2009 First International Conference on Advances in P2P Systems

Environmental security in P2P networks

Díaz-Verdejo, J.; García-Teodoro, P.;
Maciá-Fernández, G.
Dpt. Signal Theory, Telematics & Comm. — CITIC-UGR
University of Granada
Granada, Spain
e-mail: *{jedv,pgteodor,gmacia}@ugr.es*

Soriano-Ibáñez, M.
Dpt. Telematics Engineering
Politechnic University of Catalonia (UPC)
Barcelona, Spain
soriano@entel.upc.es

Abstract— **The great impact and growth of P2P networks in recent years make them an interesting target for hackers. But the development of P2P is aimed at improving the behavior of the networks, in computational terms, or to hide the transactions from observers. Security in P2P networks has been usually undervalued and not taken into account. This paper tries to highlight the major topics and challenges regarding P2P security, from a network infrastructure point of view (environmental security), providing some insights in current developments and available techniques that could be used to solve those problems.**

Keywords: P2P security; Intrusion detection; Anomaly detection; Network attacks.

I. INTRODUCTION

Network services have been traditionally offered according to the client-server paradigm. However, in the last years, more and more efforts are devoted towards offering services and resources in a totally distributed way, being the *peer-to-peer* networks (P2P) one of the winner technologies in this approach. According to [1], "P2P is the sharing of computer resources and services by direct exchange between systems". In P2P environments, all the nodes (peers in the P2P terminology) play, a priori, the same roles. This way, a peer offers services or resources to the community, while at the same time, it can consume services/resources from others. Thus, a more technical definition is provided in [2], stating that a P2P network is "a distributed network architecture, where the participants of the network share a part of their resources, which are accessible by other peers directly, without passing intermediary entities". From the security analysis point of view, the key point in P2P networks is the direct exchange between peers which "met each other" just for the current transaction. Usually, there is no a priori knowledge about the peer providing the resource nor its trustworthiness, as is the case in the client-server model, for which the server and the provided service are publicly known and the clients access an specific server (apart from load balancers and/or server farms). In this case, a malicious node can hide itself among all others and, for example, monitor the traffic that users submit to the network, inject false resources that prevent users accessing desired resources or impersonate known nodes in the network.

In recent years P2P systems have become more and more popular due to the appearance of applications that offer a platform for the exchange of any content type. From the supposedly first system, Napster, in the 90s to current systems as Emule or BitTorrent, a big shift in underlying technologies and social impact has been observed. But those systems are not only used in a content sharing scenario. Applications such as SETI@home or Skype have shown the possibilities of P2P technologies in other contexts, enabling systems for the distributed storage of information, computational resources sharing, web-caching and alike.

This way, the evolution of P2P underlying technologies has been driven by two main different motivations. On one hand, the improvement of the performance and the applicability of P2P systems leads, for example, to better search algorithms, novel architectural approaches and better resilience and error tolerance. Thus, these systems are evolving towards other more systematic and organized architectures such as JXTA [3] or JMobiPeer [4], whose goal is to provide a solid ground for high availability and scalability applications. On the other hand, legal aspects motivated changes in the technology. The big popularity of sharing networks can be mainly attributed to the possibility of exchanging copyrighted material without paying the corresponding property or intellectual rights. The war against piracy promoted by right owners, with cases as notorious as Napster paying a big fine and going out of business, enforced system designers to consider the legal issues. This way, more decentralization is being used just to avoid legal liabilities, as no single user or machine will be responsible for the global functioning of the system. At the same time, transactions among peers are increasingly hidden by means of port randomization and ciphering, among other techniques [5]. This way, service providers have a difficult task in detecting and filtering out P2P traffic, just in the hypothesis they were interested or forced to do so. Furthermore, right owners or authorities will face even legal problems in detecting copyright violators as the traffic

978-0-7695-3831-0/09 $26.00 © 2009 IEEE
DOI 10.1109/AP2PS.2009.29

IEEE computer society

should be decoded to demonstrate the contents. Those “distributing & hiding” techniques are adopted in most popular P2P sharing networks as BitTorrent and Emule.

