Advances in Environmental Biology, 8(12) July 2014, Pages: 1441-1445

AENSI Journals

Advances in Environmental Biology

ISSN-1995-0756 EISSN-1998-1066

Journal home page: http://www.aensiweb.com/AEB/

Examining types of attacks in Peer to Peer networks and presenting security

[1]Ali Hosseini and [2]Sajjad Baghernezhad

[1]Young Researchers and Elite Club, Beyza Branch, Islamic Azad University, Beyza, Iran
[2]Department of Computer, Darab Branch, Islamic Azad University, Darab, Iran

ARTICLE INFO

Article history:
Received 19 June 2014
Received in revised form
19 September 2014
Accepted 29 September 2014
Available online 10 November 2014

Keywords:
Peer to peer, security, attack, network

ABSTRACT

Background: The decentralized architecture of P2P networks, a dynamic system management without harmonization of a defined center and increasing internet use have led to consider such networks security very important. **Objective:** It is necessary to find different attacks and use appropriate defenses in order to secure such networks so contrary to previous studies in this article it was attempted to examine defensive mechanisms appropriate to each attack. **Conclusion:** Meanwhile, encryption and anonymous nodes were proposed as general solutions to secure P2P networks.

To Cite This Article: Ali Hosseini and Sajjad Baghernezhad., Examining types of attacks in Peer to Peer networks and presenting security. ***Adv. Environ. Biol., 8(12),*** *1441-1445, 2014*

INTRODUCTION

P2P networks were proposed as dynamic and flexible networks by standards since computer networks appearance and when internet entered into houses new and special applications were used to broadcast news and files in a way that P2P created more than 60 percent of the internet traffic. A P2P network is an overlay one embedded on internet in which all nodes are in the same level concerning their service to the nodes namely they are P2P [1].

The most accurate definition for P2P networks is as follows, "The systems completely distributed in which all nodes are equal completely and their function are similar completely"; security is proposed as a new problem due to such distributed and decentralized architecture; in other words, the essential question is how it is possible to secure a dynamic system without central harmonizer against different attacks. It is very important to identify the attacks and defensive methods to secure any network specially the P2P ones. In this article first the security importance is examined in the P2P networks and then general and special attacks of such networks are examined by presenting defensive methods. Finally we propose two security solutions related to dataflow during transfer in the network and the systems' peers; such methods are more favorable than previous ones due to inherent features [2].

2 – Security in P2P networks:

Much data are available to us due to different choices which are cheat and usually free and P2P networks applications specially file share possibility; when internet entered into houses such networks were used for special and new applications; for instance, news broadcasting and file distribution in a way that more than 60 percent of actual traffic in internet has been created by P2P networks so security is proposed seriously against threats due to users' misuse; on other hand, by virtue of the P2P networks' independence they encounter many problems to provide confidentiality, reliability, comprehensiveness, integrity and different levels of availability to users; in these networks the nodes are considered as unreliable parts and there is no supposition about their behavior in the network. Generally the P2P networks security is examined in following categories:

Integrity: The existences cannot change the data without permission and the attackers cannot replace a deed by another one.

Confidentiality: Confidentiality guarantees the data be available to only ones who have permission [3].

3 – Attacks and Defensive methods:

3 – 1: DOS attacks:

A DOS attack causes lack of service on the network or computer. The forged packets are distributed torrentially in the P2P networks to prevent legal traffic of the network. Another type of such attack is involving a node as a prey in heavy calculations to lose possibility to reply other requests.

Corresponding Author: Ali Hosseini,Young Researchers and Elite Club, Beyza Branch, Islamic Azad University, Beyza, Iran

By virtue of several hosts the DOS attacks are more destroyer namely in the DDOS attacks the attacker may control remotely the users' system with high bandwidth and guide the attack in its favorable rate or network.

Defensive method: The first problem is to distinguish the attack. The DOS attacks using reflection are not successful in blocking a user playing some role in the attack because they are numerous.

Besides, when the attacker plays some role in the attack only directly often it is difficult to distinguish the source of the attack; that is why there is no general method to block DDOS attacks.

A technique to prevent DOS attack is pricing; before the demand computation done by clients the host gives them a puzzle so it guarantees the clients do heavy computations. Pricing may be corrected so when a host finds it is attacked other puzzles become harder and distributes them to decrease the effect of the attacks. So this method is effective in few simultaneous attacks while defeated against distributed attacks(Figure 1) [4].

