SECURITY ENHANCEMENT OF MULTIPLE PATH TRANSMISSION CONTROL PROTOCOL WITH TRANSPORT LAYER SECURITY

[1]Ameer Hamza*, [2]Farooq Javid*, [3]M. Ikramullah Lali*, [4]Faraz Ahsan**

*Department of Computer Science & IT, University of Sargodha, Sargodha, Punjab, Pakistan.

**Department of Computer Science, HITEC University, Taxila, Punjab, Pakistan

[1]mameeerhamza@gmail.com, [2]farooqjavid@yahoo.com, [3]drikramullah@uos.edu.pk, [4]faraz.ahsan@gmail.com

ABSTRACT*— Mobile devices are multi-homed nowadays which provide multiple interfaces like Wi-Fi, 3G, and 4G/LTE. User demands maximum utilization of these resources to work quickly and securely. Transmission Control Protocol (TCP) is a widely used connection-oriented transport layer protocol but unable to establish a connection with multiple interfaces at the same time. Multiple Path Transmission Control Protocol (MPTCP) is the extension of TCP which establishes a connection with multiple interfaces between peers. It provides an optimal solution for current Internet scenario without changing the regular TCP. However, MPTCP becomes vulnerable due to one or more TCP connections. Consequently, MPTCP faces network security implications. Therefore, these security implications affect the expectations of other entities in the environment when the protocol extension is required. This article is focused on the security of MPTCP using Transport Layer Security (TLS). We investigate the applicability of TLS on MPTCP, to provide secure, faster and reliable communication. Our study shows how to adopt TLS for MPTCP as a better security solution.*

Keywords— Secured Multipath TCP, MPTCP Secure with TLS, MPTCP security solution

I. INTRODUCTION

TCP is widely used protocol for end host communication. TCP establishes a logical connection using combination of IP addresses and port numbers. This connection initially assigns an IP address to a packet and the related port number so that a packet can travel on a particular path. This kind of TCP defined as single-path [19]. However, there comes a gap that a single-path TCP cannot send packets on different multiple interfaces [23]. The efficient solution to fill this gap is to use multiple-path TCP (MPTCP). MPTCP is an extension of TCP in order to send packets over multiple available paths [4]. At the architecture point of view, MPTCP is also called a shim layer in between socket of TCP and multiple TCP flows [8].

When client-server communication support MPTCP and multiple interfaces are available, then peer can set up a MPTCP connection and transmit connection's data across multiple interfaces [7]. The key goal of multipath TCP is to provide uninterruptable reliable communication, maximize the throughput in multi-homed devices and also backward compatible with regular TCP [5].

The primary security consideration for Multipath TCP is to be more secure than regular TCP or at least the same security as regular TCP [18]. Multipath TCP uses multiple interfaces for single connection, which raise security hazard [23]. An attacker has the capability to add his own interface in victim connection. For defeating the security hazards of Multipath TCP, authentication should be needed [20]. Authenticate the numerous multiple paths of MPTCP connection during the initialization of a connection, the data that should be received by actual path of a connection and the request for adding or removing paths should not be old [17]. Default security provided by MPTCP is not able to counter different attack [22]. Here we specify the security threats and vulnerabilities of MPTCP.

A. Security Threats and Vulnerabilities on MPTCP

A Multipath TCP (MPTCP) connection comprises one or more TCP connections due to which MPTCP becomes vulnerable, at least the same set of risks that TCP is already exposed, e.g. SYN flooding attack, spoofing attack, and routing attack [15]. Consequently, MPTCP would face network security implications with respect to attackers and types of attacks respectively, e.g. attackers (partial time on-path active Eavesdropper and off-path active attacker) and types of attack (Eavesdropper in the initial handshake, ADD_ADDR attack, DoS attack on MP_JOIN, SYN flooding amplification). Significantly, these security implications would effect the expectations of other entities in the environment when the protocol extension is required. However, network infrastructures do not expect MPTCP to behave in similar ways to the traditional TCP's. This section summarizes security threats and vulnerabilities on MPTCP.

1) Security Implication with respect to attackers:

Generally, a network attacker is a software agent who interrupts communication or makes efforts to block or re-direct communication services from designated destination to the attacker's preferred destination.

In network communication, there are three major types of network attackers, i.e. location-based, action-based, and hybrid. Location-based attackers are subdivided into three categories: off-path attackers, partial-time on-path attackers, on-path attackers. Action-based attackers are categorized into Eavesdropper and Active attackers. Hybrid attacker means combination of action-based and location-based attackers. This attackers can be identified as follows: an on-path eavesdropper, an on-path active attacker, an off-path active attacker, a partial-time on-path eavesdropper, and a partial-time on-path active attacker [25].

