International Journal of Control and Automation
Vol. 11, No. 11 (2018), pp.1-18
http//dx.doi.org/10.14257/ijca.2018.11.11.01

A Multi-homing Based Framework Against Denial of Service Open Threat Signaling in Healthcare Environment

Piyush Yadav[1] and Rajeev Agrawal[2]

[1,2]Department of Electronics and Communication Engineering,
G L Bajaj Institute of Technology and Management, Greater Noida, India
[1]piyushyadav1985@gmail.com, [2]rajkecd@gmail.com

Abstract

Transmission of critical data in ubiquitous healthcare solutions requires a high degree of reliability. Literature on several threats to uninterrupted data transmission and suggested schemes to avoid them or minimize their effect are available. Denial of Service is one of the severe attacks which can result in complete failure of the network connectivity in terms of no service error. It is therefore crucial to detect such attack and deploy schemes which can recover the connectivity and access to services. This paper discusses the instances, effect and mitigation plans for a network under the Denial of Service (DoS) open threat Signaling in healthcare environment. The aim of this paper is to evaluate the multiple methods and shows how the Multi-homing feature of Stream Control Transmission Protocol (SCTP) can be exploited to combat such open threats. The performance analysis of suggested methods during DoS attack has been studied in terms of network metrics such as received packets, dropped packets, packet drop rate and throughput using Network Simulator 2 for electronic health (e-health) and mobile health (m-health) applications. The Simulation results indicate that the proposed multi-homing SCTP (MH-SCTP) framework improves the performance significantly in terms of meeting the quality of services (QoS) requirements under the DoS.

Keywords: *TCP, SCTP, Multi-homing, DoS, e-health, m-health, Quality of Service*

1. Introduction

The Advancement in the Communication systems and technologies in the recent time has touched different aspects and experiences of human life. Health is one of the major concerns, and providing healthcare service to common people irrespective of its location was a great challenge. However, due to exponential growth in mobile and other form of communication, it is possible to extend these services to even the remote areas using m-health and telemedicine initiative. Use of Information Technology for such critical application brings a new set of challenges which are more stringent and demanding in nature [1]. The devices are becoming smarter day by day with the advancement of long term evolution (LTE) systems. Recent version of Personal digital assistants (PDAs) and Smartphone's support several radio interfaces such as Bluetooth, Wi-Fi, Universal Mobile telecommunication systems (UMTS). Furthermore, it's important to leverage the potential of such multihoming environment in an application which are ubiquitous in nature and are highly mobile. Healthcare services are one such which is critical in nature with high level of diversity and pervasiveness [2].

Due to the nature of the healthcare data (*e.g.*, patient's medical history and diagnosis), e-health network reliability and security against the DoS threats are crucial and need to be addressed. Since early 2000, DoS attacks have been on the

Received (August 5, 2018), Review Result (September 3, 2018), Accepted (September 28, 2018)

ISSN: 2005-4297 IJCA

rise continuously, when the e-commerce sector became the first victim with a damage of $1.7 billion suffered by the targeted sites [3]. This has become one of the major concerns to test the reliability of any Electronic health (e-health) or mobile health (m-health) application. In a normal telemedicine or m-health application where the multiple hospitals, healthcare institutions and medical practitioners are connected, such attacks can have a very significant impact due to loss of critical as well as confidential data of the patients which can be further misused or corrupted. According to an International Business Machines (IBM) Corporation report, cyber-attacks directed towards healthcare ended up compromising 100 million healthcare records in the year 2017 [4]. The majority of these attacks are aimed to acquire patient's records which provide the attackers an easy access to a rich database of personal information such as credit card numbers, date of birth, *etc*. In 2014, Boston's Children Hospital in Massachusetts, USA, became the first health care organization to come under a potentially large scale DoS attack [5, 6]. The attack had the potential to disable the routing of electronic prescriptions to pharmacies, slow down critical emails shared within the departments and pose problems in accessing the health records of patients. Similarly, the U.S. Veteran Administration has suffered multiple cyber-attacks since 2011 [7].

In hospitals and healthcare centers, the normal profile of data is generally in the form of the patient's body parameters, patient's records and diagnosis reports, *etc*. The loss or theft of any of these data can straight away affect the patient's life in many cases [8]. Therefore, it is required to review the different methods which could help in mitigating the deleterious effects of any possible DoS attack. Reliability and security of the data for m-health are some of the key parameters which are to be addressed. While e-health network reliability and security have been the focus of research in recent years, still it remains an interesting research problem in terms of better models and their performance.

To overcome above discussed problems, we require a system within the framework which is specifically designed pertaining to the needs of a healthcare environment to tackle off effects of future DoS attacks. Taking this into cognizance the propose work studies the performance of different control protocol such as TCP with filtering and SCTP for more critical applications *i.e.*, Telemedicine. The presented paper discusses various non-conventional plans to implement an infrastructure that is better equipped against a DoS attack. The network configuration for TCP with filtering, SCTP and MH-SCTP is designed and QoS parameters of the propose network are compared, the network with multi-homing exhibits better performance in case of DoS attack in the healthcare environment.

The rest of the paper is organized as follows: Section 2 outlined the related work with a concise overview of the nature of a DoS attack and existing approaches to mitigate them. Section 3 gives the Proposed Research Design for Mitigation of DoS in Healthcare while Section 4 discusses the methodology. Section 5 provides an insight to the simulation process of the methods and discusses the results obtained. Finally, conclusions are given in Section 6.

2. Related Work

2.1. Review of DoS Attacks

DoS attack is an attempt to render certain resources unavailable for the intended user [9]. Attacks could be categorized as either as brute force and semantics attacks. Brute forces simply target networks by flooding them with high volume of useless traffic, while semantics attacks target the various vulnerabilities in the victim system. The basic DoS attack can be also of types such as:

(a) Smurf: In Smurf type attack, the attacker node sends out huge internet control message protocol echo traffic towards a set of internet protocol broadcast addresses. The Internet Control Message Protocol (ICMP) message, hence, have the spoofed source address as the victim. Smurf attacks end up flooding the victim's bandwidth. Ping of Death attack is a famous DoS technique that generates and sends non-standard ICMP packets to victim systems, crashing them easily.

(b) User Datagram Flood: Random ports in remote nodes are flooded with a large number of user datagram protocol (UDP) packets [10]. The purpose of this flooding is to slow down the victim so that it can no longer process any valid connection. One way of detecting and avoiding UDP flood is to monitor if the number of UDP datagrams from any source exceeds the decided threshold.

(c) Synchronization Flood: Occurring in TCP, synchronization (SYN) flood [11] exploits the technique of three-way handshake, a characteristic of TCP communication. SYN flooding is one of the most common methods for DoS.

In normal conditions, the client and server establish a communication link by the means of certain message signals as shown in Figure 1. The client requests a service from the server by the means of SYN signal. In return, the server responds by sending a SYN + ACK (Acknowledgement) signal back to the client, which at last sends another ACK signal in return, thus establishing a connection.

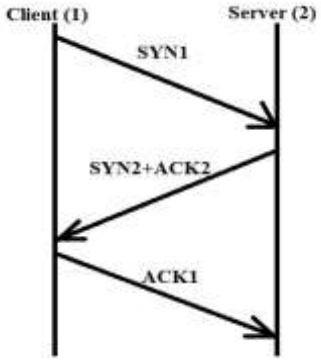

Figure 1. Three Way Handshake in TCP Proposed

In the case of SYN flood, the ACK signal from the server never arrives. This could be due to network congestion created by the attacker by flooding the network with an abnormally large number of unwanted packets. One of the most common ways to defend a network against a SYN flood attack are increasing the SYN-ACK queue length and decreasing the waiting time for time-out acknowledgement to arrive in a three-way handshake [12].

2.2. Existing Approaches to Mitigate DoS Attacks

Apart from the conventional methods that are used to tackle a case of Denial of Service, three other methods have been taken in consideration which might prove to be effective in alleviating DoS effects in a network. These methods are discussed in the following subsections.

