International Journal of Information & Network Security (IJINS)
Vol.3, No.6, December 2014, pp. 381~391
ISSN: 2089-3299

An Efficient Dynamic Prevention Technique for TCP/IP DDoS Attacks over MANETs

Mohammed J. Bawatneh*
* Departement of Computer Engineering, AL-QUDS University

Article Info

Article history:

Received Jun 12th, 2014
Revised Aug 20th, 2014
Accepted Aug 26th, 2014

Keyword:

DDoS
Three-Way Handshake
TCP-DCM
TCP-WELCOME
ATCP
DYMO
MANET
TCP-PDCM

ABSTRACT

Distributed Denial of Service (DDoS) attack is one of the most challenging security issues over Wireless Ad Hoc Networks that deprive all legitimate flows from a fair share of bandwidth by overwhelming the buffer space of network resources. The attack process is performed by controlling many of hosts called "zombies" to attack a single victim by planting a zombie program on these machines. With lots of zombie hosts cooperation, the size of an attack can be damaging. The great demand for security, place particular emphasis on the detection and prevention approaches. This paper is focusing on DDoS attack that exploit the weaknesses in Transmission Control Protocol (TCP) over Mobile Ad Hoc networks (MANETs), TCP incorrectly triggers the congestion control mechanism to defend against DDoS attack, which leads to performance degradation.

The simulation results show that our Protected Dynamic end-to-end Congestion avoidance me-chanism used in TCP-PDCM has the best perfor-mance results under DDoS attack of all other TCP variants over MANETs.

Corresponding Author:

Mohammed J. Bawatneh,
Departement of Computer Engineering,
AL-QUDS University,
Jerusalem / Palestine.
Email: mbawatneh@science.alquds.edu:bawatnah@gmail.com

1. INTRODUCTION

Distributed denial of Service (DDoS) attack is one of the major security challenging issues that affect network resources such as network bandwidth and CPU cycles. TCP/IP protocol has numerous weaknesses over Mobile Ad Hoc Networks (MANETs) environment such as incorrectly triggering congestion avoidance technique to handle the DDoS attack. Attacker with malicious objectives can take advantages of these shortcomings to overflow the victim resources with large amount of traffic in order to prevent victim from accessing normal traffic.

The mechanisms used to manage the buffer queue such as DROPTAIL and Random Early Detection (RED) [1] cannot distinguish between legal packets and illegal packets, this makes the detection of DDoS attack a difficult process especially, when attacker use spoofed valid IP addresses.

DDoS attack is divided into two types: bandwidth attack and application attack. In bandwidth attack, attacker consumes the network resources such as: routers and servers, which has limited processing resource, with an immense number of malicious packets, in order to prevent normal users from accessing legal services. In application attack, attacker exploits the shortcomings of protocols such as TCP to overwhelm victim resources and prevent him from normal requests.

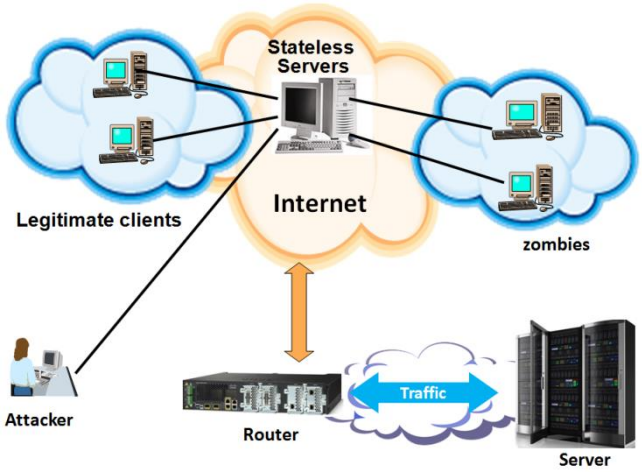

Figure 1. DDoS attack model

Attacker logs on to a stateless server, such as Internet Relay Chat (IRC) [3] that does not store IP addresses and provides anonymous access in order to coordinate attacks, as in Fig.1
The attacker also uses zombies, which are unprotected hosts. Besides, the previous insertion of DDoS tools to zombies allow the attacker to control them remotely by instructions after being activated.
Traditional Intrusion Detection Systems (IDSs) are not designed to solve the problem of DDoS over MANETs due to several reasons related to its nature. In addition to the limitation in mobile node's resources and the Infrastructure-less nature that prevent the exist of centralized node to monitor the traffic, the dynamic topology of nodes in MANETs makes the separation between anomaly and normalcy traffic quite difficult.
This paper organized as follows: section 2. Is about MANETs characteristics and routing protocols. In section 3. I will talk about related works. In section 4, problems of DDoS attack over MANET. Section 5, includes proposed mechanism in TCP-PDCM to decrease the impact of DDoS attack. Section 6, shows an analysis and simulation results. Finally section 7, is the conclusion.

