Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.655 – 659

RESEARCH ARTICLE

A Data and Control Integrity Infected Attacks Study in P2P Network

Anup Dogra
Student, M.Tech
Deptt. Of electronics and communication.,
Pratap university ,Jaipur,Rajasthan
anupdogra91@gmail.com

Ankit Kumar Singh
student,mtech
Department of electronics and communication
Pratap university ,Jaipur,Rajasthan
visenankit19@gmail.com

Anabik Shome
Asst. Prof.
Dept. ECE
Pratap university
anabikshome@gmail.com

Abstract—A Peer-to-Peer network is the resource and information sharing networks having the effectiveness in terms of shared network. P2P network can be a wired or wireless shared network. This network is having the security issues in terms of internal and external attacks. This network is having the attack consideration under two main aspects called the data plane and control plane. In this paper, different attack that affects the data packets or the communication controls are defined. The attacks considered in this study are Rational Attack, File Poisoning, Sybil Attack and Eclipse Attack. The paper has explored these attacks along with the detection and prevention mechanism against these attacks.

Keywords: Sybil, Eclipse, P2P Network, Data Plane, Control Plane

I. INTRODUCTION

Peer-to-Peer Network is one of the most traditional distributed networks that interconnect the nodes in a limited area network. These kind of network can be wired or the wireless. P2P networks are basically defined to share the information or the resources. This network type does not have any centralized controller or the server. Such kind of P2P network is also called Pure P2P network, Where each node as a client as well as a server[1][2].

Another common type of P2P network is Hybrid P2P network that having the same features of Pure P2P network as well as having a centralized controller or the server. P2P networks are the most effected network having its importance in file sharing systems because of the high speed and the low price communication. According to the new faster access algorithm like

Caltech's Fast Algorithm, P2P networks are about 6000 times more faster than the current internet protocols. These communication networks are capable to control and monitor the communication effective. Generally largest quantities of data is communicated over it such as movies, music, games etc[3]. The basic architecture of a P2P network as the file sharing system is shown in figure 1.

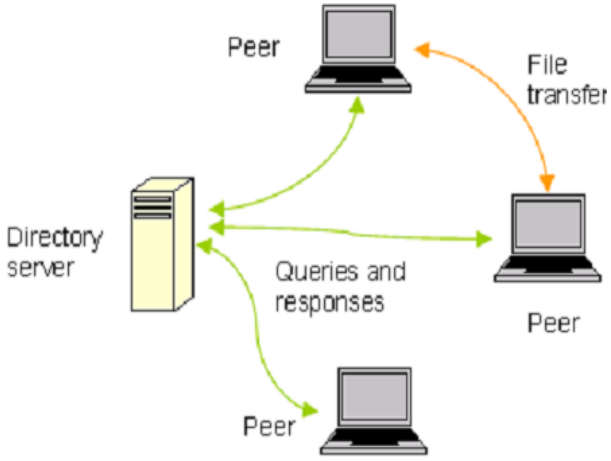

Figure 1 : File Sharing P2P Network

One of the most critical issue in P2P network is the security. The security issue becomes more critical when the P2P network is a wireless ad-hoc network. The security attack in such network is identified in such network as an inappropriate and incorrect communication activity[4][5]. Different kind of attacks or the security issues in such networks is shown in figure 2.

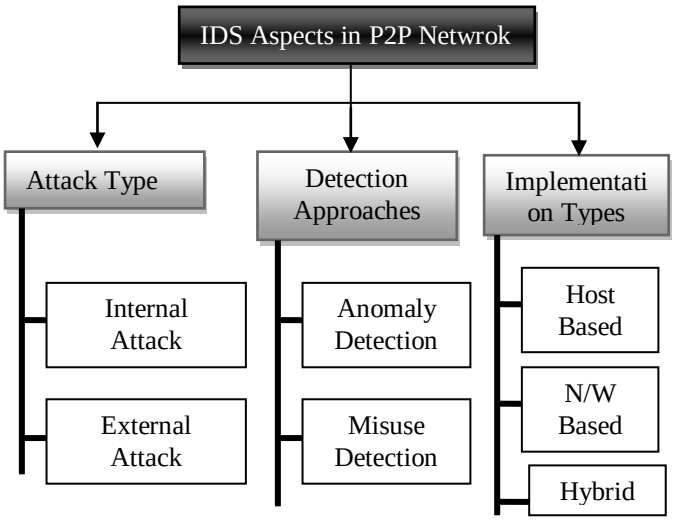

Figure 2 : Different Aspects of P2P Networks

Here figure 2 is showing the all associated terms, activities and approaches of P2P network. As shown in the figure, these networks suffer two types of attacks called internal attack and the external attack. The internal attack is performed by the network member to reveal the communicating data or to disturb the communication. This kind of attack is more critical, because the nodes have already proven the identity. These kinds of attacks are identified by analyzing the suspicious activity over the network. Internal attacks exist in wireless as well as wired network. External attacks are critical in wireless network where a new intruder not is introduced in the network[7][8].