2.2.1. Filtering in TCP: TCP filtering can be used as the first line of defense in the entire hospital network since most of the communication across the hospital happens through TCP. The DoS attack easily hack the data as in the case of Boston's Children Hospital. In the wireless sensor network, the TCP filtering methods track

the vital parameters of the patients within the hospital and these parameters are used to predict the normal profile or the nature of the data in advance. The data that can be categorized under this profile are patient's body parameters such as Electrocardiogram (ECG), Electroencephalogram (EEG), blood pressure, oxygen saturation level *etc.*, and allowing a filter to check and analyze the characteristics of incoming data[13], such as the flow and the size help in mitigating the effect of any possible DoS attack.

In this approach, the performance of the network against DoS is improved by making a small alteration in the existing TCP network structure. In a general environment, the normal profile, *i.e.*, the packet size, packet rate (flow) *etc.*, of the incoming information is usually predictive since we are aware of the type of data that is being transmitted. Using this property, a system was designed which uses a simple counter at the node to receive the data. The counter works as a preliminary screening to interact with the incoming data before the victim nodes and stores the packet information of the data coming from a reliable IP address as a 'cookie' and then checks every incoming packet against this parameter. The node rejects any data, deviating too much compared to the packet parameter value that is stored.

2.2.2. Stream Control Transmission Protocol: In [14, 15], the SCTP is used to replace TCP network and it was checked how effective an SCTP connection in case of a DoS attack. SCTP is a reliable unicast and connection-oriented network, which in many ways is like the TCP but different in some others as discussed in [16]. SCTP provides 32 bits cyclic redundancy check against TCP's 16 bit checksum. Also, SCTP can support multi-homing unlike TCP, the multi-homing is said to be a better option against DoS because of its better immunity against SYN flood. As a prevention strategy against SYN flooding, SCTP uses the cookie method during connection establishment. SCTP uses a four way handshake rather than three-way as in the case of TCP. The difference is the use of cookie which is a collection of all states and required by the server to ensure that the connection is valid as shown in Figure 2.

However, the SCTP can be implemented in any network by changing in the transport stack of the node of the network. This is the main challenge to implement the SCTP in place of TCP, which has already asserted its dominance in the networks. Even though due to its benefits, SCTP still remains a less popular choice than TCP. However, we have analyzed the performance of SCTP under Distributed Denial of Service (DDoS) in particular, and conclude whether switching to SCTP from TCP is a better option despite the need for change in the networks that it would require.

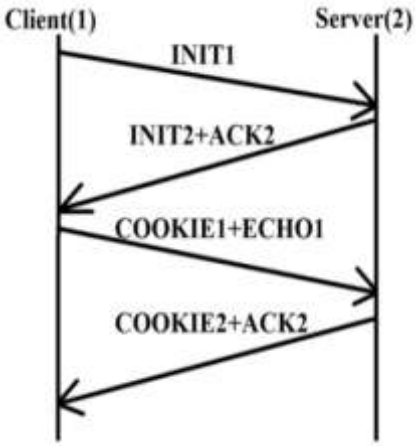

Figure 2. Four-Way Handshake in SCTP

Mobile Nursing Carts (MNC) [17] is an area where SCTP has major application. These MNCs requires uninterrupted wireless connection as well as the need to switch over to the other communication standards, where a suitable switching-tunnel protocol is needed and SCTP serves as the perfect option [18]. The SCTP is implemented as a tunnel between two different communication standards and it can help in tackling the effects of a possible DoS attack, especially SYN flooding as discussed earlier. Therefore, it is a crucial concern to make the hospital network more reliable against cyber-attacks and network overloading.

3. Proposed Design for DoS Mitigation in Healthcare: MH-SCTP

In the healthcare industries, the methods discussed above are generally used to overcome the problem of DoS attack.

The proposed approach of this paper is Multihoming SCTP (MH-SCTP). In a multi-homing system [19], the nodes are connected through more than one network. This ensures better reliability and performance. Multi-homing also proves to be an effective option for fault tolerance, transport network survivability and load sharing [20]. In Multi-homing systems, to reach the desired endpoint more than one transport address can be used as a destination address. The in-built multi-homing feature in SCTP allows it to support link backup for multi-homed nodes. When the primary link transmission fails, the data is sent over through the back-up (or secondary) link. Through SCTP multi-homing system, one transport layer association can be linked with multiple IP address at the multiple ends of the association. One of the advantages of using multi-homing is its need for minimal changes in the existing system of hosts and routers.

In this approach, features of multihoming are used where a circuit backup framework is used. In case a problem is detected in the network a path is automatically switched to other route to avoid the possible DoS attack in the network. We utilize route based architecture with general router by multihoming. One such instance can be considered the case of Boston's Children Hospital cyber-attack. Generally, attackers disable the routing of prescriptions from the department directed towards the pharmacy and derail the functioning of the hospital. The MH-SCTP is a better option in such cases of the hospital or in a healthcare environment to solve the issue by routing the data towards the secondary link, when the primary link was found to be dysfunctional, as shown in Figure 3.

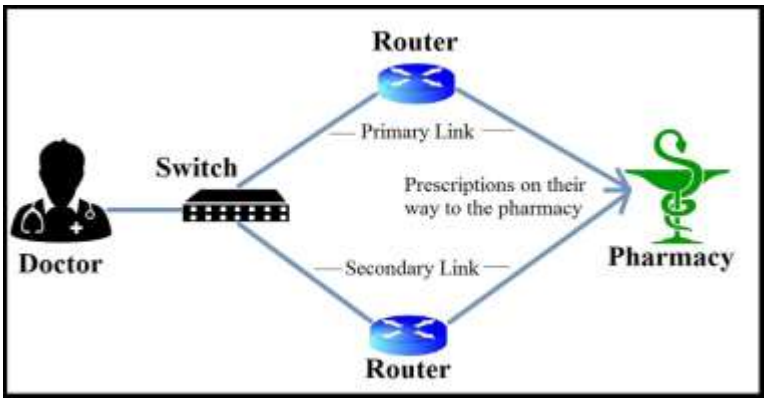

Figure 3. Proposed Multi-homing Design for Healthcare

To mitigate the effects of Denial of Service, we proposed a framework which is based on concept of backup path which helps restore the link in any Wireless network. Wireless sensor network (WSN) find a major application in healthcare

environment with each patient in a hospital as an individual node in the network which helps in keeping track of health parameters (such heart rate, oxygen saturation *etc*.) through sensors attached to the patients [8]. Like any other network, WSNs are also vulnerable to malicious attacks such as DoS. An attack on WSN especially in a hospital environment can even end up jeopardizing lives of the patient as crucial patient data can be at high risk. Here, noting the ability of nodes in a WSN to route themselves, we have proposed MH-SCTP to be used in case of a possible Denial of Service attack in WSNs as shown in Figure 4.

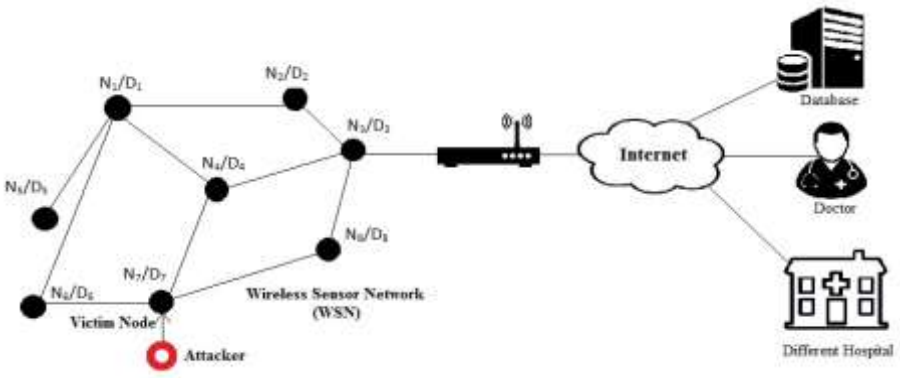

Figure 4. Denial of Service Attack on a WSN in a Hospital Environment

4. Methodology

4.1. Detection of the Victim Nodes/ Devices

Our course of action is described by the Algorithm to detect the victim node as shown in Figure 5, establishing a backup link in case of a DoS attack involves the identification of the victim node, or nodes, where the attacker has latched onto the network and from where the attack is being carried on.

