Multipath Transfer Control Protocol based Approach with Energy Savings and Qos in a Multi Homed MCC Network Environment

M. Induja, S. Bhavan Kumar, V. Gopalakrishnan, R. Karthi and Dr.M. Prakash

Abstract--- The mobile cloud computing (MCC) systems in multi homed devices can transmit the data through several paths simultaneously by using the Multipath Transfer Control Protocol (MPTCP). By using the MPTCP connection under a network attack, it gives a poor path or broken path, it also affects the stable paths. It leads to the performance degradation. The MPTCP technology in MCC consumes high energy consumption and it gives low services. In this paper, we propose a Energy efficient framework in multilevel clustering performance to build a hierarchical network. To reduce the Low rate distributed denial of service (LDDOS), the Quality Oriented Distributed (QOD) Routing increases its efficiency by using i) neighbor selection of node to reduce transmission delay. ii) traffic redundant elimination to increase transmission throughput.

Index Terms--- Mobile Cloud Computing, Multipath TCP, Error Detection, Energy Efficient Usage.

I. INTRODUCTION

With the ever-growing appeal for mobile computations, and the widespread of wired and wireless systems, the several heterogeneous wireless networks with increased quality of mobile cloud computing (MCC) and present Internet services are accessed by mobile Internet. The MPTCP has emerged with the high download speed of vast cloud data to increase their overall throughput by using several network path simultaneously in the multi-homed mobile devices. The MCC devices is embedded with one or more network interface and it is attached with heterogeneous multi access at same time.

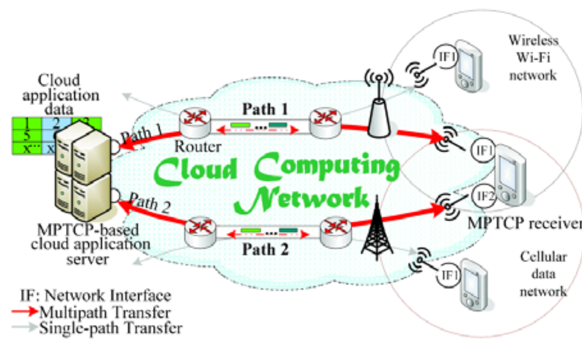

Fig. 1: A MPTCP Mobile Cloud Network

The MPTCP that provides simultaneous use of multiple network interfaces and permits cloud systems to benefit the multiple access links for simultaneous data transmission. Figure 1 illustrates the MPTCP cloud network that involves a cloud application data, MPTCP based cloud server (UE-A), which can communicate each other by wireless and cellular network. Thus MPTCP has a good bandwidth aggregation resources and it is not only beneficial for the MCC systems but also for the better network based connectivity robustness. However, MPTCP provides the similar socket APIs, backward-compatible cloud application and regular TCP. The backward compatibility will be the success of MPTCP in the current and future enhancement cloud network applications.

M. Induja, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:induja26.1997@gmail.com
S. Bhavan Kumar, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:bhavansuga555@gmail.com
V. Gopalakrishnan, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:gopalakrishnan.vcse@ksrce.ac.in
R. Karthi, UG Scholar, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:karthiksr7696@gmail.com
Dr.M. Prakash, Assistant Professor, Department of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, Namakkal. E-mail:mmsprakash@gmail.com

The first important aspect of MPTCP-based data transmission in cloud computing platform is completely related to prevent the utilization of poor-performance paths in multipath transmission. Though MPTCP has many attractive benefits to MCC applications, it is a hopeful technology for data delivery, and it faces many challenges to be addressed. While applying MPTCP into the mobile cloud multipath transmission, an each and every path individually performs data traffic in the cloud according to its corresponding QoS-related parameters. Allocation of cloud application data in a poor-performing path leads to the transmission interruption to the stable paths. That is, the poor performance path can also affect other significant paths and affects the overall performance in application level.

The important topic for MPTCP cloud computing services is to define a poor performing path and transmitting the cloud application data.

In this topic, more researchers are doing researches of detecting the poor performance in the multipath and how to manage it by using its management mechanisms. Now-a-days the MPTCP has avoided that its performance is degraded by cyber attacks, low rate distributed denial of service (LDDOS), TCP retransmission timeout (RTO) mechanisms to attack a TCP connections. The development of cloud computing is depends upon network security and it shows that LDDoS attacks is prevalent on future Internet due to moderately low rate and ingenious concealment. The LDDoS attacks does not investigate the MPTCP performance it is likely to be achieved when it is applied to MCC applications.

