Transmission control protocol is a single path per connection in spite of that unite paths often exist between end points. When the data has been transmitted through the connection with multipath TCP and it is lost then the data is transmitted with normal TCP which is more vulnerable to the attacks. The survey made in this paper proved that most of the security attacks like IP source route, Routing Information Protocol etc can be overcome when we send the data through the option enabled with multipath TCP as the data flows in multiple paths simultaneously thus increasing the utilization of the resources by the applications that are based on the internet. It is been observed that through the study made in this paper that the throughput of the application can be improved when the connection is established through Multipath TCP compared to normal TCP.

KEY WORDS: TCP attacks, Multiple Subways, Moving Nodes.

1. INTRODUCTION

In today's communication, everything became Multipath: Servers are multihomed, mobiles are having cellular and WiFi access, but traditional TCP is still a single path. MPTCP is a major extension to TCP. Multipath-TCP (MPTCP) is an as of now exploratory TCP expansion that is intended to add extra usefulness to TCP whirled remaining to provide backward compatibility with most existing systems and gadgets which continue to use TCP (Pamela & Godwin Premi, 2015) MPTCP changes TCP's conduct from how it is regularly comprehended in ways that go past the security of MPTCP itself. MPTCP allows the concurrent use of multiple paths between two end points and thus helps to improve performance. It enables distributed data transfer between two end points on multiple TCP sub flows. There are no MPTCP packets; there are only multiple TCP packets. Mostly MPTCP are used for better resource utilization, best throughput and smoother reaction to failures. TCP/IP which is widely used today has a number of serious security flaws inherent to protocol. TCP/IP functions mainly on a end to end connection between two systems, this is also a drawback as it cannot support instances where connection is to be maintained where device needs to change their network addresses without dropping the connection. MPTCP is designed/ developed to counter these shortcomings of TCP (Bagnulo, 2011) while maintaining secure transmission of data. The design objectives of MPTCP are to Improve Throughput; Do no Harm, Balance Congestion. This paper focuses on the analysis of security issues in various perspectives in Multipath TCP. First view says the various attacks that take place in TCP.

Attacks in TCP:

**Denial of Service:** Denial of Service is the attack takes the resources and services of the nodes in the server and prevents to provide services to lawful users by consuming their resource. SYN Flooding (Luo & Yang, 2014) is one of the popular attacks that happen in DOS. This attack takes place when attacker sends many TCP requests with spoofed source addresses. The destination node will be waiting for the source to send the message after sending the acknowledgement. In the time being all the resources of the destination node will be washed-out so that no further requests cannot be considered and thus denying the legitimate accesses.

**IP Source Route:** IP Source route is transmission of the IP packet by the sender through a specific route in the network. Assume the target node uses the reverse of the source route in a TCP open request for return traffic. The source of the connection likes to specify a particular path for some reason – may be the regular route is dead - replies may not reach the originator if a different path is followed. Then the attacker may pick an IP source address including that of a trusted machine on the target's system so that the information will be seen by the attacker.

**Routing Information Protocol Attack:** The Routing Information Protocol (RIP) contains the routing information in networks, especially broadcast media. The intruder may send fake routing information to a destination host, and to each of the gateways on the way representing as a particular host. This attack claims that route to a particular unused host, rather than to a network; this makes the packets transferred to the intruder's machine rather going to destination node (Zhu Dawei, 2014). This made the protocols which relayed on address-based authentication is compromised. By this attack attacker benefit's a lot. The attacker claims a route to be an active host. The packets will be routed for that host will be gone through the intruder's machine so that the attacker can inspect the packet and may alter the packet. Then they are sent to the actual destination using IP source address routing, by this attack an attacker can capture confidential data. This attack may use to track the calls as well, thus, when a user calling from the targeted host may disclose sensitive information over the calls. This attack can be encountered in TCP as in built congestion control algorithms are used to prevent syn flooding of nodes or routers. But in MPTCP these attacks (Kostopoulos, 2010) can be prevented as the data packets are fragmented and send them through sub flow which makes difficult for the attacker to send the false information.
Attacks in MPTCP:

**Denial of Service:** MPTCP designed for greater availability of the bandwidth in each connection. The attacker establishes the connection to the source using multiple sub flows and starts downloading the traffic. The source thinks that all the other sub flows are congested, which is not and start sending the data by the sub flow requested by the attacker. This may be avoided if the reach ability test i.e. 3 way hand shake for each new address pair in MPTCP which prevents flooding attacks.