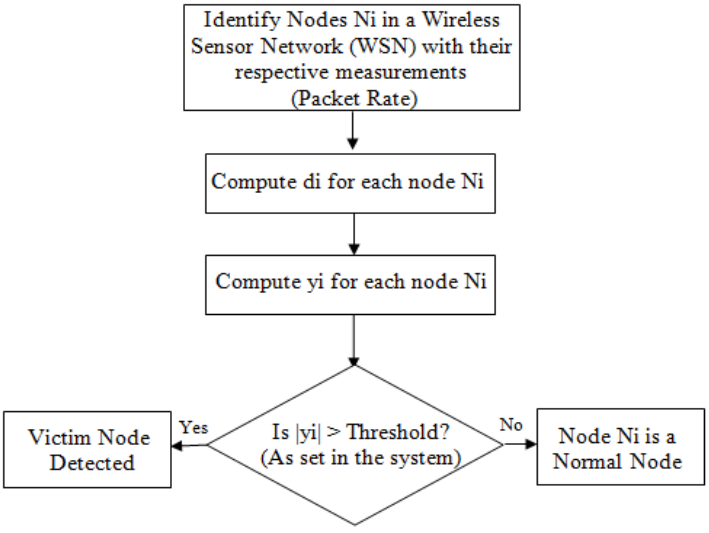

Figure 5. Algorithm to Detect the Victim Node

To find out the victim node(s), first of all the neighbouring nodes of N_i are identified, N_{i1}…..N_{ij} along with their measurements such as packet flow rate (or any other parameter set by user for the observation for any aberrance in the system).

The median med_i of all the measurements $[p_1^i, p_2^i, p_3^i \ldots p_j^i]$ is calculated and comparison of all the nodes are given in [21],

$$d_i = p_i - med_i \quad (1)$$

For n number of nodes, the algorithm computes di ∀ n (*i.e.*, X= $\{d_1, d_2, d_3 \ldots\ldots\ldots d_n\}$). Now, mean of X is calculated as [21],

$$\mu = \frac{1}{n} \sum_{i=0}^{n} di \quad (2)$$

To find any difference in usual pattern of packet flow in the network, the standard deviation of all nodes *i.e.*, of X is computed next, and given as [21],

$$\delta = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(d_i - \mu)^2} \quad (3)$$

After standardising X, we get set Y = $[y_1, y_2, y_3 \ldots\ldots\ldots\ldots y_n]$, where,

$$y_i = \frac{(d_i - \mu)}{\delta} \quad (4)$$

4.2. Link Placement Depending Upon the Number of Links Affected

The above algorithm helps in detecting the victim node, however, there might be more than one victim node and as a result more than one link may be affected or hampered. This observation translates into a need of instructions for correct link placement method depending on the number of link failed that will ensure uninterrupted data transfer by re-routing the packets on some back-up path, avoiding the victim links.

To suggest the best backup path link placement for any network, we will use the technique used for the same in case of link failures. Here instead of detecting the victim node, the probability of failure of any link is computed [22].

In case of one link failure, the probability that a backup link will be sufficient for k primary links [21],

$$1 - (1 - p)^k - kp(1 - p)^{k-1} \leq \varepsilon \quad (5)$$

where, p is the probability of link failure and ε is survivability guarantee parameter.

Taking the above condition, it is concluded that the backup network for single attacked link is given as [21]

$$\varepsilon \leq p < \frac{\sqrt{\varepsilon}}{M-1} \quad (6)$$

where, M is the total number of primary links.

In such a case, cycle protection is optimally suitable where

$$\varepsilon \leq p < \frac{\sqrt{\varepsilon}}{N^2 - N + 1} \quad (7)$$

For multiple link failure, cycle protection does not prove to be efficient and thus a one-hop approach is best suitable for multiple DoS affected links.

5. Model Analysis

5.1. Experimental Topologies

A test scenario is created to gaze the performance of a widely used TCP and state-of-art SCTP as shown in Figure 6. In the test network a node is created which act as an

attacker which is connected to the server through a router. To avoid any possible congestion in a network a high capacity of 5Gbps is used to simulate the test network. The hardware configurations of server and attacker nodes are treated to be identical to avoid any bias or advantage to the individuals. The nodes are having the configuration as Intel Core i7 4600 U 2.7 GHz (with Virtualization support), 8GB RAM, 45 GB hard drive. The router used for this is TP-Link Archer C1200 Gigabit Wireless Wi-Fi Router having 8GB RAM and an Ethernet Adapter with 2 ports.

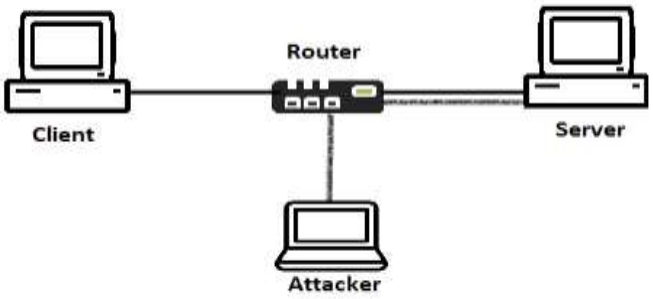

Figure 6. Test Scenario for Single Homing

A network as represented by Figure 7 is used to evaluate the performance of different SCTP specific attacks with the same network configuration as above. The processing speed of the router is taken higher than the speed of server and client node, the higher speed is taken to avoid any congestion in the network as simulation study will be carried out by increasing the rate of attack entering the network. The Simulation study was done in an open source environment using Ubuntu 16.10 LTS Debian Kernel.

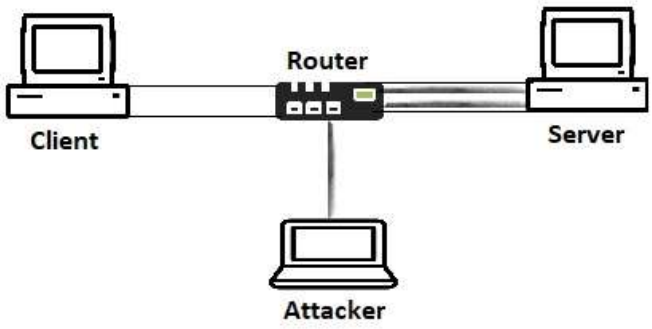

Figure 7. Test Scenario for Proposed MH-SCTP Design

The simulation was regulated in an environment where the network is affected by the attack and it was treated that a successful link was established within the client and the server with handshaking. In the process first server send a request to establish a connection with a client or vice-versa, client send an acknowledgement/ready signal to server and finally the data is send to the client. For a simulation environment the link from server to client is active for 130 seconds, however, the attacker nodes starts sending malicious packets after 35 seconds from the start of the server for 60 seconds. Between the client and server, the connection was limited to 100Mbps by dummynet [23] to avoid the environment becomes bottleneck resulting in congestion.

5.2. Simulation Validation and Results

Network Simulator 2 (NS2) was chosen as the platform for simulation [24] because of its ease of availability. Simulations were done on self-designed networks for the TCP with filtering, SCTP and Multi-homing as shown in Figure 8, Figure 9, and Figure10, respectively. The figures illustrate the network design of TCP, SCTP and MH-SCTP in NS2.