According to the type of attack or the attack criticality, the security of the network is affected in two ways. In first way, the intrusion attack is performed over the network that actually steals the information or destroys the information. In second kind

of attack, misuse of the network communication is performed. The misuse is about to increase the unnecessary increment in the communication over the network or utilizing the available bandwidth suspiciously. To achieve the security against these kind of attack, the network communication monitoring is performed and identify the abnormal behavior of node. As the node is identified, the restriction on that node is applied or sometimes the node is set as block node. The security implementation in such network can be either host based or the network based. Host based security is applied on each node of the network and the network based security is applied on the centralized node or the gateway node. Sometimes, if the security issue is more critical, then both kind of security system can be implemented[6][8].

In this paper, the exploration to the security threats in P2P network is defined. The security threats is about the exploration of different attacks in the network. In this section, the overview of P2P network is defined along with different security aspects. These aspects are in terms of issues and the relative solution. In section II, the work defined by the earlier authors in the area of P2P security issues is defined. In section III, the exploration to the critical security threats in P2P network is presented. In section IV, the conclusion obtained the presented work is discussed.

II. EXISTING WORK

Lot of work is already done in P2P security issues. Some of the work defined by earlier researchers in this area is defined in this section. Charlier Isaksson has defined a work risk leveling to reduce the traffic anomalies. Author defined a data mining based approach to analyze the risk factors and present it as the global model. The main stress of author was on Distributed DOS attack identification. Author defined a scalable system to identify the problem and to mitigate the attack[1]. Another work on anomaly detection based on energy assessment as defined by Li Yao. Author defined the work to detect the mis-configuration in a energy specific environment. Author analyzed the energy loss and based on this analysis the attack is identified[2]. A work on the response oriented intrusion detection was defined by Peyman Kabiri. Author defined a survey to ensure the reliability of the network under the intrusion detection and prevention so that the security in the system will be improved. Author defined a feature assisted approach using honey pots to mitigate the attack[3]. A theoretical model based on distributed HMM approach was defined by rahul khanna. Author defined a frequency analysis approach to identify the attack so that the network improvement will be done. Author defined the defensive response analysis to identify the misbehavior[4].
Pengfan Yan as defined the pattern analysis based approach to secure the physical environment. Author defined the analysis on the criminal activity so that the security of the system will be improved. A RFID based authentication system along with access analysis is defined to perform the attack tracking and to provide the effective and reliable communication over the network[5]. A conditional analysis based work on intrusion detection was proposed by Kapil Kumar Gupta. Author defined the attack defensive approach under the random conditional analysis. Author defined the task analysis mechanism to mitigate the attack[6]. Jaao B.D. Cabrera has presented the classification and detection of intrusion by performing the sequence mining. Author defined dictionary analysis based approach for anomalies detection. An anomaly count based substantial analysis approach is defined by the author[7].

Sandip Ashok Shivarkar has presented a hybrid system for intrusion detection using the conditional random field analysis. Author defined the monitoring and analyzing approach based on the incident analysis as well as the threat violation analysis. Author defined an accuracy and efficiency oriented work for intrusion detection[8]. Richard J. Bolton has presented a statistical approach for fraud detection in the network. Author defined a learning approach under the defect activity analysis such as credit card fraud. Author defined tool based work for the attack detection[9]. A command based work on anomaly detection was defined by Ramkumar Chinchani. Author defined the realistic data analysis along with statistical approach for test data detection. Author defined an algorithm for dataset analysis based approach for intrusion detection in P2P network[10]. Ping Yan has presented a markov model based Poisson process analysis approach. Author used the WIPER tool for the probabilistic analysis of the anomalies. Author defined the work on the emergency situation to detection the attack. Based on this analysis a Detection and Alert System was defined by the author[11].

K. Hanumantha Rao has presented a K-Means clustering based approach for dataset partitioning and the distance similarity analysis for attack detection over the network. Author defined an algorithm approach for classifying the normal and abnormal activities over the P2P system[12]. A Human Immune System inspired intrusion Detection system was presented by R.Sridevi. Author defined the work robust and error tolerant system so that effective detection of attack will be performed[13]. Mathew G. Schultz has presented a data mining based approach for detection of malicious node or activity. A pattern analysis on the network statistics was presented by the author[14]. Christopher Kruegel presented the work on anomaly detection on web based system. Author presented the work for web servers so that the applicational statistics

analysis will be performed to detect the attack. The structural analysis along with parametric analysis was defined by the author[15].

III. SECURITY ATTACK IN P2P NETWORKS

In this section, two different kind of attack planes in P2P network are defined called the data plane and the control plane. Data Plane defines the interest of the intruder in data such as infecting the communicating data over the network. The control pane basically disturbs the functionality of the communication. The communication control attack is a slower and inefficient attack type. A network can also have these two types of attacks collectively such as the corruption of data files will destroy the data as well as disturb the downloading activity. Different attacks relative to the P2P network is shown in figure 3. Here figure 3 is showing the most critical and common attacks of P2P network. These attacks and the relative solution are defined in this section,

A) Rational Attack

The reliability of the P2P network is based on the cooperative nature of the nodes while performing the communication or the sharing of data. But if some node over the network consumes the maximum resources of the system in such case, this coordination of sharing information is disturb.