Nevertheless, few efforts have been made in the direction of improving the security of the P2P networks, as the users are usually not worried about it. Most users (peers) are worried just about accessing to a resource, name it a file or a computation service, and “using” it. But P2P technologies pose some serious new threats to networks and users. First, due to its widespread use, they constitute an interesting target for hackers just as an enabling technology to perpetrate intrusions or attacks (*e.g.* new vulnerabilities) and as a vector or tool for more sophisticated attacks (*e.g* worms or viruses distribution, users’ profiles creation, etc.). Second, as the connections are established among equals with no previous knowledge, the trustworthiness of peers is not guaranteed.

Therefore, security risks can range from simple leechers accessing to resources without any cost or contribution to the community to rapid widespread deployment of viruses and worms. Furthermore, it is relevant that, according to the last reports, traditional botnets are migrating from more or less sophisticated client-server architecture to pure P2P networks. The above mentioned tendencies in P2P developments even increase the associated risks. In this context, preventive and proactive security in P2P networks becomes a must.

According to the scenario described, the present paper focuses on the study of some of the open issues in terms of security, operation and design in P2P environments, integrating distinct networks with special emphasis on the security of the nodes themselves.

The rest of the paper is structured as follows. In Section II, major security concerns in P2P networks are identified and briefly described. Among them, the so-called environmental security is presented. Section III is devoted to the description of environmental security and its different aspects and possible associated risks. In order to avoid those threats, some comments on the available technologies are presented in Section IV, while the challenges to improve, adapt or develop specific tools are described in Section V. Finally, some concluding remarks are drawn in Section VI.

II. Main Security Topics in P2P Environments

As seen in the preceding paragraphs, although it is consistently widespread, P2P technology still presents a number of shortcomings that should be resolved in terms of security, operation and design. Next we will briefly describe the main open issues and point to some methodologies and techniques available.

A. Copyright protection

The distribution of contents through P2P networks greatly simplifies the illegitimate and massive distribution of copyrighted content. The copyright protection can be achieved through two types of strategies: a priori protection (prevent from copying) and a posteriori protection (detection of copy). The a posteriori protection seems to be the only mechanism with any chance of success; in this case the system does not avoid the users to change or to illegally redistribute the document, but they are discouraged from doing so, since they can be identified. The primary purpose will be to avoid, or at least reduce, the attacks that malicious users can perform when acting alone or when colluding with others. The usual techniques for solving this problem are watermarking and fingerprinting, the latter through schemes with traceability properties.

There are various schemes in the literature with tracing properties for easy identification of fraudulent behavior when sensitive or proprietary information is made available to a large number of users [6] [7]. These schemes are valid in general when the number of colluders is small, and the associated decoding schemes are not computationally efficient [6] [8], which could not be the case in P2P networks.

B. Trustworthiness

In P2P networks users continuously access resources provided by other unknown users which, therefore, can be untrustworthy. All these interactions in which the nodes act both as clients (asking for resources) and servers (providing resources) can be used to know the degree of confidence that can be put into the nodes with which one has interacted (reputation). This reputation information can be stored and shared using reputation systems. This way, a reputation system could be used to determine which nodes are trustworthy and which are not. Usually, reputation is used in the process of request for resources to decide what the best supplier is. In fact, reputation may be taken into account when making any kind of decision that requires interaction with other nodes.

There are different types of reputation systems. The simplest ones are local reputation systems, in which the reputation information comes solely from own experience, and it is stored locally without being exchanged with any other entity. Other more sophisticated systems take into account the reputation of others. For instance, Xrep [9] is a protocol based on votes for a Gnutella-like environment that provides facilities such as assignment, sharing and combination of reputations. The reputation systems based on transaction certificates [10] exchange reputation information by sending certificates, which can be either of satisfaction or complaint.

C. Privacy

In some cases, the taste, interests, behavior and social structure of the contacts of a user set up the search that will later be compared with the network resources. This requires collecting large amounts of personal user information [11]. This information is so sensitive that it should not be exposed to malicious nodes invading the privacy of users. The distributed computing environments with large replication of information are an added problem because the user cannot control where his/her private information is being stored [12].