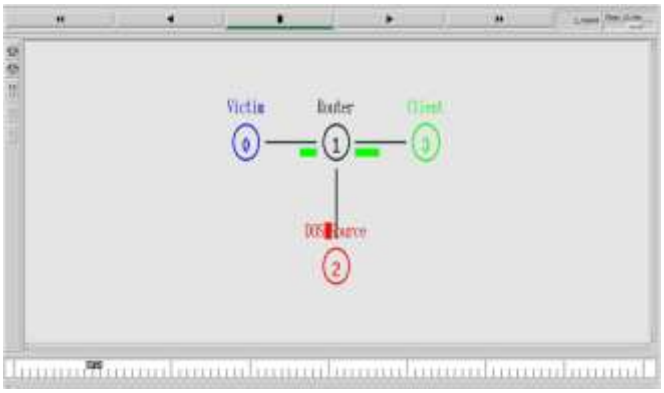

Figure 8. Simulation Configuration for TCP Network

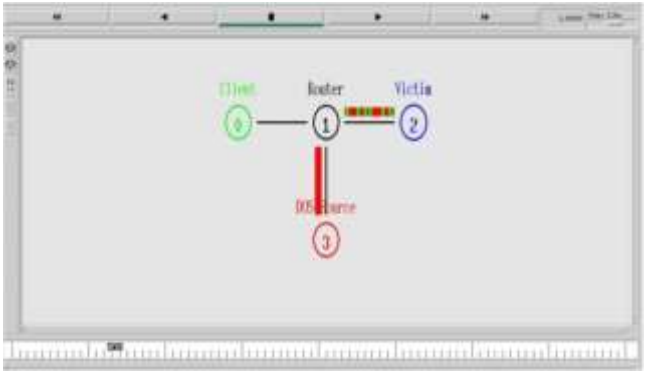

Figure 9. Simulation Configuration for SCTP Network

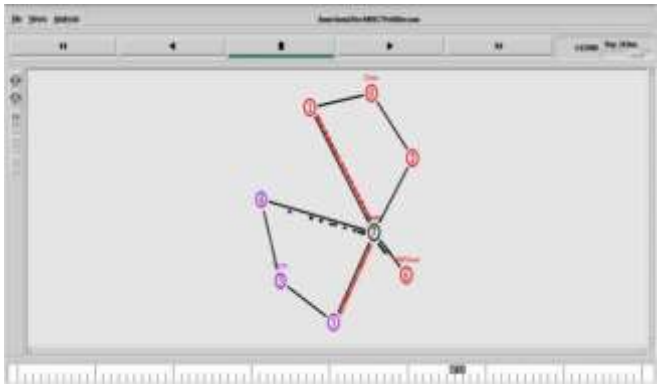

Figure 10. Simulation Configuration for Multi-homing SCTP Network

We have compared the performance of all the three methods by using the simulated results. Figures 11, 12 and 13 shows the comparison of the Throughput, received packets and the Dropped packets of TCP connection respectively, for the cases, *i.e.*, in the normal conditions, when a DoS event occurs and when TCP filtering is done. As observed from the figures, the TCP filtering alleviates the

impact of a DoS attack to some intensity. The improvement in performance goes as high as 50% for all the considered factors. Thus, this approach of a filter interacting with the incoming data prior, to be transmitted to the client can serve as the first line of defense and as an indicator of a DoS attack.

