International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 6435~6445
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp6435-6445

Analysis of threats and security issues evaluation in mobile P2P networks

Ali Abdulwahhab Mohammed[1], Dheyaa Jasim Kadhim[2]
[1]Department of Remote Sensing, College of Remote Sensing and Geophysics, Al-Karkh University of Science, Iraq
[2]Electrical Engineering Department, University of Baghdad, Iraq

Article Info

Article history:

Received Dec 21, 2019
Revised Apr 16, 2020
Accepted Jun 5, 2020

Keywords:

Attacks
Encryption
Mobile P2P network
Network security
Web threats

ABSTRACT

Technically, mobile P2P network system architecture can consider as a distributed architecture system (like a community), where the nodes or users can share all or some of their own software and hardware resources such as (applications store, processing time, storage, network bandwidth) with the other nodes (users) through Internet, and these resources can be accessible directly by the nodes in that system without the need of a central coordination node. The main structure of our proposed network architecture is that all the nodes are symmetric in their functions. In this work, the security issues of mobile P2P network system architecture such as (web threats, attacks and encryption) will be discussed deeply and then we propose different approaches and we analysis and evaluation of these mobile P2P network security issues and submit some proposal solutions to resolve the related problems with threats and other different attacks since these threats and attacks will be serious issue as networks are growing up especially with mobility attribute in current P2P networks.

Corresponding Author:

Ali Abdulwahhab Mohammed,
Department of Remote Sensing, College of Remote Sensing and Geophysics,
Al-Karkh University of Science,
Baghdad, Al-Karkh Side, Haifa St. Hamada Palace, Iraq.
Email: ali_abdulwahhab@kus.edu.iq

1. INTRODUCTION

The first appearance of peer to peer concept was file sharing system, and according to the history in 1980, Usenet used the idea proposed by Tom Truscott and Jim Ellis (the creators of Usenet) in 1979 for connecting the severs of the between each other without any central coordinate node, then it was followed by several applications like the FTP server in the 1980's [1], and in the 1997 hotline produced the idea of file exchange through the chat. However peer to peer system get its popularity and its true identity through Napstar software by Shawn Fanning a freshman student who was to thwart because of the difficulty to locate music'swhile a lot of peoples have it on their hard Disk so he created a software by taking advantage of a type of real-time Internet text messaging well known as internet relay chat (IRC), important software publishing property such as operating systems, and important search functions for different search engines named it Napstar [wki. Napstar], after that a lot of applications followed like Gnutella, eDonkey2000 (in 2000), Freenet (2001) and then followed 2003 by the bit torrent at 2002 [1].

The peer to peer model composed of many nodes that are acquired the self-organization (decentralization) which also can act like a server or a client, that's to say any node can provide resources or receive them. The following properties shown below should be available for P2P model to acquire the self-organization feature which it is most important feature for new network research trends such as IoT, M2M, 5G communications and so on [2]. These properties are listed as follows: (1) Resource Participation: Each peer in the P2P system contributes its resources with the other peer in the system, however must of P2P

systems suffer from "free rider" and the "leechers" which i will explain them in peer to peer security section. To achieve the first property, we can see is that the concept is similar to the "ad hoc networks". (2) Self-Organization: All the peers are determining locally, that's to say all nodes gain the limited information on set of the nodes that nearby [3]. (3) Networking: If we come back a little to the definition, we will conclude that all the nodes in P2P system must be interconnected with each other. (4) Decentralization: P2P is a system by which exchanging the information is done between the users themselves without any need to use a high-performance node as a central control point in the system. Although it has benefit it would represent a major security problem especially with the security we will see later. (5) Symmetry: All the nodes in the system have the same functionality and any node can act like a server or client according to the needs from that node. (6) Scalable: It means that the time of the response would not grow as the pees increase in the system but the bandwidth will grow and that make the availability of the object become big. (7) Stability: This is an important characteristic in P2P and many researches are dealing with property because at maximum churn rate. Peer to peer system must be stable. So P2P's client must know its network graph and able to route the request of the demand's node within its practical hop-count bounds. Churn refers here to either connection or disconnection of peers to and from the overlay network, which changes number of peers in the network [4]. So churn rate may give the exact number of nodes or peers that leaves the P2P network though a given time usually one hour. Really this is a big challenge to calculate the churn rate especially large scale networks. In the other side, hop-count bound is the value of hope count as the massage request to route forward between the peers before the system drop this request as no response for the request [5].

The main problem motivation of this work is the dealing with mobility at P2P Network while ensuring that security functions and mechanisms still affect to be defined by influencing business operations, and there will be trade-offs between circuit scale, wages, effectiveness, relevance, protection, and privatization. In this work, security and privacy issues will be discussed and discussed to determine the various security features used to provide privacy, safety, or provision functions. There are also some issues associated to human's identities. These issues have to be considered for networking policies and privacies, as they are necessary for effective general administration in the next technologies.

2. MOBILE P2P NETWORK MODEL

From the definition of the mobile P2P network, we can guess that it needs another system like the Internet to provide connections and to exchange and share their resources which this is simply impossible according to the global sharing of the information (by mean users for different places). Peer to peer system uses the same concept as the Internet by the mean of the overlay networks. Overlay networks that a computer network which its nodes are being considered they are connected by logical (virtual) links according to the path that would be taken to reach its destinations that could be done either by one physical link or by many links of the underlying layer [6] as shown in Figure 1. As for the Internet it is overlay on the telephone network while P2P is overlay above the third layer (TCP/IP) on the application layer. So P2P System is an overlay network over the Internet, in such a design using the overlay application layer for indexing and node discovery and the direct Internet direct connection for exchange the information, as we mentioned P2P run above the internet layer (TCP/IP) although such design allows the flexibility of communication and the availability of the object in case of peer to peer system but it would represent a major security problem with the decentralize of P2P especially defending against malwares and attackers [7] as will be discussed later. Although the mobile P2P networks can be also classified asshown in Figure 2.

