International Journal of Computer Networks and Communications Security

VOL. 5, NO. 6, JUNE 2017, 126–129
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Improving Security and Performance in the TOR Network

Diyar Salah Fadhil[1], Ababakr Ibrahim Rasul[2] and Younus Ameen Muhammed[3]

[1, 2, 3] Department of Computer Science, Faculty of Science, Soran University, Kurdistan Region, Iraq

[1]*diyar.fadhil@soran.edu.iq*, [2]*ababakr.rasul@soran.edu.iq*, [3]*younus.muhammed@soran.edu.iq*

ABSTRACT

TOR software covers the browsers securely. This option makes the journalists, militants and some authorities to be unknown over internet. TOR (onion router) is very successful in low latency anonymous communication. TOR gives more benefits like untraceable network to both local adversary controlling a small network and companies that are low enough to support anonymous use and also remote login. There is other software like AN.ON, crowds and anonymiser.com also provide anonymous communication over networks but TOR software had proved its efficiency in the networking market especially in field of network security ,The IP addresses will be hidden in the server.

Keywords: *TOR network, authentication, IP hidden in the server*.

1 INTRODUCTION

The idea of anonymous communication was first acquainted by Chaum in the year 1981. In his proposal, who first sent all the messages to a server called "mixed server" in which all the messages are mixed together irrespective of their source and then forwarded to their respective destinations. In the above method the communication was anonymous. The main advantage of anonymous is security enhancement within networks. At present anonymous communication is divided into two types: 1) low latency and 2) high latency. In these two types low latency communication is more successful. TOR (onion router) is very successful in low latency anonymous communication. TOR gives more benefits like untraceable network to both local adversary controlling a small network and companies that are low enough to support anonymous use and also remote login. [1].

Anonymous communication means the server or the destination doesn't know who the client or the source is from. IP addresses of the initiator of the communication will be unknown to the end user but communication will be successful. For secured communication in a network anonymity will play the vital part. For example, in big companies privacy is provided by letting the users interact without disclosing their respective partners [2].

In the current networking field securing a network is considered as the most difficult task. However technologies such as onion routing, CBAC and AAA authentication help to secure the IP addresses, switches and routers from hackers. Because of all these features only online banking is successful at present.

TOR is the software used in recent times for anonymous communications. There is other software like AN.ON, crowds and anonymiser.com also provide anonymous communication over networks but TOR software had proved its efficiency in the networking market especially in field of network security.

LITERATURE REVIEW:

TOR software covers the browsers securely. This option makes the journalists, militants and some authorities to be unknown over internet [3]. Hackers can puzzle out where do you live, what u like and what all your interest by tracing your IP address and browsing history. Even service providers can trace all these information. So in order for secured browsing you have to get accessed with TOR software. TOR software provides a free and secured browsing over internet. TOR project put a mask over the IP address and does not reveal the source IP address which will be hidden. When a web page is loaded, it first enters the network via TOR network which is the entry point to the browser and is also known as relays. These relays encrypts the data send which runs a copy of TOR software with it and these relays sends the packets in a random manner to confuse the hackers watching one's internet activity. The packets send from source passes through different nodes and finally open the required web page requested. Backtracking is much more difficult

because the web page once open again it will jump back to the TOR network before reaching the host. The basic disadvantage of TOR is that whenever a web page has to be opened one have to jump to the TOR network which consists of multiple nodes over the network and shares less than 1000 nodes of all the TOR users. One can bring down the traffic by using own TOR relay.

In internet anonymous communication has been successful in present days. Initially technologies like onion routing and free network used to provide anonymous but due to discovery of TOR project which is also called as second generation of onion routing previous technologies (onion routing and free network) have put to end. People who have geographic restrictions, higher authorities who want to hide their data to local authorities and reporters widely use TOR project. User's system is attacked by some practical attacks due to the familiarity of TOR project. For this problem there are lots of mechanisms introduced to solve it. One of the mechanisms is called user tunable mechanism. This mechanism is used for selecting the best router based on their bandwidth capabilities. TOR network has its own bandwidth values for the selection of bandwidth [4]. This bandwidth values are used for building tunnels in the network. Since TOR project uses its own bandwidth it assumes the maximum value of bandwidth for higher anonymity for all the users of TOR. The mechanism which is introduced easily goes with the traffic from users to different destinations. Practical attacks are hard tasks to perform in this method. Tunable performance is implemented in both simulation and experiments method to catch their performance basically. This method ultimately reduces the attacks. Also this method enhances the anonymity protection without sacrificing much loss in performance.

Fig.1 the time required to send 1MB data over TOR network in more number of trails [4]. The user tunable mechanism proved to be much secured without much anonymity protection.

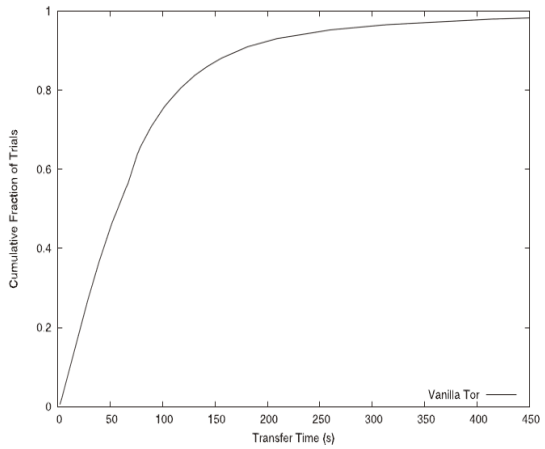

Fig. 2 . Cumulative distribution function of the time required to transfer a 1 MB file over the Tor network in July 2009 (18,422 trials).