Regarding location-based attackers, off-path attacker is described as an attacker that could not requires to be in between any subflows of MPTCP connection in entire MPTCP session. Partial-time on-path attacker is described as an attacker that could requires to be in between at least one of the subflows of MPTCP connection in any time of entire MPTCP session. On-path attacker means that requires to be in between at least one of the subflows of MPTCP connection in entire MPTCP session [16].

Regarding action-based attackers, Eavesdropper refers to the attackers that capture few packets of the MPTCP communication but are not able to alter, suspend, or postpone any segments of the MPTCP connection. And, Active attacker means that can alter, suspend, or postpone any segments of the MPTCP connection.

2) Security Implication with respect to type of attacks:

Generally, a network attack can be understood in terms of an activity that is performed either to interrupt network communication or block or re-direct communication services. Network researchers have identified network attacks targeting transport layer that is mainly responsible for control communication like TCP, MPTCP, etc. Currently, we are only emphasizing network attacks related to MPTCP [26].

For instance, [25] has discussed five different types of attacks and attacks' mechanism (how attack happens step by step). In further, type of attacker involved in a particular attack are identified. Those five types of attacks are as follows: ADD_ADDR, DoS attack on MP JOIN, SYN Flooding Amplification, Eavesdropper in the initial Handshake, and SYN/JOIN.

According to [11], first of all, ADD_ADDR happens due to off-path active attacker when the attacker makes an effort to hijack MPTCP session using man-in-the-middle strategy for attacking. Second, off-path active attacker also participates in DoS attack on MP JOIN so that the host would not be able to establish new subflows. Third, again off-path active attacker also amplify flooding attack through SYN plus MP JOIN requests to exhaust the server resources for avoiding to add a new subflows. Fourth, partial time on path eavesdropper [12] presented in, one of the path of MPTCP connection during the establishment of MPTCP session (where keys are negotiated between hosts) to hijack the MPTCP connection in the future. Fifth, partial time on path eavesdropper also present in one of the path of MPTCP connection, modify the SYN/JOIN request for change the source address [26].

For defeating the security risk of Multipath TCP, Transport Layer security mechanisms will be used [17]. Transport Layer Security (TLS) protocol is responsible to provide confidentiality, data integrity, authenticity, and privacy for secure communication between two applications [2]. The TLS Handshake protocol and TLS Record protocol are the two sub protocol of TLS. TLS Handshake protocol provides server and client authentication using cryptographic keys and encryption algorithm before application protocol send and receive data [1].

A MPTCP connection comprises one or more TCP connections, due to which MPTCP is going to be vulnerable [6]. Consequently, MPTCP would also face network security implications. Significantly, these security implications would affect the expectations of other entities in the environment, when the protocol extension is required [21].

Our work is focus on real time implementation of MPTCP along TLS security. We evaluate MPTCP connectivity with secure data transmission and present the comparative analysis of MPTCP with TLS and TCP with TLS.

Rest of the article is organized as follows: **section 2** presents the related work. In **section 3**, experimental setup is conferred. Afterward, Analysis and Evaluation are described in **section 4** and Finally, Conclusion and Future Directions are given in **section 5**.

II. RELATED WORK

In [7], Multipath TCP mechanism was described and shown that how to achieve the deployable goals. They had described the experience of implementing MPTCP in Linux kernel and evaluated its performance.

When client and server support MPTCP and multiple subflows are also available, client can set up a MPTCP connection and transmit connection's data across multiple subflows. The key goals of multipath TCP is to provide uninterruptable reliable communication, maximize the throughput in multi-homed devices and also backward compatible with regular TCP [5].

In [3], Williams proposed the support for Multipath TCP (MPTCP) in FreeBSD-10 kernel. A kernel patch is developed against FreeBSD-10 for MPTCP implementation. Few modifications are required in FreeBSD-10 and implemented MPTCP kernel. For enabling the support of MPTCP, TCP Control Block (TCPCB) modified as Multipath TCP Control Block to control subflows of Multipath TCP and some other changes are specified to perform MPTCP operations. His further research will be in congestion control of MPTCP [3].

Default security provided by MPTCP is not able to counter different attack. Here we give the security measurements to prevent those attacks and vulnerabilities on MPTCP [10].

A. Security measurements to prevent attacks on MPTCP.

The security measurements in order to avoid and prevent network attacks are presented in [26]. Currently, we are only emphasizing network attacks related to MPTCP.

For instance, [25] has discussed security measurements to prevent those given five different types of attacks. In further, type of attacker involved in a particular attack are identified.

According to [11], first of all, ADD_ADDR can be prevented using the following strategies.