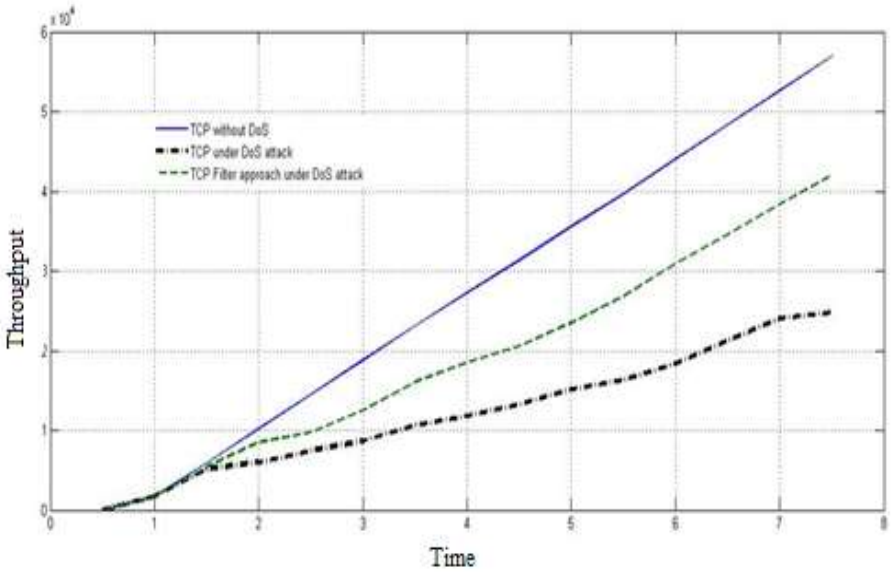

Figure 11. Throughput Comparison – TCP Filtering

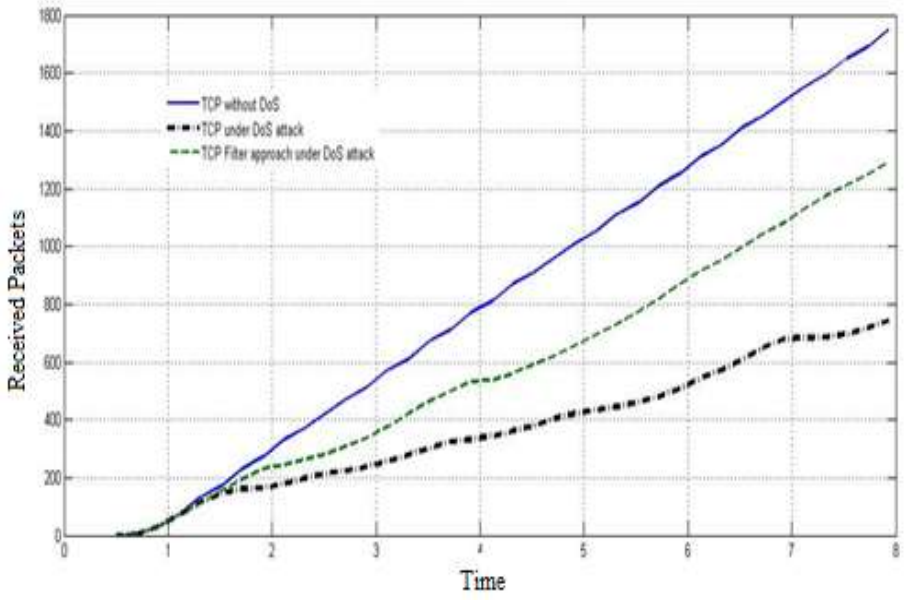

Figure 12. Received Packets Comparison– TCP Filtering

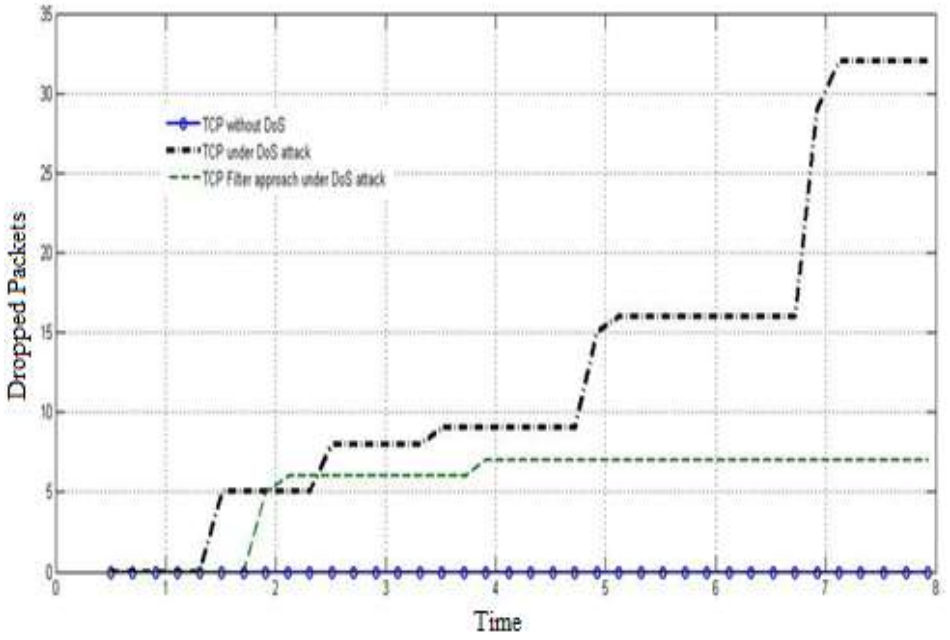

Figure 13. Dropped Packets Comparison – TCP Filtering

Figure 14 and Figure 15 shows the parameters of the throughput, and number of packets, respectively, while the Figure 16 shows the number of packets dropped. From Figures 14, 15 and 16 we can conclude that SCTP connection is less efficient under the DoS attack. However, in case of SYN flooding, SCTP is still effective because of its four-way handshake mechanism.

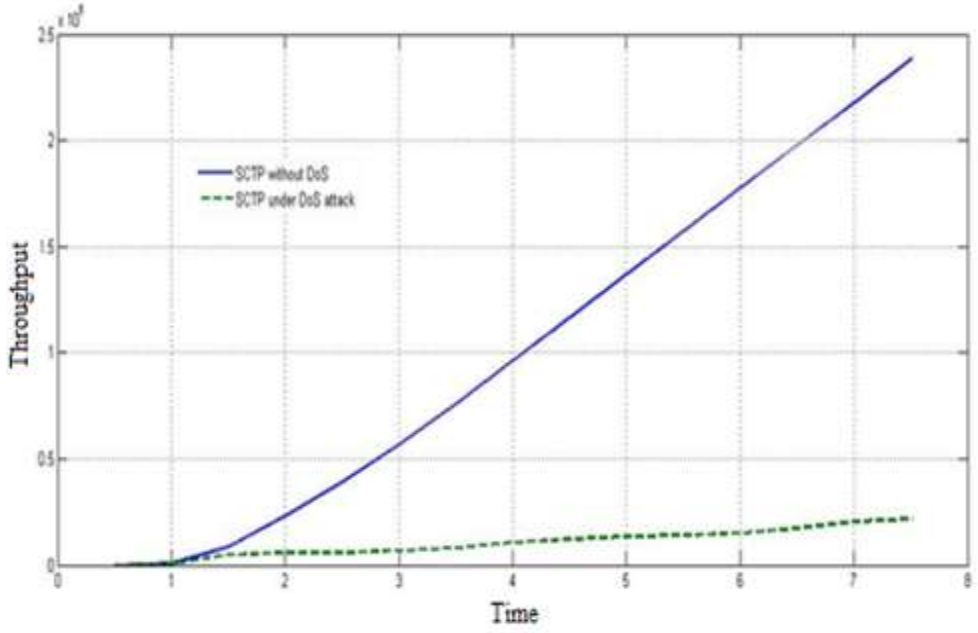

Figure 14. Throughput Comparison - SCTP

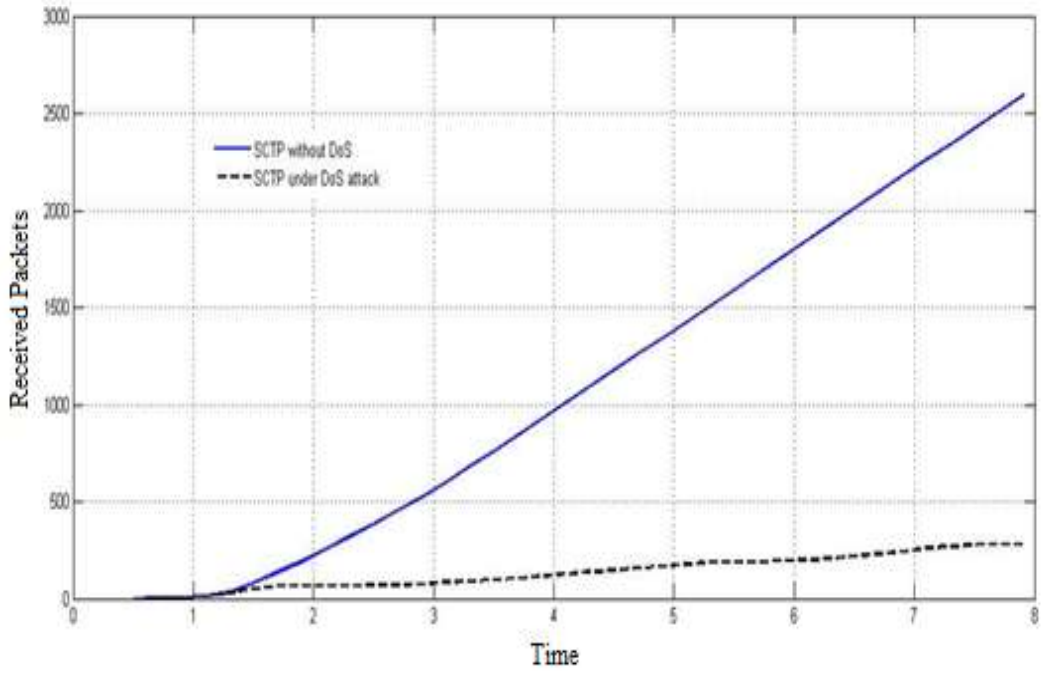

Figure 15. Received Packets Comparison – SCTP

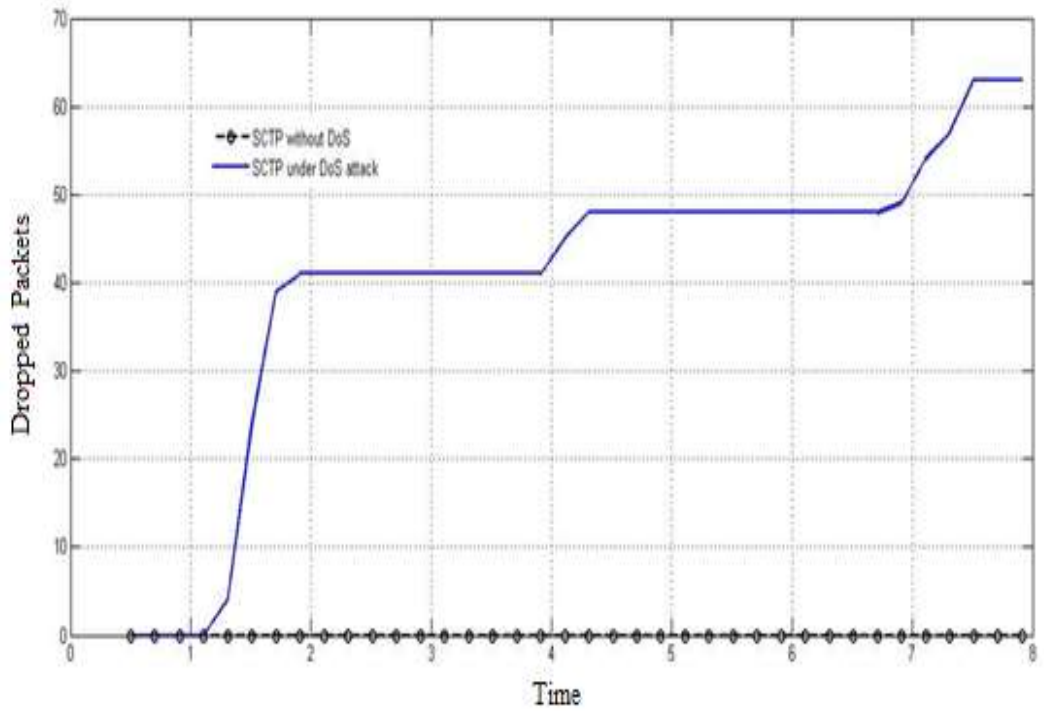

Figure 16. Dropped Packets Comparison – SCTP

The throughput and number of received packets in a multi-homing connection with an active DoS attack is shown in Figures 17 and 18, respectively.