D. Prevention and protection against attacks and intrusions

P2P nodes act as information servers and as such they are susceptible of suffering different types of attacks. Security related to the protection of the nodes that comprise the P2P network can be called "environmental security" [13], in contrast with the security relative to the exchanged information.

This is a broad topic as it includes many kinds of risks, mainly related with vulnerabilities, both in the applications deployed at the nodes or in the network software or protocols, and/or with deficient security policies. The security mechanisms that can be considered at this level to prevent or mitigate the risk includes virus scanners, firewalls, intrusion detection systems (IDS), virtual private networks (VPN), service specific protection, honeypots, etc. Some of those systems are the subject of active research (*e.g.* IDS, virus detection) while others are more consolidated (*e.g.* VPN, firewalls). Anyway, those technologies cannot guarantee the security of the systems and therefore more efforts are needed to improve the technologies or to develop new technologies.

The next section details some relevant aspects of environmental security and the associated threats in the context of P2P networks.

III. Environmental Security Threats

In a first approach, the attacks to nodes in P2P networks and, by extension, to the network itself, can be divided into two categories according to their specificity. The first one includes the attacks that are not specific to P2P networks, that is, those attacks that, although are performed against nodes of the network, do not exploit the P2P networking peculiarities. Therefore, the prevention, detection and response techniques and mechanisms required to secure the network and the nodes are common to any network and profusely described in the literature.

The second group considers attacks related to the nature of the P2P network or the associated software. For this, two complementary approaches can be considered. On one hand, specific measures and techniques have to be developed and, on the other hand, the general techniques available have to be adapted to the particularities of the scenario and the attacks.

In this sense, in what follows, the study will focus in the second category, as it requires specific developments.

A. P2P specific environmental security

The first aspect to consider is the existence of P2P specific attacks and threads and a general overview of the most representative types.

A study of P2P attacks can be found in [14]. Among the specific P2P attacks, we can mention the propagation of viruses and/or worms that use the P2P infrastructure, file poisoning, the routing attacks against requests or searches, the denial of service attacks (DoS), and those attacks that exploit P2P software vulnerabilities to access to P2P nodes. The presence of a Trojan in the software of Kaaza constitutes an example of the last type of attacks.

The propagation of viruses and worms in P2P networks presents specific characteristics with regard to the habitual form of propagation through the Internet [15] [16]. In particular, P2P propagation is much faster and, consequently, implies greater security risks. Several studies that try to analyze and to model the propagation of this type of threats in the network can be found in the literature [15] [16].

On the other hand, routing attacks consist in sending malicious information to the network, for instance by using the request and search information mechanisms of the P2P network [14] [17]. These attacks not only degrade the quality of service, but can also be used as part of other more sophisticated attacks. The problems associated with P2P networks are very similar to the routing problems that arise in ad-hoc networks.

Vulnerability attacks appear not only in P2P but almost in any networking scenario. Nevertheless, they are specific to the targeted application or protocol in the sense that they exploit a concrete flaw in the design, implementation or operation of the target.

File poisoning consists in the injection of fake files in a P2P sharing system [14]. Although it can be seen as innocuous by many authors, it can be considered as a P2P specific kind of DoS attack, as it wastes network resources (*e.g.* bandwith) and users' resources that could be used in other transactions.

In general, DoS attacks cause the incapacity of the nodes to access to the desired resources. DoS attacks can be generic or specific for the P2P network depending on the mechanism used to generate the attack. In this sense, the most used and best known techniques to generate DoS attacks are brute force and vulnerability attacks. In the first case, the attack is unspecific to P2P networks as it consists in sending a very high number of service requests yielding to the saturation of the service (flooding). In the second case, the attack is carried out by sending a specially crafted message exploiting the vulnerability, that is, it falls in the category previously discussed. In this context, it is worth to mention the "Sybil" attack [18], in which a single entity presents multiple identities thus affecting the behaviour of the system by controlling some key properties or mechanisms of the network (e.g. reputation scores or routing mechanisms in ad-hoc networks). However, recently new DoS methods based on timing schemes that give rise to the so-called low-rate DoS have appeared [19] [20] [21]. This kind of attacks are somewhere “in the middle”, as they use a general strategy (unspecific) and some knowledge concerning the service (specific). Up to now, it is not clear whether P2P networks are vulnerable to this.