Another important aspect is multipath transmission and it is caused by applying the MPTCP to MCC. MPTCP not only provides the good performance but also it has a high energy cost to the MCC devices. Since there is a limited power capacities in the batteries in mobile devices, the efficient energy utilization is the urgent topic in investigation. Recently many researchers has concentrated on the energy optimization in MPTCP. To define their solutions they concentrates on low energy consumptions and long life battery by shifting the packets from high energy cost path to low energy cost path.

In this paper we propose solution for energy efficiency in MPTCP for multi-homed MCC systems to address the issues in energy consumption and LDDoS attacks. The goals of MPTCP-La/E^2 are: i) to optimize the energy while maintaining the quality of multipathing in cloud services. ii) to avoid the performance degradation in multipath transmission that are caused by LDDoS attacks. The proposed system has a vast area of evaluation in performance metrics. The simulation results illustrates how multipath performs in MTCP specifically in QoS and in energy efficiency. The MPTCP has important contribution in the following aspects:

- It introduces energy efficient MPTCP cloud data scheduling algorithm to overcome the LDDoS transmission performance and its path states
- It explores the familiar LDDoS attacks on MPTCP performance and it provides LDDoS-aware multipath management mechanism.

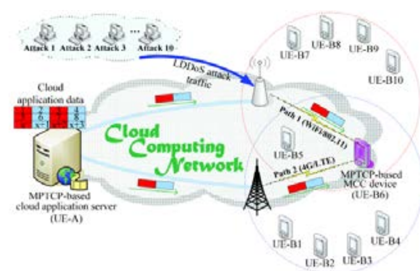

Fig. 2: A Dual-Dumbbell Simulation Topology with LDDOS Attacks

II. PROBLEM STATEMENT

To investigate the performance of MPTCP, the dual dumbbell simulation topology has a reasonable LDDoS attack traffic illustrated in Fig 2. In this topology, The MPTCP has sender and receiver based on cloud application and it is connected through a network interface and it is attached with a LDDoS attack traffic. The bandwidth between each node is set to 100Mb with 25ms of propagation delay. The entire simulation time is 60 seconds.

Since LDDoS attack has the UDP protocol with Constant Bit Rate (CBR) traffic, the attackers such as (Attacker.1, Attacker.2,…, Attacker.10) generates UDP/CBR packets and the attack starts at 5.1th second of simulation time. The characteristics of LDDoS attacks, LDDoS (T, L, R) = LDDoS (100 ms, 100ms, 1 Mbps), in which the T denotes attack period, L denotes attack duration and R denotes attack rate respectively.

In MPTCP cloud computing, each and every path has its own congestion window (cwnd), the sender executes the TCP New Reno congestion control mechanisms to each path separately. However, the paths in the MPTCP connections does not perform alone, it influences each other in fully-ordered data delivery services. It identifies the LDDoS attacks against the current network platform are likely to increase the performance of cloud computing widely. If a network path performs LDDS attacks, it frequently experiences the abrupt transmission interruption. Due to this, the application level performance degradation will occur.

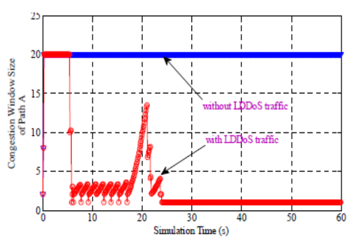

Fig. 3: The Congestion Window Size of Path A with or without a LDDoS Attack

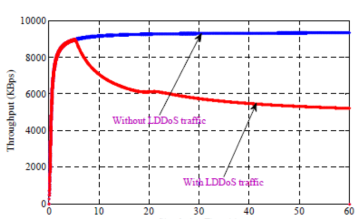

Fig. 4: The throughput Comparison with or without a LDDoS Attack

Fig. 3 Shows the congestion window size of path A with and without traffic. This graph denotes the value of path A decreases when LDDoS attacks has launched after 5.1 seconds of simulation. The LDDoS attacks can exploit the TCP's RTO mechanism and make MPTCP sender frequently experience a RTO event on path A and its cwnd is set to same segment repeatedly due to the timeout.