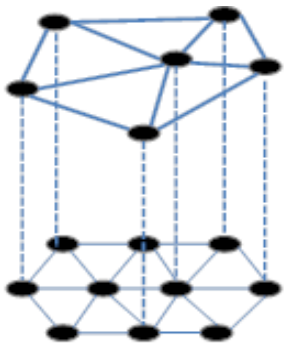

Figure 1. Overlay network over the main physical network

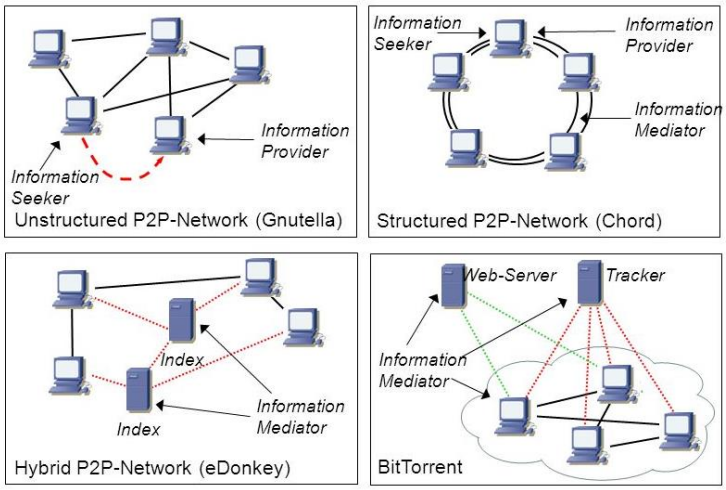

Figure 2. Different mobile P2P network structures

2.1. Structure mobile P2P network

A centralized system which it is a pure system that has in its distribution system each node knows about all nodes and the way to reach all of them in that system by gaining a routing information using key-based routing method [2, 8], in this mobile P2P network, the connection between the nodes are fixed and each use indexing method to assign a location for each node in the system, and for the node who search for a desire file (even if it is be very rare) all he have to do is to route a search (using a protocol utilize for this purpose) the network to know how many nodes that can offer the file to him (Pastry, CAN, Chord, Tapestry, Napstar) [9].

2.2. Unstructured mobile P2P network

A decentralized system pure, easy to build, free scale, low power random mobile P2P network which can be established arbitrary, each node (peer) in this system if he want to get a file he must flood query in all the network to find how many nodes can offer his desired file, also the peer depend only on the neighbor nodes to deliver the message to the other peers (Freenet, Gia, Gnutella, Fast track.....etc.).

2.3. Hybrid mobile P2P network

This network system consist of a high computing power ,performance and fast network connection node or nodes act like a (server) usually called super node, this node/nodes job is to arrange the entire network and assign the connection and location for the peers in the network (Kazaa, bittorrent) [2].

3. PROPOSED SOLUTION FOR MOBILE P2P NETWORK SECURITY

The goal this research work is to enhance the mobile P2P network's security and then we want to give a clear idea about how mobile P2P network is actually break the rule of the information security, well that is right the way that the P2P work allows the mobile user's network to be open to the other users in the network, which it will be expose to various type of attacking, theft and malware harm, also mobile P2P network sometimes allows backdoor access to the user's system information. An example on theft like an employee could steal a copyright material like software, files or (documents) of a company which they are very confidential by using any of the (Wrapster) software which they are available in the internet to disguise these files as an music files (mp3) and share it by the P2P to pass it through the company's system security and anyone outside the company can download the file and unwrap it and he will get that material, also for backdoor access and piggybacks if the software that is used for making the P2P communication if they are infected with some kind of viruses could allow the hacker to gain access to the user's system information, hard storage and bandwidth connections also for a high performance attacker he could infect may nodes in the network (malwares) causing what called Botnet [10], which can lead also a Denial of service (DDoS) [11, 12], also there are many types of attacking and also a lot some security mechanism are proposed by the research which it will discuss literary in this work. So, our proposed solution for enhancing mobile P2P network's security can be constituted from three main parts web threats avoidance, P2P network attacks avoidance and P2P network encryption.

3.1. Web threats avoidance

Before giving the famous attacks on the P2P system, we would like to address the kinds of web threats that they can expose the mobile P2P network as shown in Figure 3 below. We will show in this work that these web threats can be avoided by two ways described below.

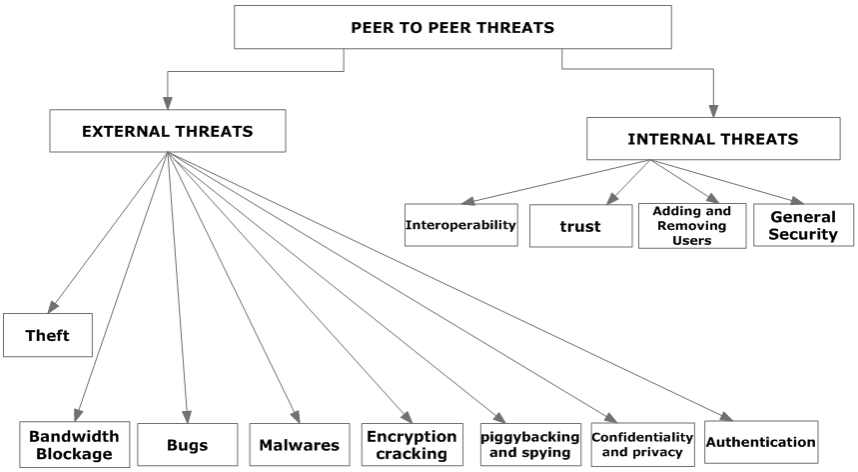

Figure 3. Mobile P2P network threats types

3.1.1. External threats avoidance

By which means a threat that comes by the fact peer to peer system is a shard system which will be exposed many threats and problems, and they are: (Theft, Bandwidth blockage, Bugs, Malwares, …, and so on). May be before reading the introduction theft problem would not be clear to the reader, but actually it's a major problem cause a lot of companies loss of millions of money because it is easy way without a lot of thinking and easy to implement with the free tools in the internet like the unwrapped. If someone (employee) want to steal a confidential files [2], all he have to is to use the wrapster to disguise the file into a music file and share it through P2Pnetwork as it will pass the company security system it will appear like a common file transaction of music files and any one from the outside can download the file and unwrap it and get the file, and you can get the result.