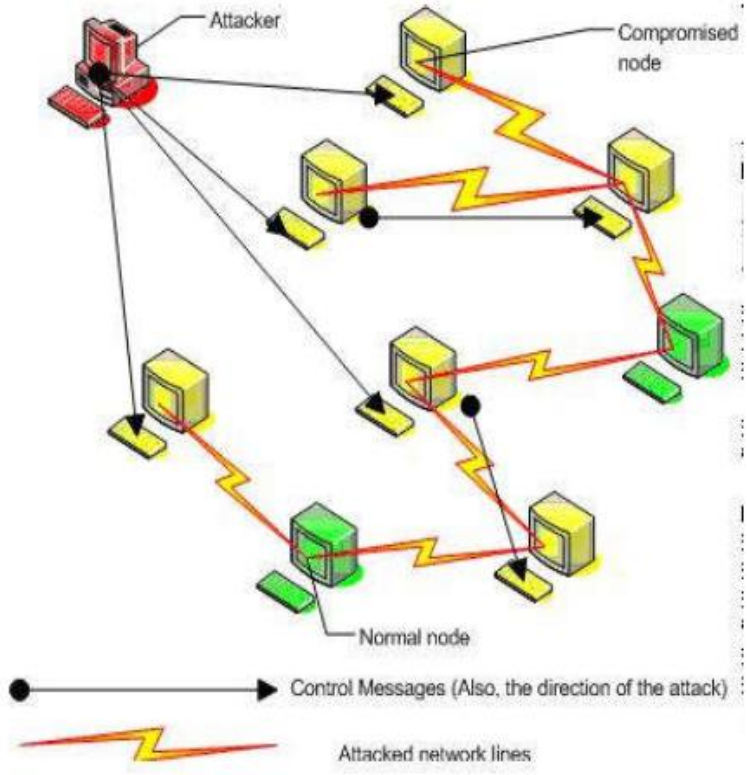

Fig. 1: DDOS attacks.

3 – 2: Man- in - the-Middle attacks:

In such attacks the attacker puts itself between two groups as an unknown element; then as an unknown element and a spy it may control the communications or manipulate actively the relation.

Such work is done by incorporating, eliminating or resending the messages during the data flow. Such attack is rarely done in P2P networks. Considering all the nodes have the same option the traffic content is shared in all so if the P2P user supports different options, the Man- in - the-Middle attack problem depends only on protocol.

Defensive method: Without a trust center (which is not usually in P2P networks) it is not possible to distinguish such attacks. The nodes have no information about their neighbors and it is not possible to take into consideration an accurate method to distinguish. Fortunately such group of attacks occurs rarely in P2P networks(Figure 2).

3 – 3: Worms distribution:

The worms have always been considered as the most important attacks in internet; nowadays they may contaminate hundreds or thousands hosts in hours. Undoubtedly the engineered worms work in very little time to achieve similar results. The worm distribution in P2P applications may be dangerous; even it can be said it is the most serious threat.

Defensive method: In defensive viewpoint it is important to know why the peer networks are effected by the worms. Following cases may answer our question:

P2P networks include computers executing similar software.

P2P applications are used to transfer big files.

Advances in Environmental Biology, 8(12) July 2014, Pages: 1441-1445

P2P programs are executed on private programs.

So a defensive method against such attacks is writing program and softwares with the least error rate(Figure 3).

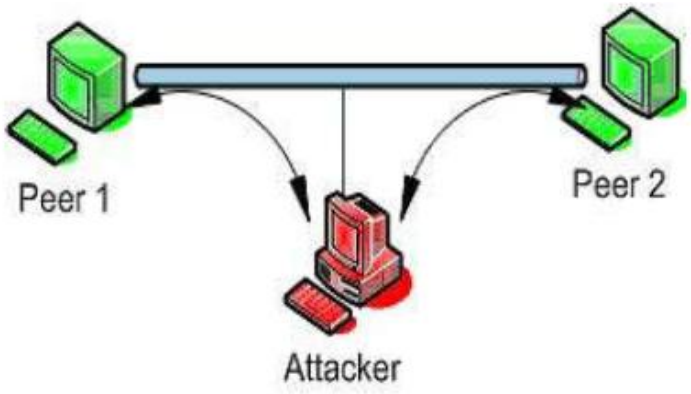

Fig. 2: Man- in- the-Middle attack.