As previously mentioned, the threats just described do not constitute an exhaustive list of the existing ones. Anyway, they allow the reader to take a snapshot of the possible problems and their diversity. Furthermore, new kinds of attacks with high specificity may appear.

IV. Overview of Available Security Technologies

The security of the P2P network should be addressed taking into account prevention, detection and response to previously described attacks and to potential new attacks.

Apart from passive measures related with the configuration of the supervised elements, the most useful technologies when securing nodes and/or networks from network-based attacks are firewalls, IDS [23] and honeypots/honeynets. An interesting alternative to IDS are the so-called intrusion prevention systems (IPS), which consider not only the IDS but also response mechanisms. We do not consider antivirus at this point as a differentiated technology due to two reasons: they are effective once the attack packets have reached the node and the technologies used are very similar to those used in IDS.

Up to now, most of the used techniques are not specific to P2P networks but a general solution. This can be a suboptimal approach, as no knowledge is incorporated into the countermeasures regarding the properties or characteristics of P2P networks. This point is especially important when IDS are considered. As recent research points to [23], in the intrusion detection field it is relevant to apply the detection in a per-protocol basis, as the performance of the detection is clearly higher. For this reason, specific security measures and technologies should be developed and deployed for securing P2P networks. For this, it is possible both to adapt currently available systems to the peculiarities of P2P protocols and to develop new techniques.

On the other hand, some of the attacks described in the previous section are highly specialized (*e.g.* the Sybil attack) which made room for specialized prevention/mitigation and detection methods. Nevertheless, this implies to analyze each individual attack in order to develop ad-hoc countermeasures or detection criteria. This is clearly not adequate due to various reasons among which the lack of scalability and the delay between the discovery of a new attack (zero-day attack) and the deployment of the solution are the most relevant.

An alternative approach can be based in the adaptation of IDS technologies to detect anomalies in the operation of the P2P network. The idea is to detect abnormal activity patterns in the contents distribution, connection activity and responses to requests in order to establish a relationship between these patterns and virus propagation or routing attacks. The scheme should also be able to detect anomalies in the usage of the P2P protocols, with special emphasis in the message exchange. This is important because abnormal message exchange is usually related to vulnerability attacks. In this context, there exist many detection algorithms and techniques described in the literature [23] that are good candidates to be adapted for the P2P case. Among them, techniques for anomalies detection based on learning like SSM [24], N3 [25], genetic algorithms and stochastic models for network traffic seem promising.

Once the detection has been triggered, some response should be activated. The simpler approach is to alert the administrator and let him/her decide the corrective actions. This is the approach in the IDS case. Other more sophisticated responses to be considered against malicious node detected are the automatic configuration of an application firewall, the deployment of honeypots/honeynets [26] and the interaction with reputation mechanisms.

V. environmental Security Challenges

In order to develop security mechanisms and systems for P2P environmental security, the following topics should be addressed:

- *Intrusion detection techniques.*
  Improvements in intrusion detection techniques are required as the current performance of both anomaly-based and signature-based IDS is not optimal. This is a general concern in the IDS field. On the other hand, it is necessary to adapt current techniques to take advantage of P2P peculiarities. In this sense, more research in applying IDS systems to P2P is required. Although many detection approaches are described in the literature, not all of them are applicable to the P2P case and it is expected that the performance of the techniques will vary in this case. Therefore, comparisons among available technologies, aside with new developments are required.