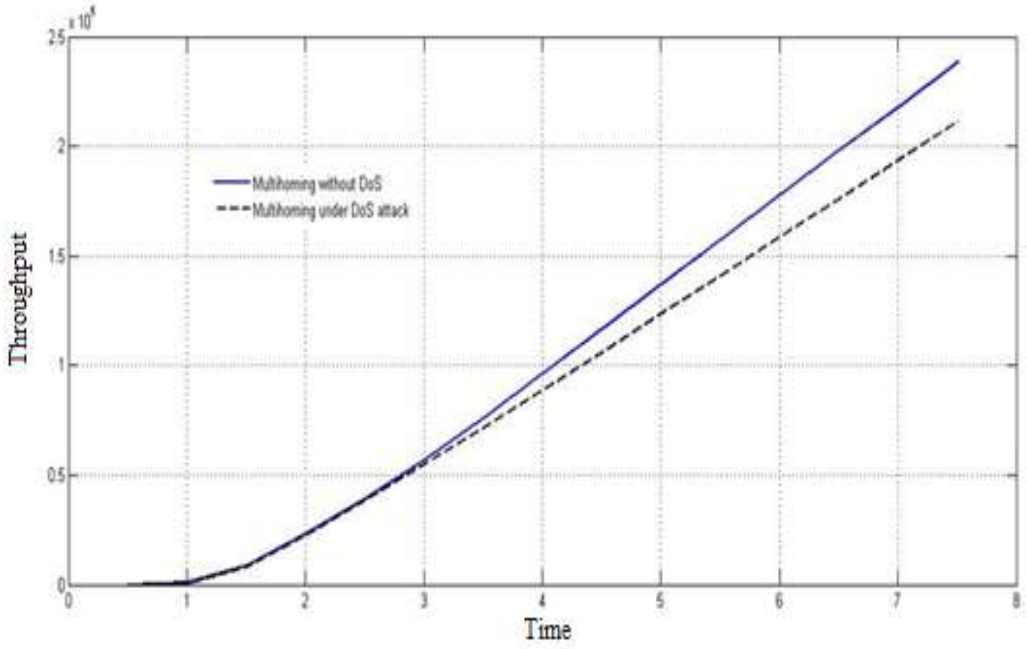

Figure 17. Throughput Comparison – Multi-homing SCTP

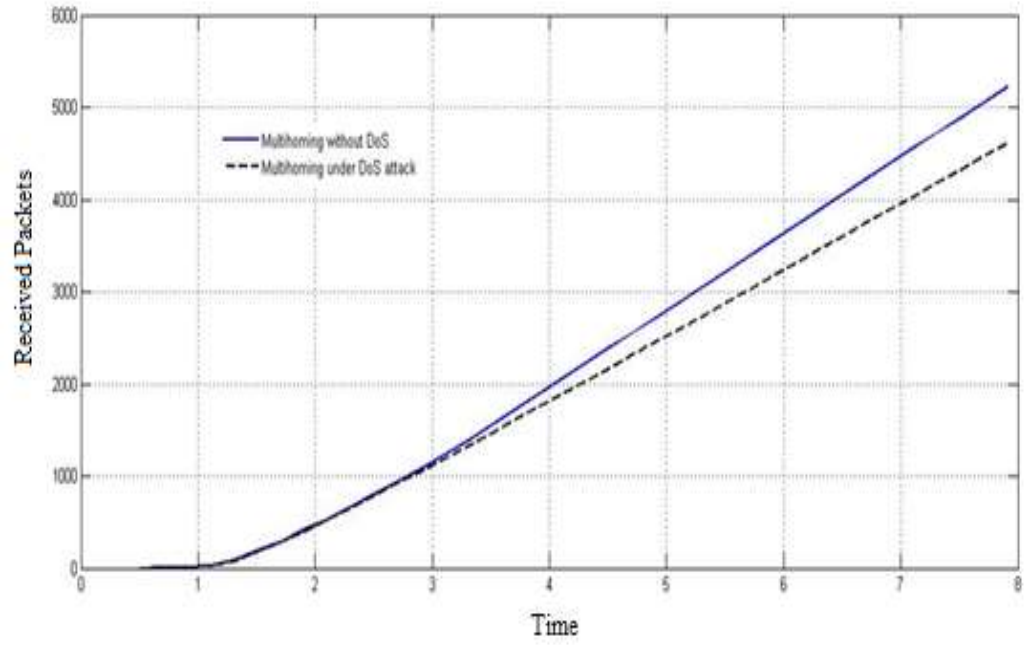

Figure 18. Received Packets Comparison – Multi-homing SCTP

It is observed that there is very less decrease in the throughput rate in the case of DoS attack. Hence, we can conclude that proposed multi-homing is good choice for the DoS attack as it is less affected for the same.

The effectiveness of all the three methods, *i.e.*, TCP filtering, SCTP and multi-homing in terms of throughput and number of packets received and dropped is also compared and shown in Figures 19, 20 and 21, respectively.

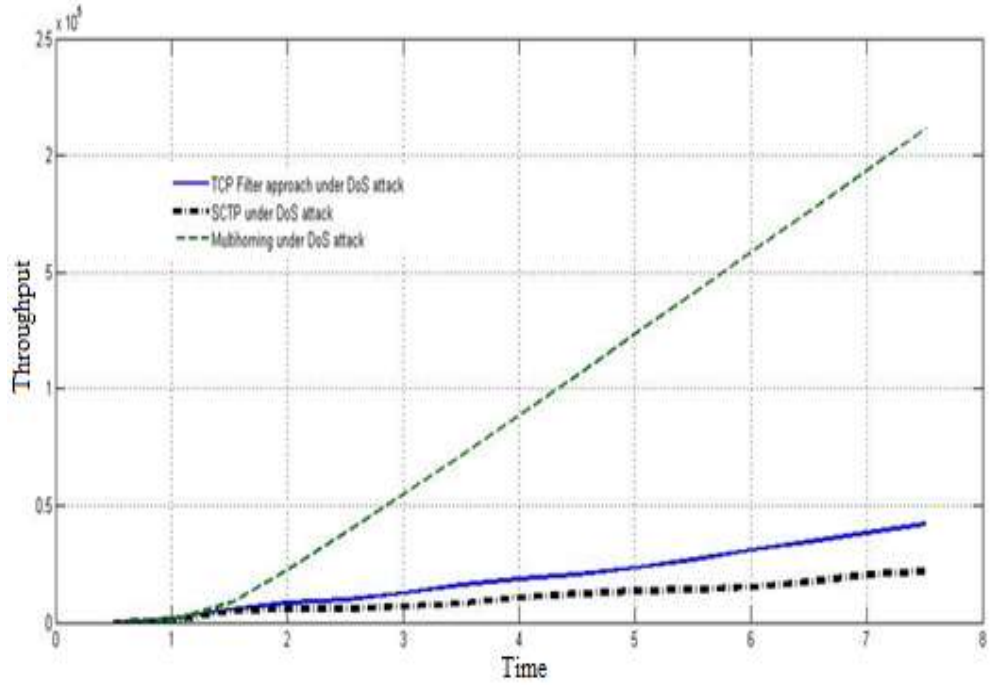

Figure 19. Throughput Comparison of Proposed MH-SCTP vs. SCTP and TCP Filter Approach