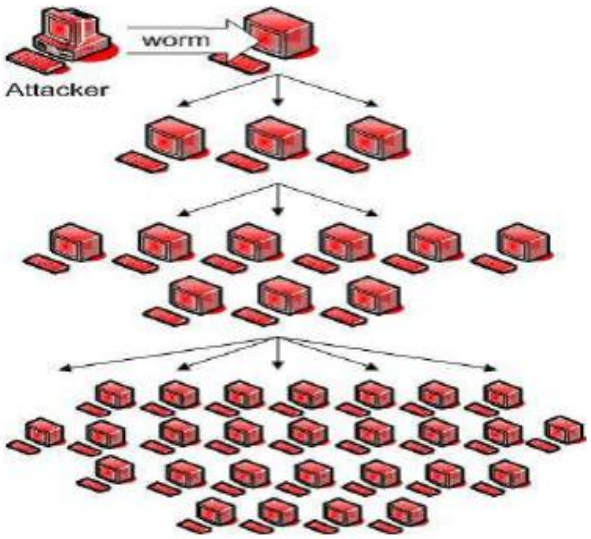

Fig. 3: Propagation worm distribution.

3 – 4: Human factors:

The human factor should be always considered as an important factor in security discussion. Unfortunately the novice users have no information about security problems in the networks so surely the attackers even with little information may benefit from this situation and penetrate into the network.

Defensive method: A user fortification specially a novice one to access the files is a serious danger. Due to queries and easy view of such users they may intentionally and without knowing share their data on another hard disc. Millions of nodes of P2P are executed unintentionally and become vulnerable for long periods. So as a defensive method it seems necessary to teach properly the users by virtue of their use of P2P applications [4].

4 – Threats and special defensive methods:

As it was mentioned before a group of attacks may be defined because of intentional features of the P2P networks; in this section we examine such attacks.

4 – 1: Rational attacks:

The cooperator nodes should interact with each other in order to have an effective P2P service, but a node is shown as an element interested in cooperation in most scenarios and there is no obligation to partnership. A rational supposition is that a high amount of the P2P nodes are rational and try to maximize the use of the system sources while they minimize the use of their sources(Figure 4).

Defensive method: The only mechanism to prevent such attacks is to create some standards in relation to how to use P2P systems so we oblige all nodes to observe some rules under defined conditions.

Out-of-band Trust: Such legalization may be executed externally to P2P systems.

Partial Centralization: A center is created to oblige the rules.

Trusted Software: If change creation is cancelled in the softwares for a user, it should operate by rules [5].

4 - 2: Sybil attacks:

When a local existence in a system selects a subset of identities to execute remote operations it may be copied several times in a remote existence. The idea of such attacks indicates an attacker may presents itself as several identities so it may have control on some part of the network.

Defensive method: As a general attitude the defensive method against the Sybil attacks is to use 'Trusted Identification Authority'. Three usual defensive methods against Sybil attacks are taken into consideration as follows:

CSS (Cooperative Storage System): Each node is defined by defining the address of IP.

NFS (Network File System): It defines the remote paths by adding an index as DNS.

Embassy: It obliges the systems by using cryptography cases installed in the hardware device [6].

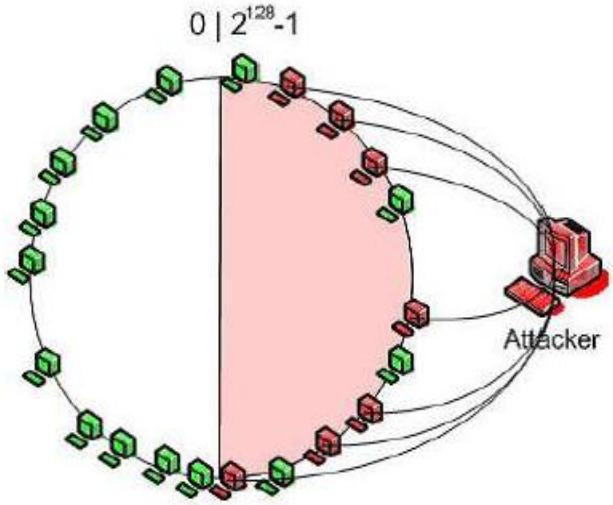

Fig. 4: Sybil attack.

4 - 3: File contamination:

In this type of attack it is attempted to enter additional and useless information into the network. Considering the P2P networks use lookup services in some way the attacker may enter many useless data into the indexes and this leads to decrease the query lookup speed.

Defensive method: When the user receives a contaminated file the security systems examine the file and then eliminate it. So after a while only the certified and without problem files are available to the user.

4 – 4: Eclipse attacks:

Eclipse attacks are more general than the Sybil ones; in this type of method the attacker may use a Sybil attack to begin an Eclipse attack, but the mechanism presented to Sybil attack is not appropriate to this method because in this method it is possible to manipulate the algorithm keeping network to attack. In this type of attacks the user divides the network in some sub-networks after having control on a series of strategic paths.

