wang, J. Chen, Hijacking spoofing attack and defense strategy based on internet TCP sessions, in: 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation, IMSNA, IEEE, 2013, pp. 507–509.

[31] N.R. Samineni, F.A. Barbhuiya, S. Nandi, Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks, in: 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, IEEE, 2012, pp. 364–367.

[32] J. Zhao, Y. Wen, Y. Wang, Model construction on prefix hijacking attack, in: 2012 IEEE 14th International Conference on Communication Technology, IEEE, 2012, pp. 866–871.

[33] C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, D. Zamboni, Analysis of a denial of service attack on TCP, in: Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097), IEEE, 1997, pp. 208–223.

[34] R. Xu, W.-l. Ma, W.-l. Zheng, Defending against UDP flooding by negative selection algorithm based on eigenvalue sets, in: 2009 Fifth International Conference on Information Assurance and Security, volume 2, IEEE, 2009, pp. 342–345.

[35] S.M. Hussain, G.R. Beigh, Impact of DDoS attack (UDP Flooding) on queuing models, in: 2013 4th International Conference on Computer and Communication Technology, ICCCT, IEEE, 2013, pp. 210–216.

[36] T. Bass, A. Freyre, D. Gruber, G. Watt, E-mail bombs and countermeasures: cyber attacks on availability and brand integrity, IEEE Netw. 12 (2) (1998) 10–17.

[37] C. Manusankar, S. Karthik, T. Rajendran, Intrusion detection system with packet filtering for IP spoofing, in: 2010 International Conference on Communication and Computational Intelligence, INCOCCI, IEEE, 2010, pp. 563–567.

[38] A. Mukaddam, I. Elhajj, A. Kayssi, A. Chehab, IP spoofing detection using modified hop count, in: 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, IEEE, 2014, pp. 512–516.

[39] A. Barua, H. Shahriar, M. Zulkernine, Server side detection of content sniffing attacks, in: 2011 IEEE 22nd International Symposium on Software Reliability Engineering, IEEE, 2011, pp. 20–29.

[40] O.B. Ahmed, Z. Choukair, Link analysis approach to improve detection of fragmentation attacks in Misuse IDS, in: 2009 First International Conference on Communications and Networking, IEEE, 2009, pp. 1–8.

[41] S. Young, D. Aitel, The Hacker's Handbook: The Strategy behind Breaking Into and Defending Networks, Auerbach publications, 2003.

[42] V. Curia, M. Tropea, P. Fazio, S. Marano, Complex networks: study and performance evaluation with hybrid model for wireless sensor networks, in: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering, CCECE, IEEE, 2014, pp. 1–5.

[43] S. Savage, D. Wetherall, A. Karlin, T. Anderson, Network support for IP traceback, IEEE/ACM Trans. Netw. 9 (3) (2001) 226–237.

[44] S.M. Bellovin, M. Leech, T. Taylor, ICMP Traceback Messages, 2003.

[45] H. Burch, B. Cheswick, Tracing anonymous packets to their approximate source, in: LISA, 2000, pp. 319–327.

[46] L. Graham, D. Knuth, O. Patashnik, Concrete Mathematics, Addison-Wesley Publ. Comp, Reading, Mass, 1989.

[47] J. Liu, Z.-J. Lee, Y.-C. Chung, Dynamic probabilistic packet marking for efficient IP traceback, Comput. Netw. 51 (3) (2007) 866–882.

[48] K. Gu, M.N. Sadiku, Absorbing Markov chain solution for Possion's equation, in: Proceedings of the IEEE SoutheastCon 2000. 'Preparing for the New Millennium'(Cat. No. 00CH37105), IEEE, 2000, pp. 297–300.

[49] R.C. Garcia, M.N. Sadiku, K. Gu, Applying absorbing Markov chains to solve Poisson's equation in inhomogeneous regions, in: Proceedings. IEEE SoutheastCon 2001 (Cat. No. 01CH37208), IEEE, 2001, pp. 166–168.

[50] J. Raviv, Decision making in Markov chains applied to the problem of pattern recognition, IEEE Trans. Inform. Theory 13 (4) (1967) 536–551.

[51] C.M. Grinstead, J.L. Snell, Introduction to Probability, American Mathematical Soc., 2012.

[52] R.B.J. Stoer, Introduction to Numerical Analysis, third ed., Springer-Verlag, 2002.

Peppino Fazio was born in 1977 and graduated in Computer Science Engineering (M.D.) in May 2004, at the University of Calabria (Italy). He took the Ph.D. in Electronics and Communications Engineering at the same University in January 2008. In the same year he spent a period of six months at the UPV of Valencia (Spain), for researching about VANET architecture. he has been Assistant Professor from 2014 to 2016 and, at the moment, he is collaborating as PostDOC senior researcher with UNICAL and VSB-TUO. He is peer reviewer and TPC member of different international conferences, as well as for many international journals, such as IEEE TVT, COMMLETT, VTM, SPRINGER TELS, MONET, ELSEVIER VEHCOMM, COMNET, SIMPAT, JESTCH. His research interests include mobile communication networks, QoS architectures and interworking wireless and wired networks, network security, mobility modeling for WLAN environments and mobility analysis for prediction purposes. He published more than 100 papers among International Journals, Conferences and Book Chapters.

Mauro Tropea was born in 1975 and graduated in computer engineering at the University of Calabria, Italy, in 2003. Since 2003 he has been with the telecommunications research group of DIMES. in the University of Calabria. In 2004 he was awarded a regional scholarship on Satellite and Terrestrial broadband digital telecommunication systems. His research interests include satellite communication networks, QoS architectures and interworking wireless and wired networks, mobility models and vehicular issues.

Miroslav Voznak was born in 1971, he received the PhD. degree in telecommunications from the Faculty of Electrical Engineering and Computer Science, VSB-Technical University of Ostrava and completed his habilitation in 2002 and 2009, respectively. He was appointed Full Professor in Electronics and Communications technologies in 2017. He is an IEEE senior member and has served as a member of editorial boards for several journals, such as Sensors, Journal of Communications, Elektronika Ir Elektrotechnika or Advances in Electrical and Electronic Engineering. His research interests focus generally on information and communication technologies, particularly on the quality of service and experience, network security, wireless networks and also on big data analytics. He is author or co-author more than one hundred articles in SCI/SCIE journals.

Floriano De Rango graduated in computer science in October 2000, and received the Ph.D. degree in electronics and telecommunications engineering in January 2005, both from the University of Calabria, Italy. From January 2000 to October 2000, he worked in the Telecom Research LAB C.S.E.L.T. in Turin with a scholarship. From March 2004 to November 2004, he was a visiting researcher at the University of California at Los Angeles (UCLA). He is now an assistant professor in the DIMES Department, University of Calabria. He received the Young Researcher Award in 2007 and is a reviewer and TPC member for many International Conferences and a reviewer for many journals such as IEEE Communication Letters, JSAC, the IEEE Transactions on Vehicular Technology, Computer Communication, Eurasip JWCN, WINET, etc. His interests include distributed wireless networks, internet of things, adaptive wireless networks, ad hoc and sensor networks, pervasive computing, satellite networks, and IP QoS architectures. He published more than 180 papers among international journals and conferences. He founded two startups working in the field of Internet of Things and Wireless Advanced Broadband Telecommunication Systems. One of his startup “Spintel srl” (www.spintel.it) has been awarded by Intel as one of the best 20 promising startup in Europe in the Intel Business Challenge Competition in 2013. He is a member of the IEEE.