- *Analysis of attacks and vulnerabilities.*
  Although some attacks and categories of attacks have been presented, a more detailed study and categorization is needed. It is interesting to identify the common aspects of P2P attacks and the approach or flaw used to carry out each attack to ease the adoption of more general solutions instead of per-attack measures. A taxonomy of the attacks in P2P environments would be very helpful for that.
  On the other hand, it would be valuable to have tools for the generation of attacks in an automatic or semiautomatic way. These tools are useful for testing purposes.

- *P2P protocols modeling*
  The knowledge of P2P protocols is useful to detect possible flaws in the design and development of security measures. In fact, some of the available

techniques for intrusion detection make use of some knowledge concerning the protocols and their implementation [27]. Unfortunately, the most used P2P protocols lack of official specifications or present many variants and extensions. In this sense, the specifications use to be obtained by reverse engineering the software or by monitoring their activity [28] [29].

- *Acquisition of real P2P traffic.*
  A key point for the development of anomaly-based intrusion detection systems is the need of data collected from the normal operation of the monitored system in order to deduct a normality model for the target environment. This information has to be captured in a real environment under normal working conditions in order to avoid biases in the model [30]. The same applies in the case of reverse engineering a P2P protocol.
  Therefore, it is necessary to monitor and to capture the P2P traffic that is flowing through the network. For this purpose, either passive or active approaches at application level can be used [31]. The passive approach requires administrative rights over the network monitored (access to routers is advisable) and arises some legal issues, although would be the best approach as no additional traffic is generated and all the P2P traffic flowing through the network can be captured. On the other hand, the active approach is simpler to carry out, as only monitors the data entering or leaving a given P2P node. In this case, there are no legal issues but at the cost of lower quality in the information captured as it is partial (only data flowing through a single node) and may be biased.
  On the other hand, for training the detectors or infer the protocol models, the traffic has to be normal and acceptable traffic, *i.e.* no attacks can be included, as the model is built from it. This way, the traffic should be real and "clean", but it is difficult to preserve both the properties and there is no control over the clean aspect in real networks. This problem still remains unsolved, although some methods have been proposed in order to, for example, filter out attacks in the captured data by using IDS. But this is a vicious cycle, as a perfect IDS is needed to filter the attacks in the training stage.

- *Traffic categorization.*
  Another important aspect to be considered is the need to detect P2P traffic among the whole traffic flowing in the network. Apart from a valuable tool for service providers in order to discriminate, filter out or prioritize the traffic flows, the capability to differentiate P2P traffic is a premise for the correct application of security tools based in P2P specificities. Additionally, as previously stated, many of the other topics discussed in this section require the disposal of traffic captured in operating networks for which this capacity of classification is required. The problem is far from trivial as the usage of occultation techniques is usual (*e.g.* port randomization, ciphering), mainly in sharing networks, to avoid legal issues. Although some approaches in this line are described in the literature [32] [33], they are based in the inspection of the payloads, which introduces legal problems and is useless if ciphering is enabled, or try to detect patterns of activity in the connectivity of the nodes. This later approach just detects with some precision whether a node is generating P2P traffic, not which the P2P flows are. Therefore, more efforts are required to obtain a satisfactory result in this direction.

- *Response mechanisms.*
  As previously mentioned, current response mechanisms are mainly based on the interaction with firewalls and honeypots deployment. But, in the context of P2P, with a high number of ports and addresses in operation, it could be very difficult to properly configure firewalls to filter out attacks. Furthermore, some attacks as worm distribution present some kind of collaborative behavior which is very difficult to avoid by simply configuring rules in a firewall.
  On the other hand, the deployment of honeypots in P2P networks requires techniques and methods oriented to make them attractive [34], which is not as easy as in other contexts, due to the distributed nature of the service provided.

VI. Concluding Remarks

Peer-to-peer applications have become one of the most successful alternatives for the storage and distribution of contents. However, until this moment there has not been a real emphasis on the security in this type of networks, probably due to the type of content exchanged at present, users have not asked for it yet.

The widespread use of P2P networks requires further study of the security requirements and the development of proper tools and techniques to guarantee a degree of security in these environments. Some of the most relevant open topics in P2P security have been described, providing some insights on possible solutions.