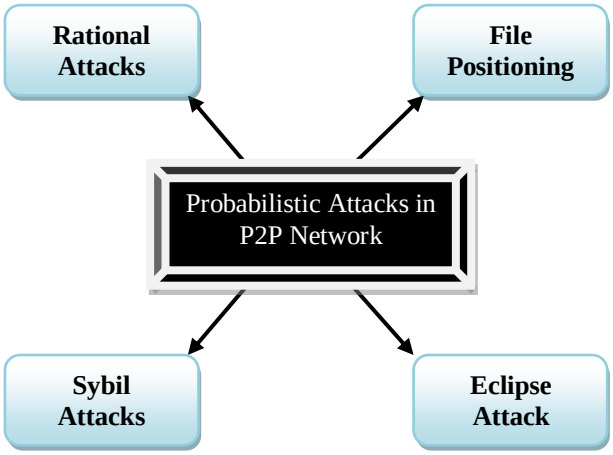

Figure 3 : Probabilistic Security Threats in P2P Network

The instability in a network is defined as the rational attack. This attack results the data loss during transmission because of less coordination between the sender and the receiver. The attack also increases the congestion possibility over the network.

B) File Poisoning

This kind of attack affects both the data plane and the control plane. This attack either infects the file over the network or replaces the file. The attack is defined as the false contents occurrence over the network. In this attack, an attacker node claims the ownership of the file and while accessing the file, replaces it with some corrupt file. This attack increases the fake copies over the network so that the availability of the network for safe communication is decreased. To overcome with this attack, a monitoring defense is required. It means while downloading or uploading the file, an inspection on file content is applied that will identify the attack and clean it if possible.

C) Sybil Attack

The control plane is the activity area of Sybil Attack. This kind of attack identifies the individual malicious identity so that the control gain over the network will be obtained. This kind of attack basically performs the control gain for the file access.

This attack also affects the counting mechanism or the sequencing mechanism of the communication so that the ordering of the packets is disturb because of which the re-communication is called again and again. This attack also increases the network traffic by performing the sequence modification. The data packet replication is also an activity of Sybil Attack. To handle this kind of attack, the central trusted authority is defined. This attack is applied on structured P2P network so that the effective reliable communication will be performed over the network. This attack is able to identify the malicious identities and the malicious activity over the network. The central trusted authority allows a reliable node to perform the communication. The type of authentication mechanism decides the security against this attack.

D) Eclipse Attack

Eclipse Attack is the next stage of Sybil attack. This attack also affects the control plane of the communication. This attack gain control over the routing information and modify the communication routes so that the reliable communication will be drawn over the network. The attack type is defined under the network and sub network based communication. This attack type includes the man-in-middle attack defined at high scale. This attack affects the strategic routing path as the man-in-middle modification. The security threat to the attack is the re-routing so that the route injection will be performed and the direction of the packet delivery will be modified.

To handle this kind of attack, the cryptographic protocol based implementation is required. This attack slow down the communication as well as handle the scalability vector over the network. This attack randomize the communication so that the effective and reliable communication over the network. Author defined the pure P2P network so that the network is randomly distributed and the control information becomes safe under the strategic route change.

IV. CONCLUSION

In this paper, the exploration to P2P network is defined along with security analysis. The paper includes the definition of different attacks over the network as well as the standard defensive mechanism. The attacks considered in this work are defined under data and control aspects.

REFERENCES

[1] Charlie Isaksson," Risk Leveling of Network Traffic Anomalies", IJCSNS International Journal of Computer Science and Network Security
[2] Li Yao," Anomaly Detection and Location with an Application to an Energy Management System".
[3] Peyman Kabiri," Research on Intrusion Detection and Response: A Survey", International Journal of Network Security
[4] RAHUL KHANNA, "Control Theoretic Approach To Intrusion Detection Using A Distributed Hidden Markov Model".
[5] Pengfan Yan," Detection of Suspicious Patterns in Secure Physical Environments".
[6] Kapil Kumar Gupta," Conditional Random Fields for Intrusion Detection".
[7] Jo˜ao B. D. Cabrera," Detection and Classification of Intrusions and Faults using Sequences of System Calls".
[8] Sandip Ashok Shivarkar," Hybrid Approach for Intrusion Detection Using Conditional Random Fields", International Journal of Computer Technology and Electronics Engineering (IJCTEE)
[9] Richard J. Bolton," Statistical Fraud Detection: A Review".
[10] Ramkumar Chinchani," RACOON: Rapidly Generating User Command Data For Anomaly Detection From Customizable Templates".
[11] Ping Yan," Anomaly Detection in theWIPER System Using Markov Modulated Poisson Process".
[12] K. Hanumantha Rao," Implementation of Anomaly Detection Technique Using Machine Learning Algorithms", International Journal of Computer Science and Telecommunications
[13] R.Sridevi," Analysis of Human Immune System Inspired Intrusion Detection System", (IJCSIT) International Journal of Computer Science and Information Technologies
[14] Matthew G. Schultz," Data Mining Methods for Detection of New Malicious Executables".
[15] Christopher Kruegel," Anomaly Detection of Webbased Attacks".