Fig. 4 shows the overall performance of MPTCP whenever the LDDoS attackers are enabled or disabled. The MPTCP performance decreases sharply at LDDoS attacks because its packets attempts to deny the bandwidth to give a sub flow in TCP connection on path A and vast path dissimilarities between the affected path A and also to the other stable paths. But unfortunately the MPTCP is not suitable for preventing the poor performance path in multipath transmission. The Effective multipath manager includes some mechanisms to by considering the intrinsic characteristics of LDDoS attacks and MPTCP. The goals of proposed system are (i) to enhance the MPTCP performance in cloud environment (ii) to declare a poor performance path and prevent the usage of that path in multipath transmission time.

III. THE DESIGN OF MPTCP-LA/E^2

Fig. 5 shows that the MPTCP architecture includes MPTCP sender (multi-homed cloud application server), MPTCP receiver (multi-homed device) and multiple asymmetric paths. In sender side, there are two component, LDDoS-aware multipath manager (LaM^2) and energy-efficient data scheduler (E^2DS). In receiver side, arrived packets will be buffered and reordered packets, when the cloud application data is split into number of packets.

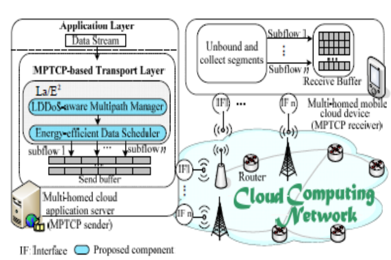

Fig. 5: Architecture of MPTCP-La/E^2

The functions of LDDoS multipath manager and energy efficient data scheduler are outlined below:

- The LaM^2 is to monitor to the transmission quality of every path in MPTCP, choosing the subset of suitable path for multipathing and switching the path to proper state.
- The E^2DS is used to detect the energy cost of each path, achieving bandwidth aggregation and energy savings by considering per-path's transmission.

A. *LDDoS-Aware Multipath Manager*

A path in LDDoS attack can frequently encounter timeout and paths are easily broken. MPTCP path management inherits TCP operations for broken path detection.

1. unnecessary retransmissions: When new data is allocated to a broken path for transmission, the sender will perform unnecessary retransmissions via broken path
2. Performance degradation: The transmission interruptions in the broken path will affect efficiency of other stable paths and degrade the performance of MPTCP.

B. *Energy-Efficient Data Scheduler*

Applying MPTCP to a MCC mobile devices consists of high energy consumption for concurrent use of multiple network interfaces. The goal of E2DS is to optimize MPTCP's scheduler and help MPTCP be more energy efficient, by jointly considering the transmission state (active, potentially broken, or inactive) and the energy cost of each path.

PSmultipathing=PSactive U PSpotentially broken

IV. ENERGY EFFICIENCY TESTING

A. *Simulation Topology*

Modern mobile devices (e.g., smartphones) are already embedded with wireless Wi-Fi and 4G LTE cellular interfaces simultaneously. All the single interface mobile terminals and UE-A are inter-communicated via traditional TCP connections.In order to convince the E2DS component is good and effective, the attack pulse R of these LDDoS attacks only varies randomly between 0-0.2Mbps.

B. *Simulation Results*

1) Energy Efficiency Comparison

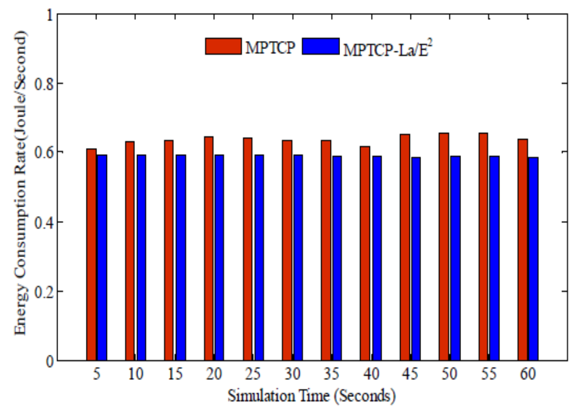

Fig. 6: Comparison of Energy Consumption Rate

MPTCP requires higher energy consumption than MPTCP-La/E2. With a total simulation time of 60 seconds, MPTCP-La/E2's energy consumption rate is 19.46% lower than that of MPTCP.

2) Throughput Performance Comparison

Calculate both the energy consumption and the current available cwnd size of each path, and then offload a certain amount of data required to be sent from a high energy-cost path to an energy efficient one.