In the same line, some current threats related with P2P networks, from the own networking perspective, have been exposed. From the analysis of the risks and currently available technologies, the challenges to improve the tools and methods needed to guarantee the environmental security have been identified.

As a result, it is clear that there still exist open problems in P2P environmental security that have to be promptly addressed.

ACKNOWLEDGMENTS

This work has been partially supported by the Spanish MICINN under projects TEC2008-06663-C03-01 and TEC2008-06663-C03-02.

REFERENCES

[1] D. Milojicic et al.; Peer-to-peer computing, Technical Report, 2002. http://www.hpl.hp.com/techreports/2002/HPL-2002-57.pdf.

[2] Schollmeier, R. A.; Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications; In Proc. of the First International Conference on Peer-to-Peer Computing (P2P01), 2002.

[3] Project JXTA. Jxta - p2p for java. http://www.jxta.org/, 2006.

[4] O. Tomarchio, M. Bisignano, and G. D. Modica; An infrastructure-less peer-to-peer framework for mobile handheld devices, European Transactions on Telecommunications, 15(6):599–612, 2004.

[5] Madhukar, A., Williamson, C.; A Longitudinal Study of P2P Traffic Classification; In Proc. of the 14th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS '06), 2006.

[6] A. Barg, G. R. Blakley, G. Kabatiansky, Digital fingerprinting codes: Problem statements, constructions, identification of traitors, IEEE Trans. Inform. Theory, 49, 4, 852--865, 2003.

[7] D. Boneh, J. Shaw, Collusion-Secure Fingerprinting for Digital Data, IEEE Trans. Inform. Theory, 44, 5, 1897--1905, 1998.

[8] M. Fernandez and M. Soriano, Identification of Traitors in Algebraic-Geometric Traceability Codes, IEEE Trans. On Signal Processing, 52, pp 3073—3077, 2004.

[9] Damiani, E.; di Vimercanti, D. C.; Paraboschi, S.; Samarati, P.; Violante, F.; A reputation-based approach for choossing reliable resources, in peer-to-peer networks. In Proc. ACM Conference on Computer and Communications Security, 2002.

[10] M. Gupta, P. Judge, and M. Ammar. A reputation system for peer-to-peer networks. In Proc. International workshop on network an operating systems, pages 144–152, 2003.

[11] K. Sripanidkulchai, B. Maggs and H. Zhang, “Efficient Content Location using Interest-based Locality in Peer-to-Peer Systems”, In Proc. 22th Annual Joint Conference of the IEEE Computer and Communication Societies, 2003.

[12] R. Hasan, Z. Anwar, W. Yurcik, L. Brumbaugh and R. Campbell, “A Survey of Peer-to-Peer Storage Techniques for Distributed File Systems”, In Proc. International Conference on Information Technology: Coding and Computing (ITCC’05).

[13] J. Kim, Hae-Kyeong, Park, E. Paik, Security issues in peer-to-peer systems, In Proc. Int. Conf. Advanced Communication Technology, 2005, vol. 2, pp. 1059 – 1063, 2005.

[14] B. Pretre, Attacks on Peer-to-Peer Networks, Semester Thesis, Dept. of Computer Science, Swiss Federal Institute of Technology (ETH) Zurich, 2005. Available at http://dcg.ethz.ch/theses/ss05/freenet.pdf

[15] Y. Zhou et als. "Breaking monocultures in P2P networks for worm prevention", In Proc. V Int. Conf. on Machine Learning and Cybernetics, pp. 2793-2798, 2006.

[16] W. Yu, C. Boyer, S. Chellappan, D. Xuan, "Peer-to-peer system-based active worm attacks: modeling and analysis", 0-7803-8938-7/05, pp. 295-300, 2005.

[17] M. Castro et als., Secure routing for structured peer-to-peer overlay networks, ACM SIGOPS Operating Systems Review, vol. 36, Issue SI , pp. 299 - 314 , 2002.