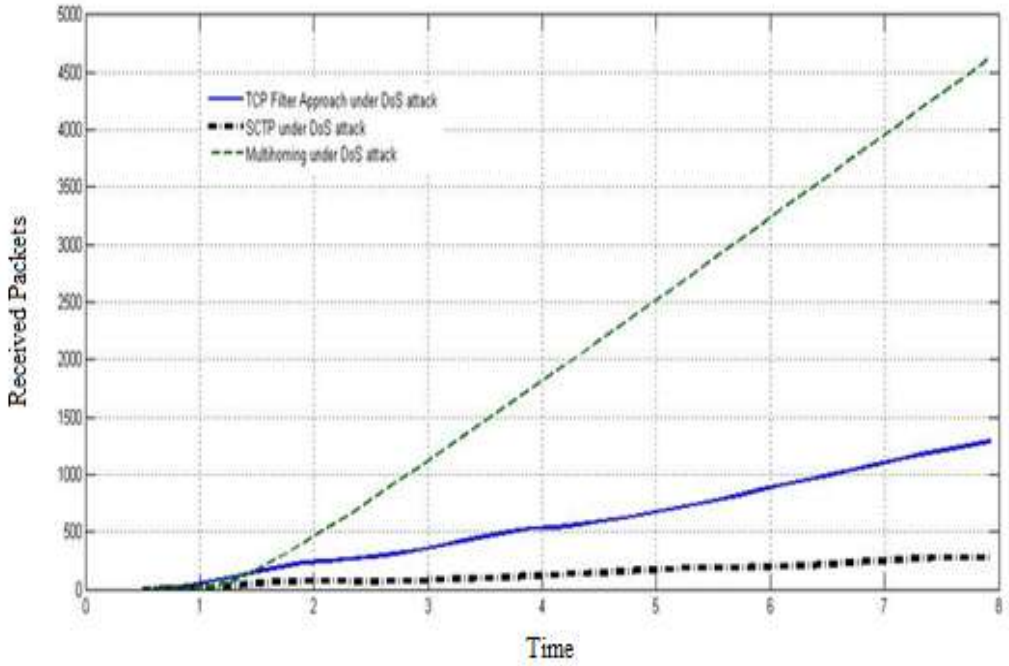

Figure 20. Received Packets Comparison of Proposed MH-SCTP vs. SCTP and TCP Filter Approach

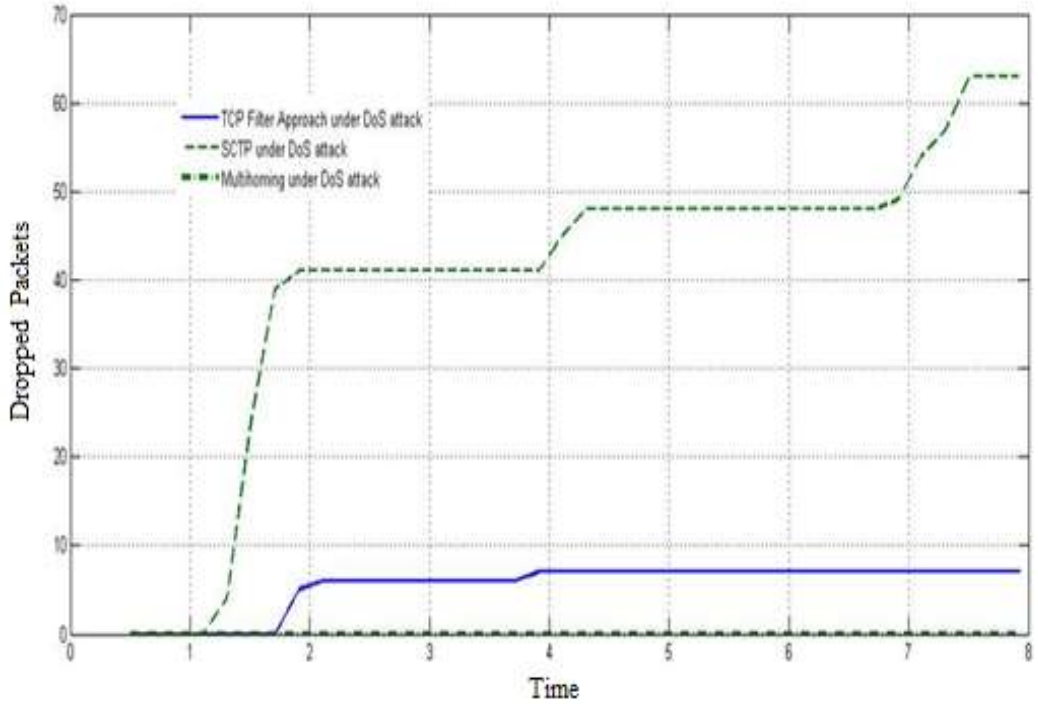

Figure 21. Dropped Packets Comparison of Proposed MH-SCTP vs. SCTP and TCP Filter Approach

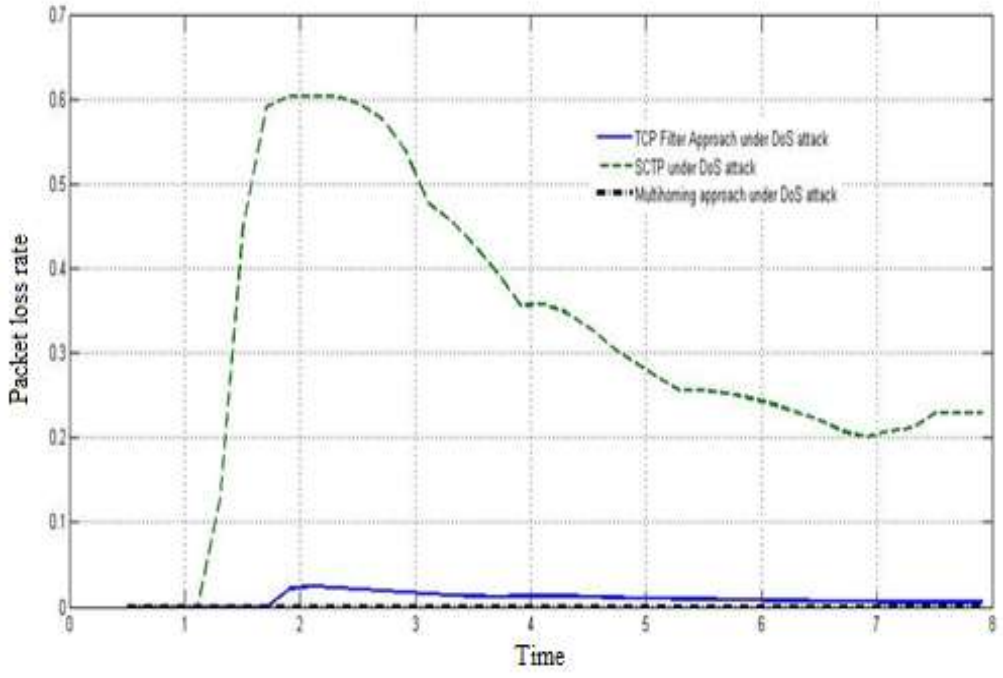

Figure 22. Packet Drop Rate Comparison of Proposed MH-SCTP vs. SCTP and TCP Filter Approach

Figure 22 represents the packet drop rate of the three methods, which is the ratio of number of dropped packets to those received by the node.