This work proposed the way that is P2P system uses for sharing and for searching cause the network to suffer from the heavy traffic and sometimes an Accidental denial of service. For example the decentralized unstructured P2P system, the client use a flood the query in the network for applying a probe to find how many node having his request, another example when the users in that network share a large file size like videos this may cause some logical links but many physical links, the first examples causes sometimes networks drowning by the query and the second may cause of network heavy traffic and time delay. These two examples give network bandwidth block out and sometimes an accidental DoS, sometimes bandwidth blocking can come through a malware causes a flood of query in the system which caused what is said distributed denial of service (DDoS) [11, 13]. This proposed approach can be described clearly by the following flowchart as shown in Figure 4a below.

3.1.2. Internal threats avoidance

By which mean threat that come from the network itself and its nodes, these threat can be put as a problems of the system more than threats. These internal threats are such (Interoperability, Adding or removing users, Trust and General security). For running P2P applications properly, end users have to install the required working program. If this program contains an error, the network may be exposed to a number of risks such as endangering the exchange of network information and sometimes system crashes.

P2P systems specially the unstructured system allow many computers to connect with each other, and If we talk about the safety of this large network, then we need a great deal of computing power is the coding applied to it. Such an encryption algorithm is difficult to manage with a high-performance hacker. Many researches deal with this problem. Some peer to peer application [2] gave its customers a freeaccount to the documents that are stored in that account's hard drive, this property give the hacker a good chance know what operating system that user and get access to a confidential files of that user.

Different nodes use different operating system that's mean different firewalls, different applications which create a complicated security requirement to satisfy all the nodes and determine the hackers in the system. A good method should provide an effective way to joining-leaving nodes process to/from the P2P network avoiding overloaded to the P2P system gaps. This means that most threats come from previous nodes and theywhich know to enter and exit the system, for example trapdoors... etc. In all peer to peer structures if a user request a file from the peers he cannot make sure it that peer is a trusted peer or it's just a hacker or even an infected node so this and every time he download something he must scan the file, problem make a lot of people do not depend on the P2Psystem to fulfill their needs. The proposed method to avoid such internal threats is clearly described in the flowchart shown in Figure 4b.

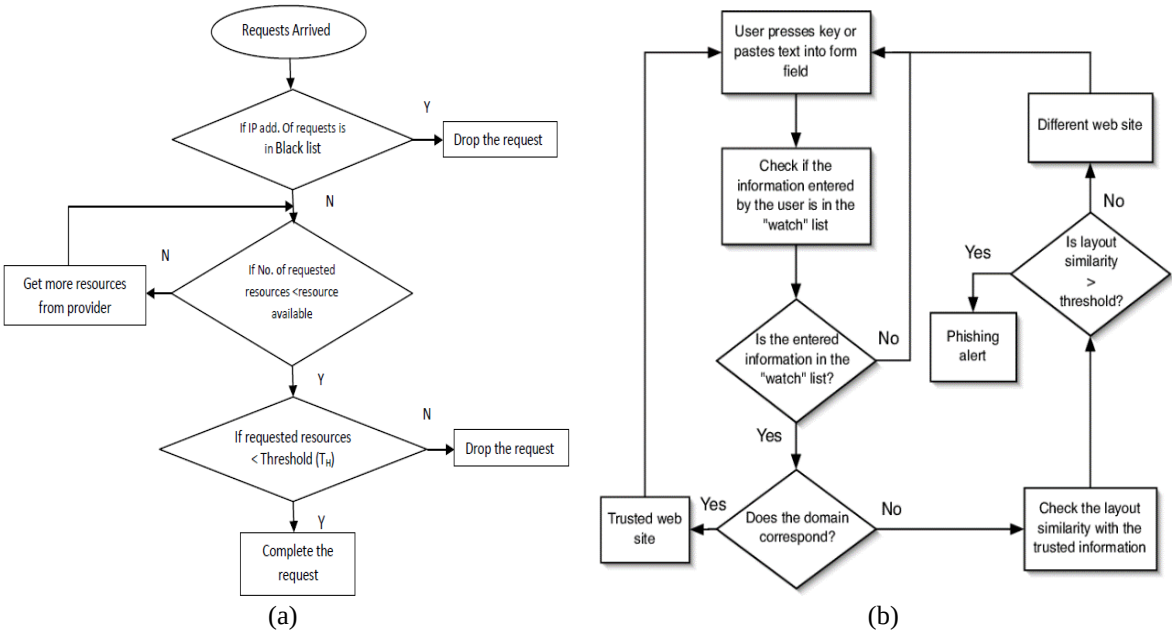

Figure 4. Proposed solution flowchart for web threat avoidance:
(a) External threat avoidance, (b) Internal threat avoidance

3.2. Attacks on mobile P2P network system

Most of the attacking on the peer to peer system causes by malwares,P2P system like another network system has a lot of attacker issues; however the most important attacks on the system according to the last papers [10-16]. We found that it has weaken the system because as we mention P2P cross the firewall boundary of clients computers, moreover for arranging the attacker that will adapt the concept of classification of [17, 18] to create newer classification of the attacker. According to that research attacking are classified into four basic class most of the attacks are under these four or a combination of them each attack lead to the other, and they are shown in Figure 5.