- Connection's token is added in the ADD_ADDR option. It would prevent the attacker to launch the attack. There is a possibility that any eavesdropper that have the ability to see the token, would near to achieve his goal by launching the attack.
- HMAC of the connection address, which is included in the ADD_ADDR option, can be accessed by using a key which is the combination of sender and receiver keys (as it is used for generating the HMAC for the MP_JOIN message).
- SYN packet's destination address can be included in the HMAC of the MP_JOIN message. Now, an attacker requires this destination address for launching an attack. Protection of this destination address, reduces the chances of an attack.

Second, off-path active attacker can be prevented using strategies like to include random number with 32-bit token in third packet of SYN plus MP JOIN during the three way handshake process. Random number is also generated by destination host using hash code, initial sequence number and local secret key. This process enables the destination host not to create state when replying to a SYN plus MP_JOIN packet. Destination host only creates state on the arrival of 3rd ACK after verifying the accurate HMAC [26].

Third, again off-path active attacker can be prevented using strategies like MP JOIN DoS attack. Another technique can be used, to prevent the impact of attack with reducing the upper limit of half opened sub-flows to 3 sub-flows [11].

Fourth, partial time on path eavesdropper [12] can be prevented using the following strategies.

- Primary set of threats in the result of remaining group of vulnerabilities can be considerably reduced by using hash chains technique [25].
- For MPTCP security, SSL/TLS keys are reused by negotiating with Application layer protocol [27].
- CGAs (Cryptographically Generated Addresses) are also used for MPTCP security which are used previously to secure Shim6 [28].
- Tcpcrypt is also another technique for MPTCP Eavesdropping attack [13].
- For the security of Mobile IP protocol, DNSSEC technique can be used.

Fifth, partial time on path eavesdropper can be prevented using strategies like secure the segment exchanged that reduce the impact of that attack.

The security goal of MPTCP is that it should be more secure than regular TCP or provide at least the same security as compare to regular TCP [9]. Currently MPTCP uses cryptographic technique in TCP option space for security. This security is not enough for secure and reliable communication. If the researchers enhance the security of MPTCP with using TCP option space then it can be a big challenge because TCP option contains limited space. Other researchers are also suggest to use tcpcrypt or TLS for securing MPTCP. MPTCP security can be opted by tcpcrypt or TLS.

Transport Layer Security (TLS) is mostly used protocol to secure Internet communications, providing confidentiality, data integrity, authenticity and privacy for two applications.The TLS Handshake protocol and TLS Record protocol are the two sub protocol of TLS. TLS Handshake protocol provides server and client authentication using cryptographic keys and encryption algorithm before application protocol send and receive data [1]. It's most likely known as the protocol that, combined with HTTP, secures the communication on web and usages the HTTPS universal resource identifier mechanism. TLS depends on a reliable transport protocol like TCP [14].

For securing MPTCP, designing the new protocols is hard enough to be backward compatible with TCP. We should utilize TLS (or SSL) for MPTCP as TLS is already adopted by many protocols of application-layer. We focus on real time implementation of MPTCP along TLS security. TLS is already adopted by TCP, therefore TLS can be adoptable with current MPTCP. This will provide more security than default MPTCP security.

III. EXPERIMENTAL SETUP

We present and evaluate the implementation of TLS with MPTCP. We implement Linux kernel v0.90 [24] of MPTCP for Ubuntu LTS 14.04 on a client machines. Afterward, we apply the services of TLS security. Client machines are connected with MPTCP enabled web server. The web server is also enabled with TLS security. We use network analyzer tools for capturing the results.

We have taken six scenarios by using two interfaces (3G Mobile and WiFi). Two of them are MPTCP with TLS enabled on both interfaces. MPTCP enabled scenarios use default TLS security and TLSv1.2. While the other four scenarios are TCP with TLS enabled by using default TLS and TLSv1.2 on each interfaces separately.

We establish a MPTCP connection with using TLS security services between the client machines and a web server. During this process we capture the packets through network analyzer tools to evaluate the implementation of MPTCP with TLS. These tools also facilitates to filter the traffic related to work. We check the behavior of this communication when adopting TLS with MPTCP and also with regular TCP.

IV. ANALYSIS & EVALUATION

In this section, first we show the MPTCP connectivity with secure data transmission. Second, we present the comparative Analysis of MPTCP with TLS and TCP with TLS. At the end, we present the final discussions on the basis of implementation and comparative Analysis.

A. MPTCP connectivity with secure data transmission

In this section, we show the MPTCP connectivity with secure data transmission.