**Fragmented Traffic:** The main objective behind the fragmented traffic in MPTCP is to ensure that the traffic is distributed over the sub flows (Han, 2006). The advantage of doing so will reduce the congestion over the sub flows as the load is distributed among the sub flows. Sometimes there come situations where a network monitoring device sees only some of the traffic in MPTCP. This is same as the multi-homed network, but the difference is that MPTCP allows single communications channels to be fragmented across the different sub flows path. In TCP the port fragmentation happens. When the traffic is broken the, different TCP connections with different endpoint and port combinations and TCP address fragmentation when it is sent from nodes with different network addresses over separate networks. Therefore the behavior of network monitoring devices with partial content is unknown in MPTCP.

**Connection Reestablishment:** Communication redundancy takes place in MPTCP i.e. when a problem is identified with a path i.e. the sub flow path may be terminated then that path is deflected without descending the overall MPTCP connection. The Network Intrusion Prevention Systems reestablish the network connection by resetting malicious and unauthorized TCP path. However, the present network intrusion prevention devices are designed in such a way that they cannot work with MPTCP. So the Internet Service Provider should be able to end the MPTCP connection in such cases. The termination of MPTCP connection is done by stopping every possible sub flow at the same time. In some cases where a valid MPTCP sub flow survived then the communication is reestablished and additional sub flows are added, beginning the process again. In present day scenario where multipath TCP is not widely employed, security impacts of multipath TCP can be broadly classified into transitional state impacts and future impacts where MPTCP is commonly used.

**Transition State Issues in MPTCP:** In the present day world where multipath TCP is widely used, the following are some of the security issues concerning the multipath TCP.

**Moving Nodes:** The nodes in MPTCP may modify their network addresses and port numbers when they are communicating with other nodes. The network security monitoring device, it should not only monitors the traffic from multiple sub flows, it should also be capable of tracing traffic across different networks as the sub flows are added and removed and network addresses during establishment of connection.

**Termination of the Connections:** The MPTCP's can route when there is a network crash which leads to the instances where MPTCP network connections becomes difficult for the termination by network operators and security devices when compared to the present's TCP connection. If all the sub flows are not killed properly their might be a chance that the MPTCP connection may still open. Moreover, the backup sub flows are obsessed by network monitoring devices as the backup sub flows will not contain much heavy traffic, and if these backup sub flows are not terminated then the connection as MPTCP will continue.

**Impact of MPTCP in Future Networks:** The following are some of the security issues that MPTCP users might face in the future where most of the systems are MPTCP.

**Traffic Splitting:** MPTCP sends the traffic to be fragmented and distributed over the network by various sub flows. Network security tools (Honda, 2011) are necessary to end the session; if not the partial data can be read through partial content visibility. We need tools that work on distributed content so that network security nodes cannot determine content by observing the traffic locally. MPTCP's monitoring systems saves the information like former coordination between devices on different organization.

**Moving Hosts:** The hosts may change the address of the network when they are roaming. This may not be the issue in MPTCP, but it is in the middle of the communication. This means the address of the host who started communication may not reach the end with same address. This clearly shows that all the possible path must be closely monitored which is expensive and resource utilization will be more.

2. CONCLUSION

Though, MPTCP mitigates many shortcomings of TCP and itself in isolation is a secure way for distributed transfer of data. But in real world when the system connects with the network, the MPTCP becomes vulnerable to some security issues. We must make sure that these issues are resolved in order to ensure secure transmission of data and wider acceptance of MPTCP. This paper discussed and analyzed the possible attacks in MPTCP in current and future networks.
REFERENCES
Pamela D, Godwin Premi M,S, TCP/IP Based Control and Automation of Temperature Process, Indian Journal of Science and Technology, 8 (11), 2015.