There is a lot of attack can be produce by the combination of the last four basic attacks but we will consider in our work the only most important called distributed denial of service (DDoS) attack. DDoS is a famous type of attacks on the whole network systems that can be launched through many ways and all the way will exhaust the sever by sending requests and not respond to it which will lead to system failure and shutdown. According to [10], in P2P system DDoS can be launch by many ways (most of the attacks from the basic class in the previous section) all of them will lead the node failure to serve the other peers in the system. Here, we will submit our proposed solutions or ways of the DDoS attackers on the peer to peer network system that can be described as follows:

- For the unstructured peer to peer system the attacker may use the query flooding nature so we will make the malicious node to send a massive query to peers without responds the will cause bandwidth Busy and overloaded which cause system to shutdown (flood DDoS [19]).
- A hacker can make use of the P2P properties(decentralized) by which make each node to act like a router as like the malicious node which the attacker will use to forward the query to a victim node overloaded him with query and closing that node [19].
- A hacker can use the infected peer to peer system so he can hack to other objects like web sites [19].

- Another kind of attack that DDoS can perform is to inject useless data, such in centralized P2P, we can inject a large amount of useless lookup-value pair into the index which will cause time latency which will led to invalid query.
- The most DDoS can be launch by either toxicityindication or routing table indication. At the beginning, a dummy record is inserted into the index indicating the target IP address and port number. When the peer searches for resources, it will receive incorrect location information from the poison index. Establish a connection with the target. If the target is accepted, DDoS for TCP connection will be started. In the second case, each other's routing table contains its neighbors O (log n), these neighbors are granted to the nodes in the network. The attacker deceives the peers and adds fake neighbors to each peer's routing table. This can be as simple as sending an advertising message to the target. As a result, the target receives a large number of communication requests [10, 14, 19].

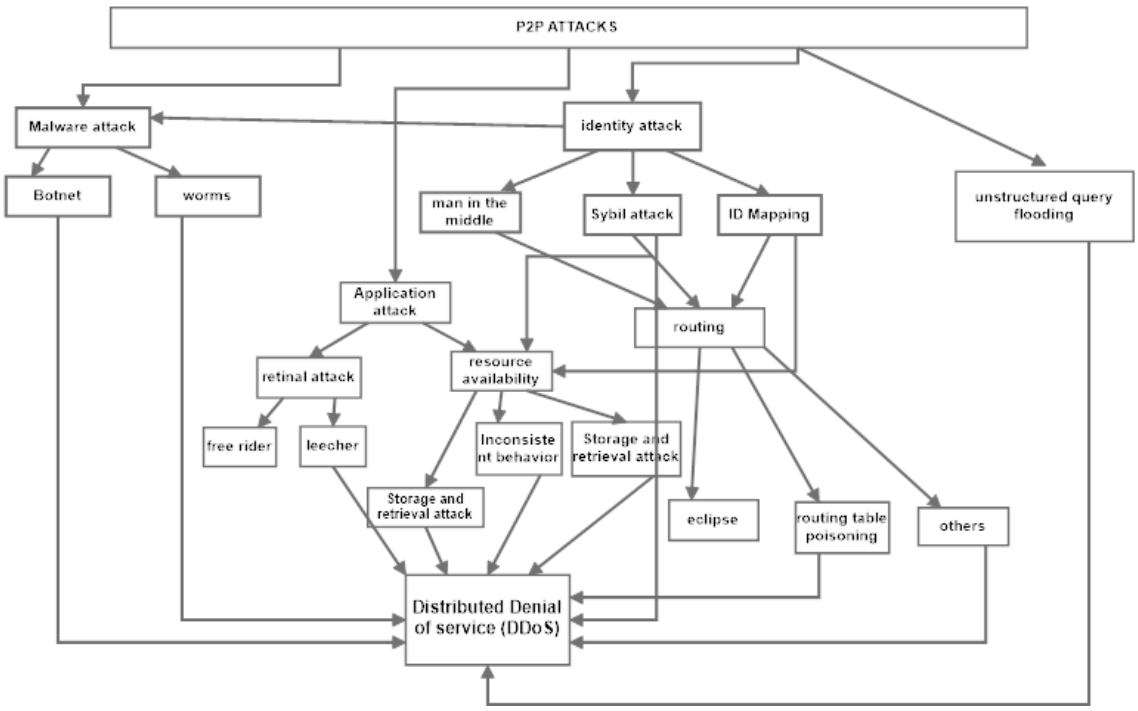

Figure 5. Mobile P2P network attacks types

By either one of these ways DDoS causes a massive harm to the P2P networks reducing the availability distract the bandwidth totally cause system destruction. When an attacker control a node or many nodes, he can launch many kinds of attack that are similar in harm to the network, such these attack like (Wrong routing forward [10]: which mean that the according to the P2P system all nodes act like a router and forward a massage between them for identification and localization, however each communication with the infected node give wrong massage or forward it to none exists node. Also Identity theft [10] and Churn attack [10, 14]: malicious node enter and exit the network continuously keep the network update its routing table in order to get the stability ,in the end it will cause to system crush.

On the other side, Worms are already considered one of the dangerous attacks on the internet. Nowadays, worms can infect hundreds of thousands of gestures within hours, and undoubtedly better engineered worms will be able to infection to reach the same result in seconds. Moreover, worm's propagation is still unknown and many research designs for that purpose [13]. So, our work proposes motivations that make the worm most uneffective attack, which:

- P2P networks are consisting of clients running the same software on their computers. If an attacker found a hole in the security of the network, he can compromise the entire system.
- P2P nodes prefer to bond with many different nodes. In fact, P2P application worms no longer lose the valuable time of other victims. You just need to bring the knot list to the victim and distribute it.
- P2P purposes are required to movebig files. Little worms must reduce its size to contain segment of TCP packet. This problem can't be considered in P2P worms and then can perform high sophisticated attitudes.