1) MPTCP initial handshake with 3G Primary Interface*:*

MPTCP initial handshake is done with default interface on the client machine. This handshake is similar to TCP 3-way handshake but contains the Multipath capable in the option space of TCP. In our Scenarios, there are two interfaces. The default one is Mobile 3G interface connected with USB tethering enabled mobile device and the second is WiFi interface connected with PTCL broadband DSL connection. The initial handshake is done by Mobile 3G interface that is the default interface of the client machine. This interface has an IP address '192.168.42.16'. As shown in the Fig. 1 client machine also send the TCP SYN request for establishing a TCP connection with Multipath capable option containing Multipath TCP Sender's key for authentication.

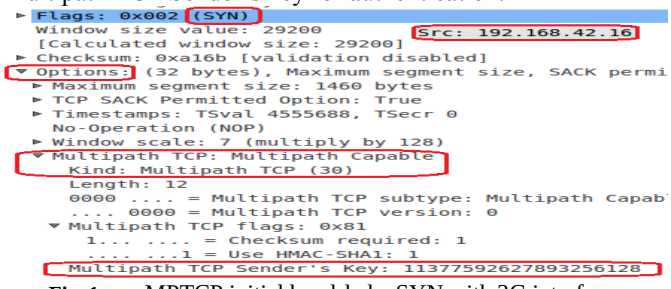

Fig. 1. MPTCP initial handshake SYN with 3G interface

2) MPTCP initial handshake SYN+ACK with 3G interface:

The MPTCP-enabled web server listens to the corresponding request and responds with SYN+ACK. As shown in the Fig. 2 client machine receives corresponding MPTCP capable option containing web server Multipath TCP key for authentication.

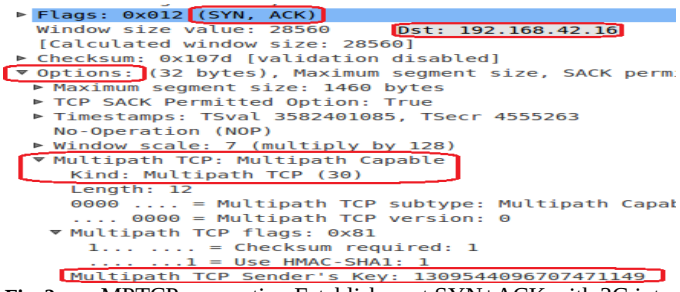

Fig. 2. MPTCP connection Establishment SYN+ACK with 3G int

3) MPTCP initial handshake ACK with 3G interface:

Afterward, the default interface of the client machine responds the web server request. As shown in the Fig. 3 client machine send the ACK request to the web server with the corresponding MPTCP capable option containing Multipath TCP client's key and Multipath TCP web server key for authentication.

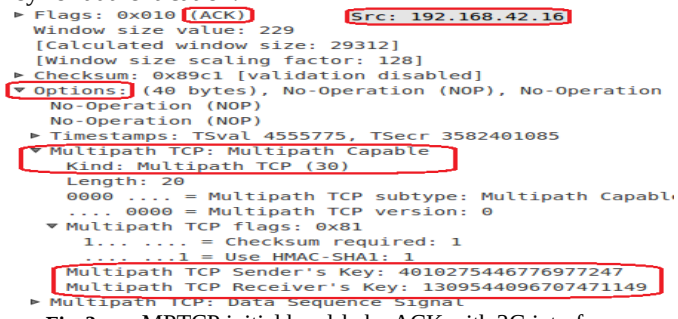

Fig. 3. MPTCP initial handshake ACK with 3G interface

Once the connection establishment is completed, data transmission will begin. If the client machine wants to add more interfaces in our Multipath TCP connection then client machine send the MPTCP Join connection request that work's same as the MPTCP connection establishment 3-way handshake work.

4) MPTCP join connection handshake SYN with WiFi interface:

In MPTCP join connection handshake, other available interfaces on the client machine can join with the established MPTCP connection. This MPTCP join connection handshake behaves similar to MPTCP 3-way handshake. The MPTCP join handshake is done by WiFi interface that is the other available interface on the client machine. This interface has an IP address '192.168.11.3'. As shown in the Fig. 4 client machine send the TCP SYN request for joining the interface with MPTCP established connection, option containing MPTCP address ID, MPTCP Server's Token, and MPTCP Sender's Random Number for authentication.