[18] J. Douceur. The Sybil Attack. In Proc. Intl Wkshp on Peer-to-Peer Systems, (IPTPS), Mar. 2002.

[19] A. Kuzmanovic and E. Knightly. Low Rate TCP-targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants), In Proc. ACM SIGCOMM 2003, Aug. 2003, 75-86.

[20] Maniatis, P., Giuli, T., Roussopoulos, M., Rosenthal, D. S., and Baker,. Impeding attrition attacks in P2P systems. In Proc. of the 11th Workshop on ACM SIGOPS European Workshop (Leuven, Belgium, September 19 - 22, 2004). EW11. ACM, New York, NY, 12. DOI= http://doi.acm.org/10.1145/1133572.1133601.

[21] G. Maciá-Fernández; J. E. Díaz-Verdejo; P. García-Teodoro; Evaluation of a low-rate DoS attack against iterative servers, *Computer Networks,vol. 51, pp- 1013-1030, 2007.*

[22] Dumitriu, D., Knightly, E., Kuzmanovic, A., Stoica, I., and Zwaenepoel, W. 2005. Denial-of-service resilience in peer-to-peer file sharing systems. In Proc. 2005 ACM SIGMETRICS international Conference on Measurement and Modeling of Computer Systems, SIGMETRICS '05. ACM, 38-49. DOI= http://doi.acm.org/10.1145/1064212.1064218.

[23] P. García-Teodoro,, J. Díaz-Verdejo, G. Maciá-Fernández, E. Vázquez, Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & security, v. 28, pp. 18-28, 2009.

[24] J. Estévez-Tapiador, P. García-Teodoro, J. Díaz-Verdejo, Detection Of Web-Based Attacks Through Markovian Protocol Parsing, In Proc. of the 10th IEEE Symposium on Computers and Communications (ISCC 2005), pp. 457-462, 2005.

[25] J. Díaz-Verdejo, J. Estévez-Tapiador, P. García-Teodoro, Aplicación de técnicas de agrupamiento a la detección de intrusiones en red mediante N3, Actas del I Simposio sobre Seguridad Informática, pp. 101-108, Ed. Thomson, 2004.

[26] H. Lee, T. Nam, "P2P honeypot to prevent illegal or harmful contents from spreading in P2P network", In Proc. ICACT'07, pp. 497-501, 2007.

[27] J.M. Estévez-Tapiador, P. García-Teodoro, J.E. Díaz-Verdejo. “Detection of Web-based Attacks through Markovian Protocol Parsing”, In proc. 10th IEEE Symposium on Computers and Communications (ISCC), vol. 5-2, pp. 457-462, Cartagena (2005).

[28] M. Izal, Guillaume Urvoy-Keller, Ernst W. Biersack, P.A. Felber, A. Al Hamra and L. Garcés-Erice, “Dissecting BitTorrent: Five Months in a Torrent’s Lifetime”, Passive and Active Network Measurement Volume 3015/2004.

[29] L. Plissonneau, J.L. Costeux and P. Brown, “Detailed analysis of eDonkey transfers on ADSL”, In Proc. Conference on Next Generation Internet Design and Engineering, 2006.

[30] J. McHugh, “Testing Intrusion Detection Systems: A Critique to the 1998 and 1999 DARPA Intrusion Detection Evaluations as Performed by Lincoln Laboratory,” ACM Transactions on Information and Systems Security, Vol. 3. No. 4, pp. 262-294, 2000.

[31] D. Hughes, J. Walerdine, K. Lee, "Monitoring challenges and approaches for P2P file-sharing systems", in Proc. ICISP’06, pp. 18-18, 2006.

[32] S. Sen, O. Spatscheck, D. Wang, Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures, In proc. WWW2004, 2004.

[33] T. Karagiannis, A. Broido, M. Faloutsos, Kc Claffy, Transport Layer Identification of P2P Traffic, In Proc. IMC’04, 2004.

[34] H. Lee, T. Nam, P2P Honeypot to Prevent Illegal or Harmful Contents From Spreading in P2P network, In Proc. ICACT2007, pp. 497-501, 2007.