- Protocols are not generally seen to be dominant, and are therefore less concerned than intrusion detection systems.
- P2P software usually runs on a personal computer rather than a server. Therefore, an attacker is more likely to access sensitive files, such as credit card numbers, passwords, or address books.
- P2P applicantsusually transmit unauthorized content (copyrighted music, pornographic content ...), so it is unlikely to report abnormal system behavior.

Most of these motivations give the attacker a purpose to apply worms in the system. However worms are divided into two parts [11]: (1)Topology scanning: In this attack the worm utilize the information from the nodes nearby the infected one this give the worm high speed for spreading. (2) Passive scanning: This kind of worms infects the shared file in the infected computers and waits for the user to download to replicate and infect more users.

Besides the attacking issues there is also the issues of trust which is means trusting that peer that he will not expose my computer if make sharing with him. Does this sharing will jeopardize the communication of my information? how can we recognize the good peer form the malicious peer all these questions will implement by the Reputation based system [15]. Reputation is applied to make a reliability between its peers based on its previous interactions and feedback from its other peers as shown in the strategy described in Figure 6 below, as for the privacy it's need specially for the VoIP like Skype, when a node offer to help with carrying the data stream which should be encrypted but there is no assurance of this also the P2P properties means sharing with public and the private files so there some basic security like private P2P and (VPN) system and the "anonymity" [20, 21].

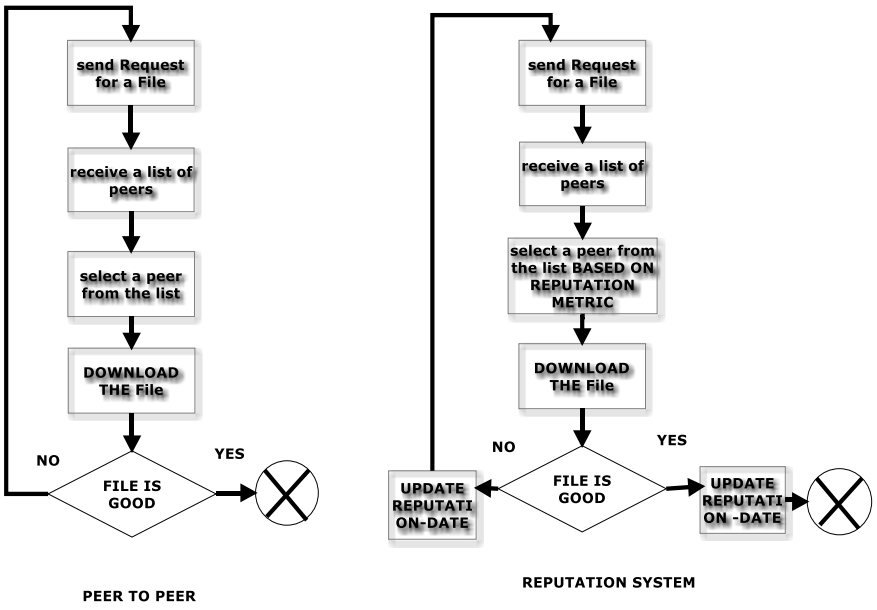

Figure 6. Reputation system strategy Vs. P2P system strategy

3.3. Encryption in mobile P2P network system

Encryption mechanisms are used in P2P system for protection from the attacking with either encrypt data stream or the connection to the other node, so that the attacking will be blocked and the attacker will fail to obtain the data stream and there are basic encryption techniques used at P2P networks as follows [22]:

(1) Secret Key Techniques: Secret key technologies rely on the incident that the transmitter and receiveradopt the secret applied in different encryption cases, e.g. encrypting and decrypting messages and creating and verifying message authentication data. This secret key must be replaced in a separate procedure before the intended connection (for example, the use of PKI).

(2) Public Key Technologies: They rely on the use of asymmetric key pairs. Usually, each user has only one key pair. One spouse is provided to the public and the other is kept secret. Since one of them exists, there is no need to exchange out-of-range keys, but the infrastructure needs to distribute the public keys in the original way. Since no pre-connection secret is required before the call, public key technology is well-suited to support security between previously unknown parties. When using public key encryption, the public key will be used to encrypt the message, but the private key can only be used to decrypt

the message. An asymmetric key pair can create the key pair mathematically linked to the secret private key and the published public key. Using these keys, you can protect the validity of the message by using the private key to create a digital signature for the message, which can be verified using the public key. It also protects the confidentiality and integrity of the message [23].

In this work, before sending an encrypted data stream the nodes, we propose using some kind of protocols to identify each other. On the other side, we propose that the nodes used between each other using some kind of private network as an Internet overlay in which the resources and infrastructure are provided by the users, and new users may only join the network by personal invitation, such a network applied to prevent the attacker from enter the system. So, we proposed to adopt using the following two approaches of encryption at mobile P2P networks as follows:

3.3.1. Proposed secure sockets layer protocol (SSLP)

Ensure that files and events sent are unchanged or invisible to anyone other than the intended recipient. Additionally, since both parties use SSL, both parties will automatically verify their identities before any information is sent over the network. The proposed protocol uses the same reliable technology used by all major website operators to protect consumer privacy and financial information sent over the Internet, and provides a mechanism to ensure confidentiality to prevent tampering with appropriate peer secrets. The following diagram Figure 7 shows our proposed procedure for encryption mobile P2P network using proposed secure socket layer protocol (SSLP).