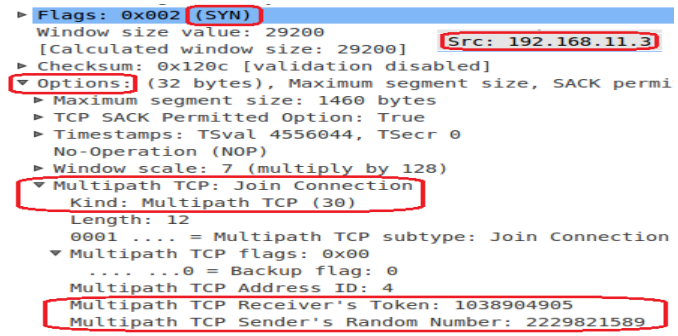

Fig. 4. MPTCP join connection handshake SYN with WiFi interface

5) MPTCP join connection handshake SYN+ACK with WiFi interface:

The MPTCP-enabled web server listens to the corresponding request and responds with SYN+ACK. As shown in the Fig. 5 client machine receive corresponding MPTCP capable option containing MPTCP address ID, MPTCP server's Truncated MAC, and MPTCP server's Random number for authentication.

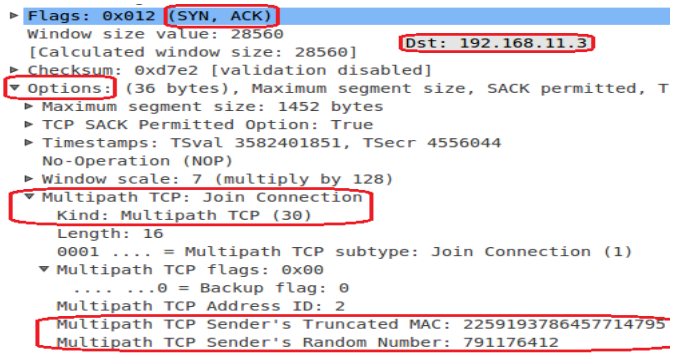

Fig. 5. MPTCP join connection SYN+ACK with WiFi interface

6) MPTCP join connection handshake ACK with WiFi interface:

Afterward, the WiFi interface of the client machine responds the web server request. As shown in the Fig. 6 client machine send the ACK request to the web server with the corresponding MPTCP capable option containing Multipath TCP client's MAC for authentication.

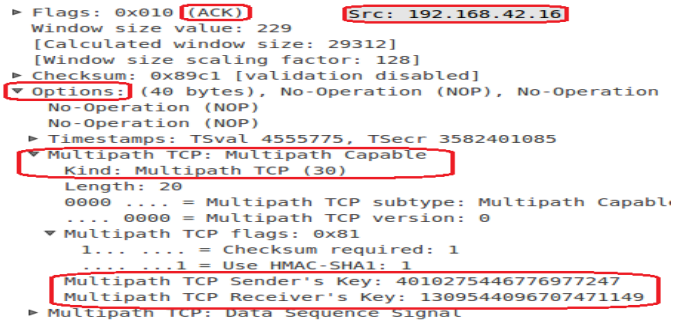

Fig. 6. MPTCP join connection handshake ACK with WiFi interface

7) MPTCP encrypted handshake and data transmission:

As shown in Fig. 7, the encrypted handshake of TLSv1.2 is smoothly done with MPTCP and the MPTCP encrypted data transmission is done by both interfaces (Mobile 3G and WiFi) as show the Fig. 8 and 9.