In contrast, MPTCP does not trade throughput performance for energy-savings, it just simply makes full use of the multipath resources for bandwidth aggregation and data delivery.

Although MPTCP-La/E2's throughput is lower than that of MPTCP, it should be noted that there is more potential for energy-savings in MPTCP-La/E2 than the MPTCP scheme. After 60 seconds of simulation time, MPTCP-La/E2's average throughput is only 4.3% lower than that of MPTCP.

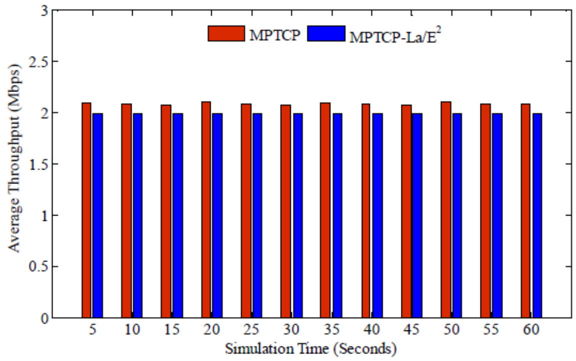

Fig. 7: Comparison of Average Throughput

3) Users' Quality of Experience for Video Streaming

Peak Signal-to-Noise Ratio (PSNR) is used to evaluate the video transmission performance.

$$PSNR = 20\log_{10}\left(\frac{Bitrate_{\max}}{\sqrt{(Thr_{\exp} - Thr_{crt})^2}}\right)$$

Threxp and Thrcrt are the average Bit rate of the video required to be sent, The values of both Bit ratemax and Threxp are 2Mbps in our tests.

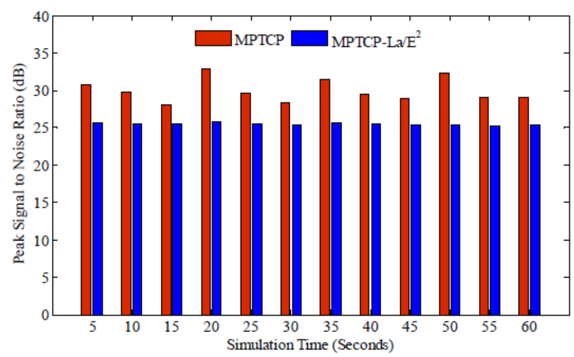

Fig. 8: Comparison of Peak Signal-to-Noise Ratio

The energy-aware scheduling mechanism of the MPTCP-La/E2 affects directly the PSNR performance which is lower than that of MPTCP. This is actually a necessary 'cost' for applying an energy optimization operation to the MPTCP.

V. Conclusion

Interested by the facts LDDoS attacks that caused by a poor performance path can present a impact on MPTCP's performance and QoS, this paper proposes a LDDoS attack-aware energy-efficient for multi-homed MCC systems. MPTCP mainly consists of two components, Energy Efficient data scheduler (La/E2) and LDDoS-aware multipath manager (LaM2) that is used to detect the transmission quality of each MPTCP path, switching a path to a proper state, and choosing a subset of suitable paths for multipathing, and energy-efficient data scheduler (E2DS) that is used to achieve bandwidth aggregation and energy-savings by considering both the transmission state and energy cost of each path When applying E2DS to MPTCP, the energy usage is optimized and the users' quality of experience is maintained. The simulation results demonstrate that MPTCP with LaM2, the potentially broken can be timely detected and the application-level performance is enhanced.

Acknowledgment

The first two authors contributed equally to this work and share the first authorship. This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61562044, and by the Soonchunhyang University Research Fund.

References

[1] H. Hu, Y. Wen and D. Niyato, "Public Cloud Storage-Assisted Mobile Social Video Sharing: A Super modular Game Approach", IEEE Journal on Selected Areas in Communications, Vol.35, No.3, Pp.545-556, 2017.

[2] Y. Liu, M.J. Lee and Y. Zheng, "Adaptive Multi-Resource Allocation for Cloudlet-Based Mobile Cloud Computing System", IEEE Transactions on Mobile Computing, Vol.15, No.10, Pp. 2398-2410, 2016.

[3] C. Xu, P. Wang, C. Xiong, X. Wei and G.M. Muntean, "Pipeline Network Coding-Based Multipath Data Transfer in Heterogeneous Wireless Networks", IEEE Transactions on Broadcasting, Vol. 63, No. 2, Pp. 376-390, 2017.