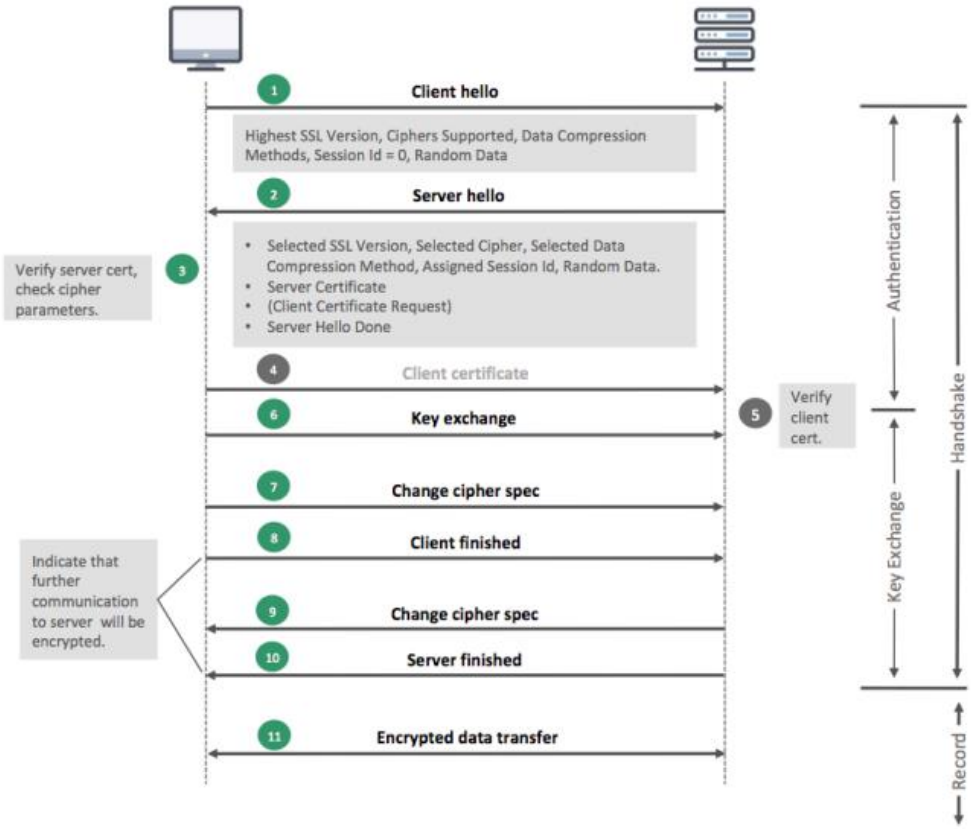

Figure 7. Proposed diagram for encryption mobile P2P network using proposed SSLP

3.3.2. Proposed virtual private network (VPN)

This is kind of private network which is linked the peers in the underlying layer while encapsulating the data and keeping it private. Our proposed VPN in peer to peer can be implemented with two kinds of protocols:

- VPN with IPSec: IP security is useful because it is most suitable for networks with remote access clients, and the security comes from the workstation's IP address or certificate (such as X.509), which specifies the user's identity and ensures the integrity of the network. The IPSec tunnel is mainly used as a network

layer to protect all the data packets that pass through, regardless of its purpose. IPSec provides two data protection mechanisms: Authentication Header (AH) and Encapsulating Security Payload (ESP), both mechanisms use security associations.

- VPNs with cryptographic tunneling protocol: to provide confidentiality by blocking intercepts and packet sniffing, we propose to allow sender authentication to block identity spoofing, and provide message integrity by preventing message alteration.

Figure 8 shows the flowchartsof workingprocedures for our proposed VPN with IPSecand VPN with cryptographic tunneling protocol respectively.