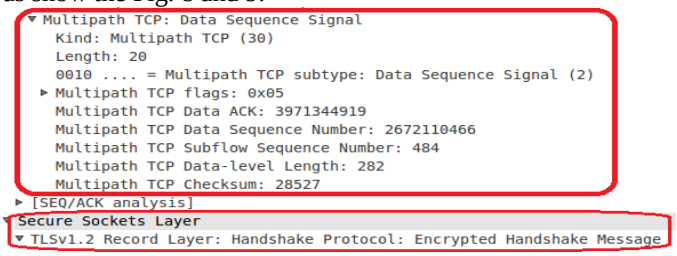

Fig. 7. MPTCP encrypted handshake with TLSv1.2

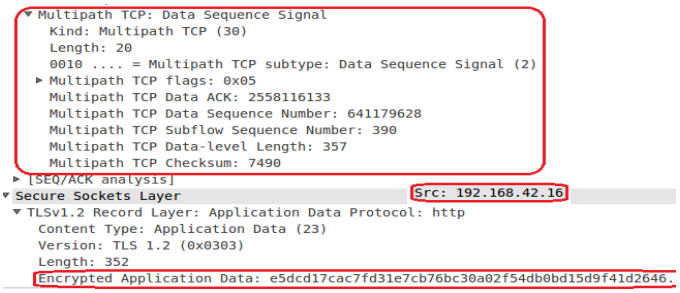

Fig. 8. MPTCP encrypted data transmission through Mobile 3G interface

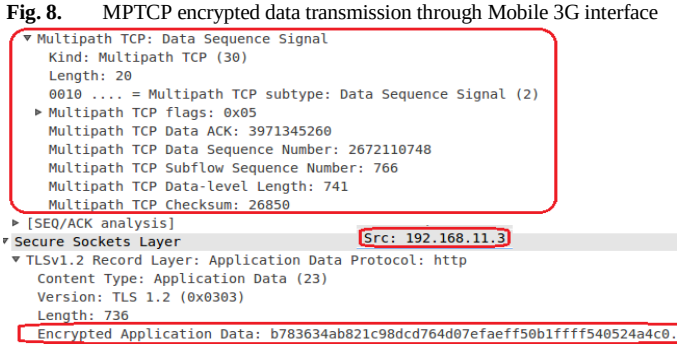

Fig. 9. MPTCP encrypted data transmission through WiFi interface

B. Comparative Analysis of MPTCP with TLS and TCP with TLS

In this section, the comparison of Multipath TCP with TLS and traditional TCP with TLS is presented. For which we have selected three parameters to evaluate our study.

1) Encrypted Packets Ratio
2) TCP Retransmission Ratio
3) TCP connection Termination Ratio
4) TCP connection Reset Ratio

1) Encrypted Packets Ratio

In Fig. 10, Encrypted packets ratio of MPTCP and TCP with using TLS are compared. The maximum number of packets are encrypted in first scenario 'MPTCP with TLS default (3G+WiFi)' and 97% packets are encrypted in second scenario 'MPTCP with TLSv1.2 (3G+WiFi)'. The other four scenarios show the encrypted packets ratio of TCP with TLS default security and TLSv1.2 by both interfaces (WiFi/3G) separately. The ratio of the TCP encrypted packets on WiFi interface are 93% and 92%. The ratio of the TCP encrypted packets on 3G interface are 88% and 87%. So the results show that the TLS provide greater security in MPTCP with respect to TCP.

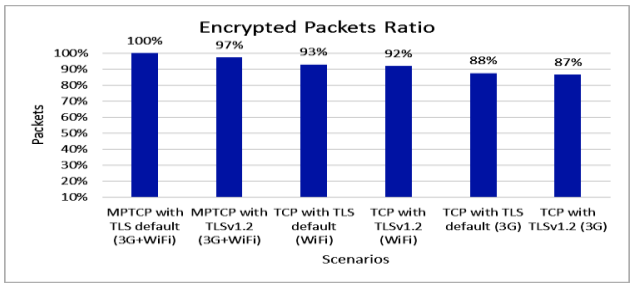

Fig. 10. Encrypted Packets Ratio

2) TCP Retransmission Ratio

In Fig. 11, TCP retransmission ratio of MPTCP and TCP with using TLS are compared. In first scenario 'MPTCP with TLS default (3G+WiFi)', 6% packets are retransmitted and 5% packets are retransmitted in second scenario 'MPTCP with TLSv1.2 (3G+WiFi)'. The other four scenarios show the retransmission ratio of TCP with TLS default security and TLSv1.2 by both interfaces (WiFi/3G) separately. The ratio of the TCP retransmission on WiFi interface is 0% because WiFi interface connected with wired connection in which no retransmission occur with respect to 3G interface. The ratio of the TCP retransmission on 3G interface is 7% and 6%. So the results show that there is minimum TCP retransmission ratio in MPTCP with respect to TCP.

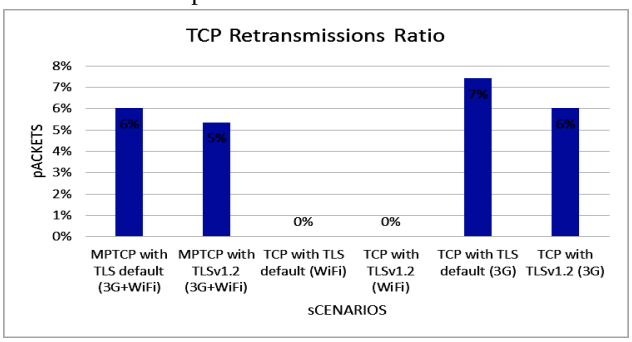

Fig. 11. TCP Retransmissions Ratio

3) TCP Connection Termination Ratio

In Fig. 12, TCP connection termination ratio of MPTCP and TCP with using TLS are compared. In first scenario 'MPTCP with TLS default (3G+WiFi)', 7% packets is sent and received for TCP connection termination and 8% packets are sent and received for TCP connection termination in the second scenario 'MPTCP with TLSv1.2 (3G+WiFi)'. The other four scenarios show the connection termination ratio of TCP with TLS default security and TLSv1.2 by both interfaces (WiFi/3G) separately. The ratio of the TCP connection termination on WiFi interface is 7% and 7%. The ratio of the TCP retransmission on 3G interface is 8% and 9%. So the results show that there is minimum TCP connection termination ratio in MPTCP with respect to TCP.