Table 1. Throughput Comparison

Time (sec)	Throughput (10^5)		
	TCP Filter	SCTP	MH-SCTP
1	0.03	0.01	0.01
2	0.1	0.07	0.24
3	0.17	0.83	0.53
4	0.23	0.13	0.84
5	0.28	0.15	1.24
6	0.37	0.17	1.57
7	0.43	0.19	1.91

Table 2. Summary of Received Packets

Time (sec)	Received Packets		
	TCP Filter	SCTP	MH-SCTP
1	70	34	35
2	246	78	503
3	384	74	1126
4	512	93	1792
5	732	213	2507
6	915	224	3237
7	1132	276	3976

Table 3. Summary of Dropped Packets

Time (sec)	Dropped Packets		
	TCP Filter	SCTP	MH-SCTP
1	0	0	0
2	6	41	0
3	7	41	0
4	8	43	0
5	8	49	0
6	8	49	0
7	8	51	0

Table 4. Packet Drop Rate

Time (sec)	Packet Drop Rate		
	TCP Filter	SCTP	MH-SCTP
1	0	0	0
2	0.015	0.6	0
3	0.01	0.52	0
4	0.0087	0.36	0
5	0.008	0.286	0
6	0.005	0.24	0
7	.0013	0.201	0

Tables 1, 2, 3 and 4 give the values of parameters in each simulation scenario. Apparent from the above comparison results, MH-SCTP shows better performance and is a better alternate to combat the effects of a DoS attack, while using a filtering method in TCP can also improve the performance of the system to a degree. SCTP, however, does not present a strong case to be used as an alternative to protect against DoS attacks.

6. Conclusion

In this paper, we have discussed the impact of DoS attacks on multiple instances in the healthcare environment and evaluated the behavior of three corrective methods under a DoS attack scenario. The performance analysis of TCP filtering, SCTP and MH-SCTP methods are presented. First, TCP filter approach is a viable option as the first line of defense against DoS attack, rejecting any data packet that deviates away from the normal profile of the expected data. In the next, SCTP

networks provides defense against SYN flooding through their four-way handshake process and works efficiently as a tunnel channel for any heterogeneous networks across the hospital. However, the results obtained from the simulations do not uphold SCTP as a highly effective method to be adopted against a DoS attack. Finally, after studying varied applications of SCTP, we have proposed MH-SCTP, which is most suitable in the case of DoS attack and based on the results presented, it is concluded that MH-SCTP exhibited a better performance in terms of received packets, dropped packets, packet drop rate and achievable throughput under the event of a DoS attack. The suggested work presents a better framework against Denial of Service Open Threat Signaling in Healthcare Environment.

References

[1] P. Yadav, R. Agrawal and K. Kashish, "Heterogeneous Network Access for seamless Data Transmission in Remote Healthcare", International Journal of Grid and Distributed Computing, vol. 11, no. 8, **(2018)**.
[2] H. Elhadj, J. Elias, L. Chaari and L. Kamoun, "Multi-Attribute Decision Making Handover Algorithm for Wireless Body Area Networks", Computer Comm. vol. 81, **(2016)**, pp. 97-108.
[3] Denial of service attack (DoS attack), In Encyclopæ dia Britannica. Retrieved from https://www.britannica.com/topic/denial-of-service-attack, **(2016)**.
[4] International Business Machines, IBM X-Force Research **(2018)** Cyber Security Intelligence Index.
[5] D. J. Nigrin, "When 'Hacktivists' Target Your Hospital", New England journal of medicine., vol. 371, no. 5, **(2014)**, pp. 393-395.
[6] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni, "Analysis of a denial of service attack on TCP", Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, USA, **(1997)** May 4-7.
[7] P. A. Williams and A. J. Woodward, "Cyber security vulnerabilities in medical devices: a complex environment and multifaceted problem", Medical devices, vol. 8, **(2015)**, pp. 305-316.
[8] P. Yadav, R. Agrawal and K. Kashish, "Protocols Performance Investigation using AdHoc WLAN for healthcare Applications", Pertanika Journal of Science and Technology, vol. 26, no. 3, **(2018)**, pp. 1333-1354.
[9] K. L. Hui, S. H. Kim and Q. H. Wang, "Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks", MIS Quarterly, Research Collection School of Information Systems. Available at: https://ink.library.smu.edu.sg/sis_research/3420, vol. 41, no. 2, **(2017)**, pp. 497-523.
[10] M. R Islam, T. K. Koirala and F. Khatun, "Network Traffic Analysis and Packet Sniffing Using UDP", In: Bera R., Sarkar S., Chakraborty S. (eds) Advances in Communication, Devices and Networking. Lecture Notes in Electrical Engineering, Springer, Singapore, vol. 462, **(2018)**.
[11] S. Gavaskar, R. Surendiran and D. E. Ramaraj, "Three counter defense mechanism for TCP SYN flooding attacks", International Journal of Computer Applications, vol. 6, no. 6, **(2010)**, pp. 12-15.
[12] P. Mutaf, "Defending against a Denial-of-Service Attack on TCP", Proceedings of First International Workshop on the Recent Advances in Intrusion Detection, Louvain-la-Neuve, Belgium, **(1998)** September 14-16.
[13] P. Yadav, M. Sehgal, P. Sharma and K. Kashish, "Design of Low-Power EEG-Based Brain–Computer Interface", Singh S., Wen F., Jain M. (eds) Advances in System Optimization and Control. Lecture Notes in Electrical Engineering, Springer, Singapore, vol. 509, **(2018)**.
[14] T. Dreibholz, E. P Rathgeb, I. Rüngeler, R. Seggelmann, M. Tüxen and R. Stewart, "Stream control transmission protocol: Past, current, and future standardization activities", IEEE Communications Magazine, vol. 49, no. 4, **(2011)**, pp. 82-88.
[15] S. Fallon, P. Jacob, Y. Qiao, L. Murphy, E. Fallon and A. Hanley, "SCTP switchover performance issues in WLAN environments", Proceedings of 5th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, **(2008)** January 10-12.
[16] R. Stewart, "Stream control transmission protocol", RFC4960, The Internet Engineering Task Force, https://tools.ietf.org/html/rfc4960, **(2007)**.
[17] H. C. Yu, I. C. Hou and Y. J. Hwang, "The assessment of the mobile nursing cart in hospital adopting", Journal of Studies in health technology and informatics, vol. 146, **(2008)**, pp. 723-723.
[18] J. Kellokoski, J. Koskinen and T. Hämäläinen "Always best connected heterogeneous network concept", Wireless Personal communications, vol. 75, no. 1, **(2014)**, pp. 63-80.
[19] S. Fallon, P. Jacob, Y. Qiao, E. Fallon and A. Hanley, "Enhancing E-learning Application Reliability Through Multi-homing", Proceedings of IADIS Mobile Learning Conference Lisbon, Portugal, **(2007)**, pp. 49-56.
[20] A. Patil and R. Gaikwad, "Comparative Analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network", Journal of Procedia Computer Science, vol. 48, **(2015)**, pp. 387-393.

[21] P. H. Cheng, B. S. Lin, Y, Chu, S. H. Hu and S. J. Chen, "A seamless ubiquitous telehealthcare tunnel", International Journal of Environmental Research and Public Health, vol. 10, no. 10, **(2013)**, pp. 3246-3262.
[22] M. Johnston, H. W. Lee and E. Modiano, "A robust optimization approach to backup network design with random failures", IEEE/ACM Transactions on Networking, vol. 23, no. 4, **(2015)**, pp. 1216-1228.
[23] M. Carbone and, L. Rizzo "Dummynet revisited", ACM SIGCOMM Computer Communication Review, vol. 40, no. 2, **(2010)**, pp. 12-20.
[24] M. Sharif and A. S. Niaraki "Ubiquitous sensor network simulation and emulation environments: A survey", Journal of Network and Computer Applications, vol. 9, **(2017)**, pp. 150-181.

Authors

Piyush Yadav received his graduation and post-graduation in Electronics and Communication Engineering from India. He is pursuing Ph. D. in Electronics Engineering. He is working as Assistant Professor at GLBITM, Greater Noida, India. His major research areas include wireless communication and ICT in healthcare with specific interest in heterogeneous networks.

Rajeev Agrawal received his graduation in Electronics Engineering and post-graduation in Systems Sciences from India. He has done Ph.D. in the area of Wireless communication from Jawaharlal Nehru Univ., New Delhi, India. He is working as Professor and Director at GLBITM, Greater Noida, India. His current areas of research are wireless networks and Ultrasound Medical Imaging.