It was relayed anonymity routers favor the users to browse anonymously. TOR helps to hide the user's identity [5]. Even though users had secured browsing using TOR network correlation attacks were more mainly on the routers. These attacks can endanger the whole network. So the author provides a new solution to get rid of these attacks. Anew model called STOR was proposed which is known as social network based anonymity. With this model it helps to prevent the routers from vulnerable attacks to obtain secured anonymity. Integrating both qualitative and quantitative attributes of social network leads to STOR. Both simulation and lab experiments are done to prove the security in anonymous networks. This model is proposed mainly for social networking sites like Facebook, twitter, etc. but can be indulged in other networks also.

Privacy on online communications had a good start with data encryption [6]. Although encryption doesn't give the original data it shows the communication or transaction, only because of the introduction of anonymous communication over internet the network is more secured. Onion router provides only the privacy through network whereas TOR software has a special option called hidden services which makes this software more reliable. This hidden service provides the users not to be visible, not available to the internet public. The main advantage of TOR is that gives full protection to the VPN connections which also gives many more uses like it gives the exact information to the destination even when the data is sensitive. TOR software depends on nodes and bandwidth. The author calls the TOR software as double-edged sword and rock solid anonymity. Without introducing the identity of the source TOR is used to observe sensitive topics such as trademark and patterns. TOR hides the accomplish details, purchasing details and other banking activities which offers a much secured browsing.

Based on [7] view, in today's web world privacy and anonymity plays a vital part. The main aim of anonymity is privacy protection for users. In anonymity TOR is the only project which gives full secured anonymous browsing. TOR is more reliable on traffic based P2P applications. On considering bit torrent traffic TOR project has been underestimated. Their usage is vast in both HTTP and bit torrent protocols. As said earlier it is an extension of onion routing. TOR exit nodes use a tunneling technique.

2 RESEARCH METHODOLOGIES TOOLS AND TECHNIQUES

This section tells the tools (software and hardware) and techniques which are used in this project. So for each objective the research methodology varies and will be explained separately for each objective. The method most important for the objective is taken as a primary research method whereas the other methods are kept as an alternate option if in case the first method fails to give the results. Dependency is more on the primary data for this project because the decision is taken to follow the method sensitively; maximum the project will be successful with all the primary data for the entire objectives.

OBJECTIVE 1: Identify the technologies in TOR network.This objective can be related to the literature review. More options are given in the above stated literature review. Technologies used in TOR network at present and previous versions of this network are explained. This objective is more or less theoretical based. More of research on different kinds of papers that are related to TOR network is enough to achieve this aim.

OBJECTIVE 2: Investigate how the TOR network operates.This objective needs more research on technologies involved in TOR network and how these technologies enhance the TOR operation. The operation explained for this objective is commonly expressed in all the websites. TOR software is already in use and its working will be explained clearly.

OBJECTIVE 3: Run a TOR network (Setup your own TOR network in the lab).This objective indulges to run a TOR network in a lab environment. By gathering information from objective 1 and objective 2, put all the knowledge and have to run a TOR network.In this objective experiments and tools are taken as the primary research method.

OBJECTIVE 4: Experiments on the TOR network.This is considered as the most important objective of all the objectives in this project. The above three objectives are combined together to excel this objective. This objective will give the live results of the idea of the project.

Critical Evaluation:

This section describes how the project excels in this current world, its limitation and the possible outcomes.

Possible Outcomes:

- A clear idea on TOR network.
- The IP addresses will be hidden in the server.
- A TOR network will be run successfully.
- A white paper based on the supervisor wish can be produced.

Possible outcomes are similar to expected outcomes till now according to my knowledge. When hitting practically only the outcomes may change.

Expected Outcomes:

- A clear idea on TOR network.
- The IP addresses will be hidden in the server.
- A TOR network will be run successfully.
- A white paper based on the supervisor wish can be produced.

3 CONCLUSION

A proper literature review is given. A clear and straight forward research method is described with good referencing. Possible outcomes and expected outcomes are explained clearly. The project is dealt with lots of scope. Even though the idea is not new experimental set up is new and opportunity to learn more in a specific task is more. As said early all the experiments will be properly reviewed and the results obtained will be watched correctly. This project may not be industry based but after the completion of this project successfully many companies will be invited to implement this project to a larger extent.

4 REFERENCES

[1] V. E. a. C.-T. Hooper, "How much Anonymity does Network Latency Leak?," 2010.
[2] R. a. M. N. Dingledine, "Effect, Anonymity Loves Company: Usability and the Network," 2005.
[3] A. Wawro, "Tor Network Cloaks Your Browsing," 2011.
[4] R. a. B. N. Snader, "Improving security and performance in the tor network through tunable path selection," 2011.
[5] P. a. L. X. a. C. A. a. C. R. Zhou, "STor: Social Network based Anonymous Communication in Tor," 2011.
[6] P. Payne, "Tor Protects Anonymous Sources," 2007.
[7] A. a. C. P. a. K. M. Manils, "Digging into anonymous traffic: A Deep analysis of the Tor Anonymizing Network," 2010.
[8] F. Dr. Slack, "Developing your research idea," 2012.