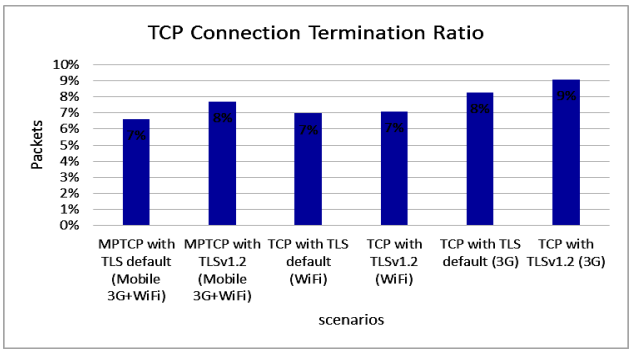

Fig. 12. TCP Connection Termination Ratio

4) TCP Connection Reset Ratio

In Fig. 13, TCP connection reset ratio of MPTCP and TCP with using TLS are compared. In first scenario 'MPTCP with TLS default (3G+WiFi)', 4% request for TCP connection reset is sent and received and 3% request for TCP connection reset is sent and received in second scenario 'MPTCP with TLSv1.2 (3G+WiFi)'. The other four scenarios show the connection reset ratio of TCP with TLS default security and TLSv1.2 by both interfaces (WiFi/3G) separately. The ratio of the TCP connection reset request on WiFi interface is 4% and 3%. The ratio of the TCP connection reset request on 3G

interface is 4% and 5%. So the results show that there is minimum TCP connection reset ratio in MPTCP with respect to TCP.

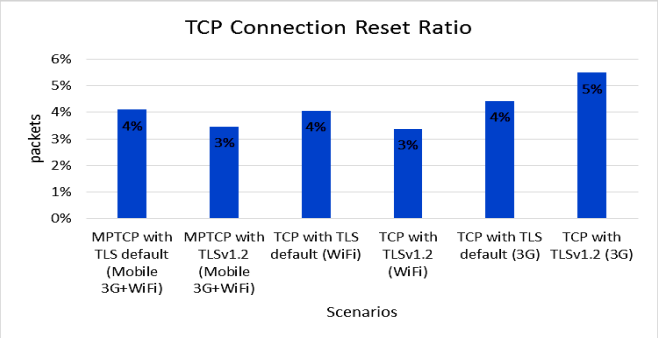

Fig. 13. TCP Connection Reset Ratio

TLS encrypted handshake is done with multiple interfaces and encrypted data is transmitted through multiple interfaces. Above implementation analysis shows that TLS is adoptable by MPTCP. In Comparative Analysis, when we have multiple interfaces, the results also show that MPTCP with TLS is effective as compared to TCP with TLS due to the better encryption rate and less connection termination for overall traffic.

V. CONCLUSION & FUTURE WORK

We present the real time implementation of MPTCP with TLS. We evaluate our work on the basis of MPTCP connectivity with secure data transmission and comparative analysis (MPTCP with TLS v/s TCP with TLS. In the first part, MPTCP connectivity with secure data transmission is done with TLSv1.2. In Second, the comparative analysis show that TLS provides greater security as compared to regular TCP. There is 96%-100% encryption is done in MPTCP while regular TCP have only 86-87%. The TCP retransmission is reduced by 14% in MPTCP as compared to regular TCP. The TCP connection termination and connection reset request is also reduced by 10%. To overcome the security hazards of MPTCP, TLS is adoptable as concluded in our research.

The further research will focus on the categorization of threats and attacks on TLS and MPTCP. Additionally, the detailed comparative analysis will be performed of all specified and proposed techniques.

REFERENCES

[1] Mahboob, A., & Ikram, N, (2004), "Transport Layer Security (TLS)–A Network Security Protocol for E-commerce", Technical report, National University of Science & Technology.

[2] Dierks, T. (2008, August). The transport layer security (TLS) protocol version 1.2 (No. RFC 5246).

[3] Williams, N., Stewart, L., & Armitage, G. (2013, April). Design Overview of Multipath TCP version 0.3 for FreeBSD-10. Swinburne University of Technology, Centre for Advanced Internet Architectures (CAIA), Melbourne/Australia, Tech. Rep. 130424A.

[4] Paasch, C., Detal, G., Duchene, F., Raiciu, C., & Bonaventure, O. (2012, August). Exploring mobile/WiFi handover with multipath TCP. In Proceedings of the 2012 ACM SIGCOMM workshop on Cellular networks: operations, challenges, and future design (pp. 31-36). ACM.