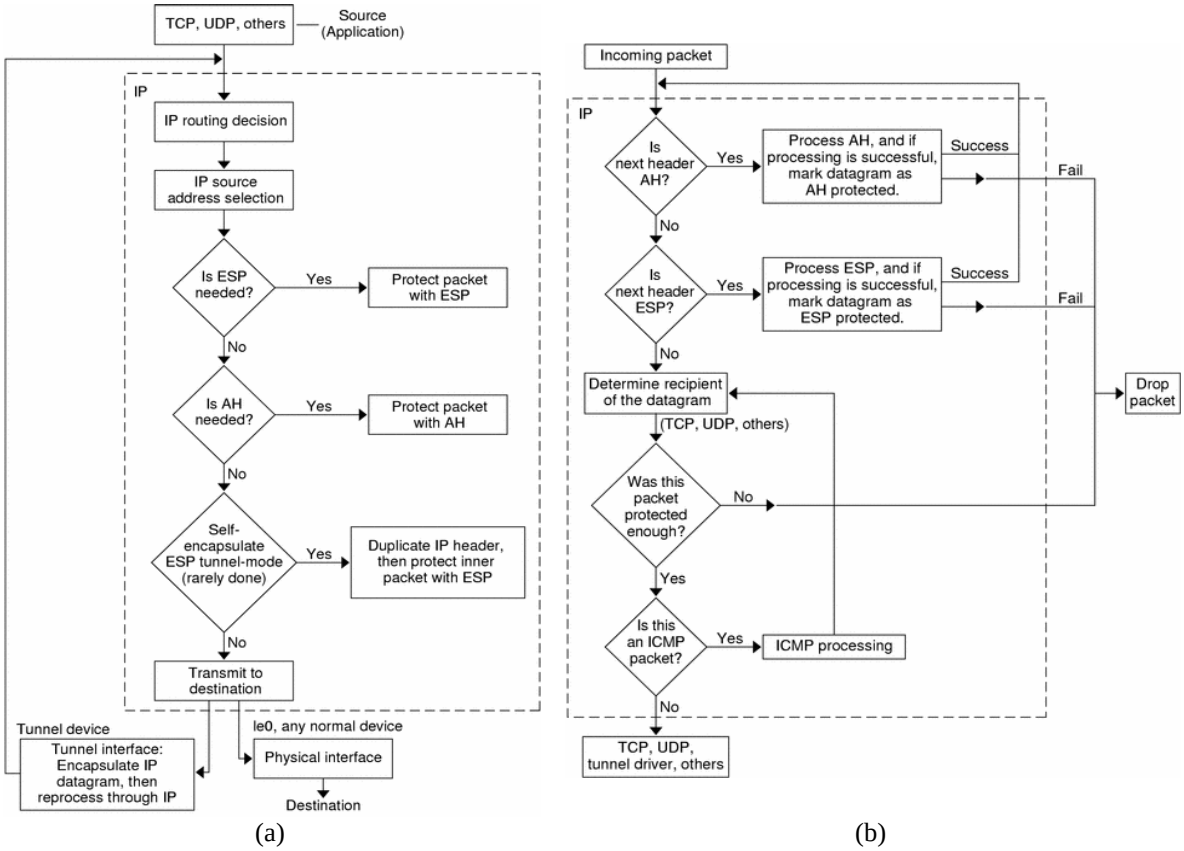

Figure 8. (a) Proposed VPN with IPSec, (b) proposed VPN with cryptographic tunneling protocol

4. RESULTS AND DISCUSSION

The research results of this work can be summarized as follows: Firstly, we introduced the mobile P2P network architecture system so any one who read this research will know what this system is. Secondly, we analyzed and proposed different solutions for this mobile P2P network threats and security issues. Thirdly, we gave a literature review about some related works in this field and what they produced. In the end as much we will speak about this network system, it will not be enough to cover the ideas on this system and its security.

Moreover there is a lot of researches that dealt with P2P security to offer a high file transaction performance with low latency, however P2P like any kind of computer network is under jeopardy as long there is a people who want always to sneak access to the system, and no matter what security design and mechanism are no match with skillful attacker, if he got enough time, he will find a way around these designs. So security must always be a step ahead from the hacker thinking, well this thought is easy to think and hard to implement.

Recently, some works were presented new ideas or implementation designs for different fields of the security of the mobile P2P network system as follows:

The work [10] introduced an efficient new concept of classifications of the attacks on peer to peer which they proposed that there is a relationship and most of the attack are actually are chain of multiple attacks, this concept analyzed the attacking to improve the methods of security in P2P system. Work [13]

proposed a several models to understand the propagation of the malware and its behavior (Mathematical file spreading model, Biological model, SIR model, SEIR Model and Empirical model) and subjected the last one to the experiments aiming build model which cross over the malware propagation in order to develop the trust among the peer and to create a reputation system that Predicts which peer is good and which is infected.

In [24], this work proposed a new design to reduce the potential of worms and virus propagation by a model called pricing model which it is built on a factor called Pearson coefficient as he stated in this work that if Nodes wish to link to other nodes that are charged higher prices for choosing links that it has low the Pearson coefficient, we can see this idea in many of p2p provider like NAPSTAR. In [25], this work presented a new model called level model based on a quantitive strategy called PLIM. This model is based on the mutual cooperation between the neighbors to determine the level of each peer in order to inhibiting the DDoS in each peer.

In [26], this work proposed a new P2P system based on an (artificial immune systems [27]) to defend the system against the flood DDoS, They propose that could be done by using AIS detectors as a probe to check incoming traffic for anomalies. The Artificial Immune Systems are computational systems inspired by the principles and processes of the vertebrate immune system. The algorithms in the AIS typically use the immune system's characteristics of learning and memory to solve a problem [27]. Work [28] dealt with Sybil attack which it is based on using Self-Registration with Judgment Evaluation (SRJE) that it is a decentralized authentication scheme to utilize a local trust mechanism for self-registration in order to heal the problem and they proved that the (SRJE) can inhabit the Sybil attack.

Some of the works that introduced in our research which deal with P2P network security had some weakness issues for example the proposed work at [10] did not mention or discuss the behavior of the malwares (like worms and botnet) that maybe by the responsible of all the attacks caused by malware but from my point this is not true according to fact the flood DDoS is not malware and also worms and Botnets in the end can cause DDoS. So we adapted this idea to produce my classification of Peer to Peer threats as shown in Figure 3, also the idea is charged to link with the other in [25] that it is lost the meaning of P2P system and give no difference with (client/server) model, as we reviewed many papers that come with this idea of using the SJRE [29] that combined with a probe mechanism like PLIM in the [27] which this will give each node a certain position and lower the probability of false registration and the ASI probe will discover any kind of malicious behavior in the system.

5. CONCLUSION

The main contributions of this work can be listed as follows: (1) We proposed two avoidance solutions (Internally and Externally) for web threats that facing mobile P2P networks, (2) our work comes with new solution for DDoS attackers against mobile P2P networks as well as motivations that make the worm most uneffective attacks. (3) Finally, we proposed two approaches of encryption at mobile P2P networks: First approach is a procedure for encryption mobile P2P network using proposed secure socket layer protocol (SSLP) and the second approach is a proposed VPN with IPSec and VPN with cryptographic tunneling protocol respectively.

REFERENCES

[1] Li, James, "A Survey of Peer-to-Peer Network Security Issues," 2007. [Online]. Available: https://www.cse.wustl.edu/~jain/cse571-07/ftp/p2p/index.html

[2] Shen X.S., Yu H., Buford J. and Akon. M., "Handbook of peer-to-peer networking," vol. 34, *Springer Science & Business Media*, 2010.

[3] Singh K., Guntuku S.C, Thakur A. and Hota C., "Big data analytics framework for peer-to-peer botnet detection using random forests," *Information Sciences*, vol. 278, pp. 488-97, Sep. 2014.