Defensive method: In this method the nodes' indegree and outdegree are used to prevent the attack. The essential idea in the method is that the indegree in the attacker node should be more than the mean of other nodes' degree during the attack so the nodes may limit the attacker by this way, but considering it may create another attack and the attacker uses the indegree of other noes and paralyses them the sound nodes should select their neighbors from the nodes with input and outgrade less than a defined rate namely both limits should be done simultaneously [7].

5 – Proposed solutions:

By virtue of types of the mentioned attacks and defensive techniques related to each one it is not possible to be safe from the attacks completely. So here two general solutions are proposed for all networks specially for P2P network.

P2P Networks Traffic Encryption: P2P Networks Traffic Encryption means the dataflow is encoded by encryption techniques not to be distinguishable easily during transfer in the network. By this method while there is real link in the network the dataflow is encrypted completely so it is not blocked, stolen or changed in P2P traffic.

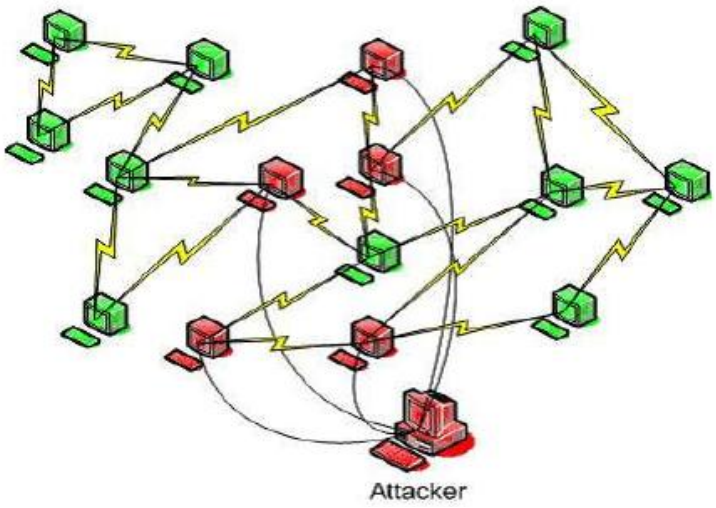

Fig. 5: File contamination.

Anonymous peers: Making peers of a network anonymous may protect the nodes' or users' identification in the network; this feature may not be secured by encryption method; as an advantage of this method we may mention that the when the peers are anonymous the attacker may hardly distinguish the origin and destination of a dataflow. The peers become anonymous by hiding identification of the users and transmitter and receiver nodes throughout the network.

Although the two proposed method have some advantages and disadvantages it is noteworthy to examine their mixture as an acceptable and safe P2P method to prevent the attacks.

6 – Conclusion:

In this article first we examined P2P networks. Then we examined the importance of P2P networks security by virtue of high traffic sustained by them in internet and general and special attacks threating them and related defensive techniques were introduced accurately. Finally P2P traffic encryption and anonymous nodes were introduced as two solutions against such attacks.

We may propose a mixture of both solutions as a mechanism for future researches and its efficiency should be examined to prevent different attacks to have more security.

REFERENCES

[1] Androutsellis, S., A. Theotokis and D. Spinellis, 2013. "A Survey of Peer-to-Peer Content Distribution Technologies", ACM Computing Surveys, 36(4): 335-371.
[2] Keong Lua, E., J. Crowcroft, M. Pias, R. Sharma and S. Lim, 2010. " A Survey and Comparison of Peerto-peer Overlay Network Schemes", IEEE Communications Survey and Tutorial.
[3] Dan, S., Wallach, 2003. "A Survey of Peer-to-Peer Security Issues", Lecture Notes in Computer Science, Springer Berlin/ Heidelberg, pp: 253-258.
[4] Autumn, Z., 2005. "Attacks on Peer-to-Peer Network" . ,http://disco.ethz.ch/theses/ss05/freenet.pdf.
[5] Seth, J., N. Scott, A. Crosby and S. Dan, 2005. "A Taxonomy of Rational Attacks", Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp: 36-46.
[6] John, R., 2012. Douceur, "The Sybil Attack", Lecture Notes in Computer Science, Springer Berlin / Heidelberg, pp: 251-260.
[7] Riedman, A. "Peer-to-Peer Security", http://citeseerx.ist.psu.edu/viewdoc/download?doi =10.1.1.60.3334&rep=rep1&type=pdf.
[8] Singh, A., M. Castro, P. Druschel, A. Rowstron, 2010. "Defending against eclipse attacks on overlay networks", Proceedings of the 11th workshop on ACM SIGOPS European workshop, Leuven, Belgium.