[5] Ford, A., Raiciu, C., Handley, M., & Bonaventure, O. (2013). TCP extensions for multipath operation with multiple addresses (No. RFC 6824).

[6] Barré, S., Paasch, C., & Bonaventure, O. (2011). Multipath TCP: from theory to practice. In NETWORKING 2011 (pp. 444-457). Springer Berlin Heidelberg.

[7] Raiciu, C., Paasch, C., Barre, S., Ford, A., Honda, M., Duchene, F., & Handley, M. (2012, April). How hard can it be? designing and implementing a deployable multipath TCP. In Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation (pp. 29-29). USENIX Association. ACM.

[8] Raiciu, C., Barre, S., Pluntke, C., Greenhalgh, A., Wischik, D., & Handley, M. (2011). Improving datacenter performance and robustness with multipath tcp. ACM SIGCOMM Computer Communication Review, 41(4), 266-277.

[9] Barré, S., Bonaventure, O., Raiciu, C., & Handley, M. (2011). Experimenting with multipath TCP. ACM SIGCOMM Computer Communication Review,41(4), 443-444.

[10] Van der Pol, R., Bredel, M., Barczyk, A., Overeinder, B., van Adrichem, N., & Kuipers, F. (2013, June). Experiences with MPTCP in an intercontinental OpenFlow network. In Proceedings of the 29th TERENA Network Conference (TNC2013).

[11] Raiciu, C., Bonaventure, O., Paasch, C., Gont, F., & Bagnulo, M. (2015). Analysis of Residual Threats and Possible Fixes for Multipath TCP (MPTCP) (No. RFC 7430).

[12] Bagnulo, M. (2014). Secure Multipath TCP. Network Working Group M. Bagnulo Internet-Draft.

[13] Mazieres, D., Boneh, D., Slack, Q., Hamburg, M., Bittau, A., & Handley, M. (2014). Cryptographic protection of TCP Streams (tcpcrypt). Network Working Group Internet-Draft.

[14] Turner, S. (2014). Transport Layer Security. IEEE Internet Computing, 18(6).

[15] Paasch, C., Khalili, R., & Bonaventure, O. (2013, December). On the benefits of applying experimental design to improve multipath TCP. InProceedings of the ninth ACM conference on Emerging networking experiments and technologies (pp. 393-398). ACM.

[16] Scharf, M., & Ford, A. (2013). Multipath TCP (MPTCP) application interface considerations (No. RFC 6897).

[17] Ford, A., Raiciu, C., Handley, M., & Bonaventure, O. (2013). TCP extensions for multipath operation with multiple addresses (No. RFC 6824).

[18] Ford, A., Raiciu, C., Handley, M., Barre, S., & Iyengar, J. (2011).Architectural guidelines for multipath TCP development (No. RFC 6182).

[19] Kostopoulos, A., Warma, H., Levä, T., Heinrich, B., Ford, A., & Eggert, L. (2010, June). Towards multipath TCP adoption: challenges and opportunities. In Next Generation Internet (NGI), 2010 6th EURO-NF Conference on (pp. 1-8). IEEE.

[20] Dreibholz, T., Zhou, X., & Fa, F. (2015, March). Multi-Path TCP in Real-World Setups–An Evaluation in the NORNET CORE Testbed. In 5th International Workshop on Protocols and Applications with Multi-Homing Support (PAMS), Gwangju/South Korea.

[21] Hesmans, B., Tran-Viet, H., Sadre, R., & Bonaventure, O. (2015). A first look at real multipath tcp traffic. In Traffic Monitoring and Analysis (pp. 233-246). Springer International Publishing.

[22] Peng, Q., Walid, A., Hwang, J. S., & Low, S. H. (2014). Multipath TCP: Analysis, Design, and Implementation. IEEE/ACM Transactions on Networking.

[23] Pearce, C., & Zeadally, S. (2015). Ancillary Impacts of Multipath TCP on Current and Future Network Security. Internet Computing, IEEE, 19(5), 58-65.

[24] Welcome to the Linux Kernel MultiPath TCP project. (n.d.). Retrieved January 01, 2016, from http://multipath-tcp.org./

[25] Díez, J., Bagnulo, M., Valera, F., & Vidal, I. (2011). Security for multipath TCP: a constructive approach. International Journal of Internet Protocol Technology, 6(3), 146-155.

[26] Paasch, C. (2014). Improving Multipath TCP (Doctoral dissertation, Universitatea Politehnica din Bucuresti, Romania).

[27] Bonaventure, O., & Paasch, C. (2012). Securing the MultiPath TCP handshake with external keys.

[28] Nordmark, E., & Bagnulo, M. (2009). Shim6: Level 3 multihoming shim protocol for IPv6 (No. RFC 5533).