[4] Y. Cao, C. Xu, J. Guan and H. Zhang, "CMT-CC: Cross-Layer Cognitive CMT for Efficient Multimedia Distribution over Multi-homed Wireless Networks", Wireless Personal Communications, Vol. 82, No. 3, Pp.1643-1663, 2015.

[5] A. Ford, C. Raiciu, M. Handley and O. Bonaventure, "TCP extensions for multipath operation with multiple addresses", IETF RFC, 2013.

[6] Q. Peng, A. Walid, J. Huwang and S.H. Low, “Multipath TCP: analysis, design, and implementation”, IEEE/ACM Transactions on Networking, Vol. 24, No. 1, Pp. 596-609, 2016.

[7] C. Xu, J. Zhao and G.M. Muntean, “Congestion Control Design for Multipath Transport Protocols: A Survey”, IEEE Communications Surveys and Tutorials, Vol.18, No.4, Pp. 2948-2969, 2016.

[8] H. Sinky, B. Hamdaoui and M. Guizani, “Proactive Multi-Path TCP for Seamless Handoff in Heterogeneous Wireless Access Networks”, IEEE Transactions on Wireless Communications, Vol. 15, No. 7, Pp. 4754-4764, 2016.

[9] Q. Coninck, M. Baerts, B. Hesmans and O. Bonaventure, “Observing real smartphone applications over multipath TCP,” IEEE Communications Magazine, Vol.54, No. 3, Pp. 88-93, 2016.

[10] B. Oh and J. Lee, “Feedback-Based Path Failure Detection and Buffer Blocking Protection for MPTCP,” IEEE/ACM Transactions on Networking, Vol. 24, No. 6, Pp. 3450-3461, 2016.

[11] Y. Cao, F. Song, G. Luo, Y. Yi, W. Wang, I. You and W. Hao, “(PU) 2M2: A Potentially Underperforming-aware Path Usage Management Mechanism for Secure MPTCP-based Multi pathing Services”, Concurrency and Computation: Practice and Experience, 2017.

[12] P. Dong, J. Wang, J. Huang, H. Wang and G. Min, “Performance Enhancement of Multipath TCP for Wireless Communications With Multiple Radio Interfaces”, IEEE Transactions on Communications, Vol. 64, No. 8, Pp. 3456-3466, 2016.

[13] Y. Zhang, H. Mekky, Z. Zhang, F. Hao, S. Mukherjee and T.V. Lakshman, “SAMPO: Online sub flow association for multipath TCP with partial flow records”, Proc. of IEEE INFOCOM, Pp. 1-9, 2016.

[14] K. Xue, J. Han, H. Zhang, K. Chen and P. Hong, “Migrating Unfairness Among Sub flows in MPTCP With Network Coding for Wired-Wireless Networks”, IEEE Transactions on Vehicular Technology, Vol. 66, No. 1, Pp.798-809, 2017.

[15] J. Wu, C. Yuen, B. Cheng, M. Wang and J. Chen, “Streaming High-Quality Mobile Video with Multipath TCP in Heterogeneous Wireless Networks”, IEEE Transactions on Mobile Computing, Vol. 15, No. 9, Pp. 2345-2361, 2016.

[16] A. Ali, J. Qadir, A. Sathiaseelan and K. Yau, “MP-ALM: Exploring Reliable Multipath Multicast Streaming with Multipath TCP”, Proc. of IEEELCN, Pp. 138-146, 2016.

[17] B. Arzani, A. Gurney, S. Cheng, R. Guerin and B. Loo, “Deconstructing MPTCP Performance”, Proc. of IEEE ICNP, Pp. 269-274, 2014.

[18] Y. Cui, L. Wang, X. Wang and Y. Wang, “FMTCP: A Fountain Code-Based Multipath Transmission Control Protocol”, IEEE/ACM Transactions on Networking, Vol. 23, No .2, Pp. 465-478, 2015.

[19] Y. Lim, Y. Chen, E.M. Nahum, D. Towsley and K. Lee, “Cross-layer path management in multi-path transport protocol for mobile devices”, Proc. of IEEE INFOCOM, Pp.1815-1823, 2014.

[20] J. Luo, X. Yang, J. Wang, J. Xu, J. Sun and K. Long, “On a Mathematical Model for Low-Rate Shrew DDoS”, IEEE Transactions on Information Forensics and Security, Vol.9, No.7, Pp. 1069-1083, 2014.