[4] Stutzbach D. and Rejaie R., "Understanding churn in peer-to-peer networks," In *Proceedings ACM. 6th ACM SIGCOMM conference on Internet measurement*, pp. 189-202, Oct. 2006.

[5] Capkun S., Hubaux J.P. and Buttyan L., "Mobility helps peer-to-peer security," *IEEE Transactions on Mobile Computing, IEEE Press*, vol. 5, no. 1, pp. 43-51, Nov. 2005.

[6] Peterson. L. L. and Davie. B.S, "Computer networks, a systems approach," *Elsevier*, Apr. 2007.

[7] Hamai T., Fujii M., and Watanabe Y., "ITU-T recommendations on peer-to-peer (P2P) network security," *Proc. IEEE Symp. International Symposium on Autonomous Decentralized Systems, IEEE Press*, pp. 1-6, Mar. 2009.

[8] Schollmeier R., "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," *Proc. IEEE Symp. First International Conference on Peer-to-Peer Computing, IEEE Press*, pp. 101-102, Aug. 2001.

[9] Wallach. D.S., "A survey of peer-to-peer security issues," In *International symposium on software security, Springer*, Berlin, Heidelberg, pp. 42-57, Nov. 2002.

[10] Zeidanloo H.R., and Manaf A.A., "Botnet command and control mechanisms," *Second International Conference on Computer and Electrical Engineering, IEEE Press*, vol. 1, pp. 564-568, Dec. 2009.
[11] Jhaveri V.J., Novik L. and inventors, "Security in peer to peer synchronization applications," Microsoft Corp, U.S.patent, 7930346, Apr. 2011.
[12] Singh, Rajendra G., "Sharing quality assured reusable learning objects on a peer-to-peer network with security controls," Ph.D. dissertation, The University of the West Indies, 2019.
[13] Schäfer J., and Malinka K., "Security in peer-to-peer networks: Empiric model of file diffusion in bit torrent," *Fourth International Conference on Internet Monitoring and Protection, IEEE Press*, pp. 39-44, May 2009.
[14] Wang L., "Attacks against peer-to-peer networks and countermeasures," *InT-110.5290 Seminar on Network Security*, Dec. 2006.
[15] Ali Aydın S., Ersin U., and Mark R.P., "A Reputation-based trust management system for P2P networks," *International Journal of Network Security*, vol. 6, no. 3, pp. 235-245, May 2008.
[16] Wilkinson S., Boshevski T., Brandoff J. and Buterin V., "Storj a peer-to-peer cloud storage network," vol. 1, pp. 1-18, 2014.
[17] Kadhim D.J., Yu X., Jabbar S.Q., Li Y., Luo W., "A New Scheme for QoE Management of Live Video Streaming in Cloud Environment," In: Paul M., Hitoshi C., Huang Q. (eds) *Image and Video Technology. PSIVT 2017. Lecture Notes in Computer Science*, vol. 10749. Springer, Cham, pp 150-161, 2018.
[18] Mohammed, Ali Abdul Wahhab, and Assad H. Thary Al-Ghrairi, "Differences between Ad Hoc Networks and Mobile Ad Hoc Networks: A Survey," *Journal of Southwest Jiaotong University*, vol. 54, no. 4, 2019.
[19] Qi. M, and Yang. Y, "P2P DDoS: challenges and countermeasures," In *2009 Sixth International Conference on Fuzzy Systems and Knowledge Discovery, IEEE Press*, vol. 7, pp. 265-268, Aug. 2009.
[20] B. Pourebrahimi et al., "A survey of peer-to-peer networks," In *Proceedings of the 16th Annual Workshop on Circuits, Systems and Signal Processing, ProRisc*, Citeseer, vol. 2005, 2005.
[21] Jabbar S.Q., Kadhim D.J., Li Y., "Proposed an Adaptive Bitrate Algorithm based on Measuring Bandwidth and Video Buffer Occupancy for Providing Smoothly Video Streaming. *(IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 2, pp. 1-10, 2018.
[22] Stallings W., "Network Security Essentials: applications and standards," *Pearson*, Aug. 2016.
[23] Khamees, Hussein Thary, and Ali Abdul Wahhab Mohammed, "Bit Error Rate Evaluation in Atmospheric Blustery for Slant Path Spread of Super Lorentz Gaussian Beam," *Journal of Southwest Jiaotong University*, vol. 55, no. 1, 2020.
[24] Rice, D.O., "A Proposal for the Security of Peer-to-Peer (P2P) Networks: a pricing model inspired by the theory of complex networks," In *2007 41st Annual Conference on Information Sciences and Systems, IEEE Press*, pp. 812-813, Mar. 2007.
[25] Yu S.C., and Li Y.C., "To Inhibit DDoS Attack for P2P Overlay Based on Level Model," In *2009 International Symposium on Computer Network and Multimedia Technology, IEEE Press*, Jan 18. 2009, pp. 1-4.
[26] Ali K., Aib I. and Boutaba R., "P2P-AIS: a P2P artificial immune systems architecture for detecting DDoS flooding attacks," In *2009 Global Information Infrastructure Symposium, IEEE Press*, pp. 1-4, Jun. 2009.
[27] Dasgupta D., Ji Z., and Gonzalez F., "Artificial immune system (AIS) research in the last five years," In *The 2003 Congress on Evolutionary Computation (CEC'03), IEEE Press*, vol. 1, pp. 123-130, Dec. 2003.
[28] Mashimo Y., Yasutomi M., and Shigeno H. "SRJE: Decentralized authentication scheme against Sybil attacks," *International Conference on Network-Based Information Systems, IEEE Press*, pp. 220-225, Aug. 2009.
[29] Lua E.K., Crowcroft J., Pias M., Sharma R. and Lim S., "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 1-4, pp. 72-93, Apr. 2005.