2. Mobile Ad Hoc Networks (MANETs)

Mobile Ad Hoc Network (MANET) is infrastructure-less based wireless network. Therefore there is no centralized control node to handle the transaction between the nodes. MANET is a self organized network [4], in which every node plays the roles of both router and host by sharing its resources such as the link's bandwidth and queue. Besides, nodes in MANET can be heterogeneous and can change their locations, which leads to frequent routing updates in order to cover the connectivity between source and destination. MANET is useful when infrastructure is expensive or not available.
This dynamic environment is essential in a wide variety of applications such as Search And Rescue (SAR) operations, military environments, meeting rooms, taxi cab network, and Personal Area Networking (PAN) applications.

2.1. Security Attacks in MANETs

Security attacks in MANETs are divided into two categories: passive attacks and active attacks. In passive attacks, attacker eavesdrops on the traffic for monitoring purpose or applying further analysis. Although there is no modification is applied to the traffic, this type of attack is difficult to detect. In active attack, a modification of the traffic is occurring. This category is divided into three subcategories: message modification, masquerade and Denial of Service (DoS). Distributed Denial of Service (DDoS) is the scope of this paper. DDoS attacks can be launched from the transport layer as: TCP session hijacking attack, in which spoofed IP address is used, and SYN flooding attack [6], in which an attacker use the structure of the TCP three-way Handshake to start a large number of half opened TCP connections.

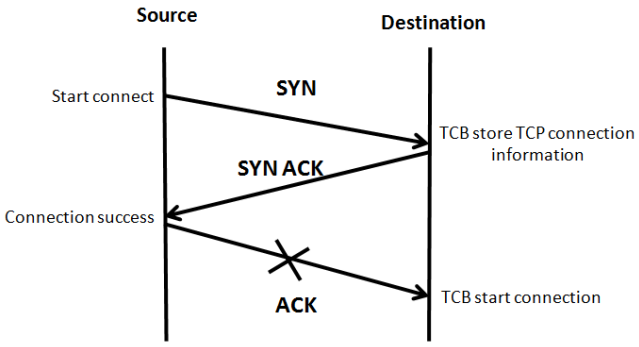

Figure 2. SYN flooding attack in TCP Three way Handshake

Transmission Control Block (TCB) store information about TCP connection as in Fig.2. Although the victim waits the response ACK, the attacker repudiates to send it.

2.1. Routing Protocols in MANETs

Routing protocols in MANETs are divided into three categories: proactive protocols, reactive protocols and hybrid. In proactive protocols, route is maintained periodically even when no need for it, this process causes high overhead. In reactive protocols, source initiate route discovery when needed, this process cause high initial delay and low overhead. Hybrid protocols are a combination of both reactive and proactive protocols.

This paper is focusing on testing the performance of TCP under DDoS attack on Dynamic MANET on Demand routing protocol (DYMO).

2.1.1. Dynamic MANET on Demand routing protocol (DYMO)

Dynamic MANET on Demand routing protocol (DYMO) is a reactive protocol which consists of two operations: route discovery and route maintenance [7]. DYMO is enhanced from AODV or ADOVv2 protocol. The performance metrics such as the overhead and the energy efficiency show that the DYMO protocol is better than AODM protocol for large network size [8]. Besides the DYMO protocol outperforms AODV in performance, it consumes less memory for routing table.

2.2. TCP variants over MANETs

The design of traditional TCP variants does not take into consideration the characteristics of MANET environment. There are several reasons that limit the performance of conventional TCP over MANET such as: frequent link failure, path length (number of hops between source and destination), network portioning, misinterpretation the cause of packet loss and challenges of security issues.

Although several TCP variants are implemented to overcome the technical deficiencies of conventional TCP over MANET [9], each TCP variant has weaknesses and strengths in solving these deficiencies.

This research is focusing on three TCP variants that are implemented to work efficiently over MANET, to determine their performance under DDoS attack. The three protocols are: Ad Hoc TCP (ATCP), TCP-WELCOME, TCP-DCM, and TCP-PDCM.

2.2.2 Ad Hoc TCP (ATCP)

Ad Hoc TCP (ATCP) is an end-to-end approach that uses network layer feedback to monitor the status of network path [12]. ATCP uses Explicit Congestion Notification (ECN) and implement a thin layer between traditional TCP layer and IP layer in order to minimize the required changes to the TCP layer. Sender node has four states as in Fig. 3.

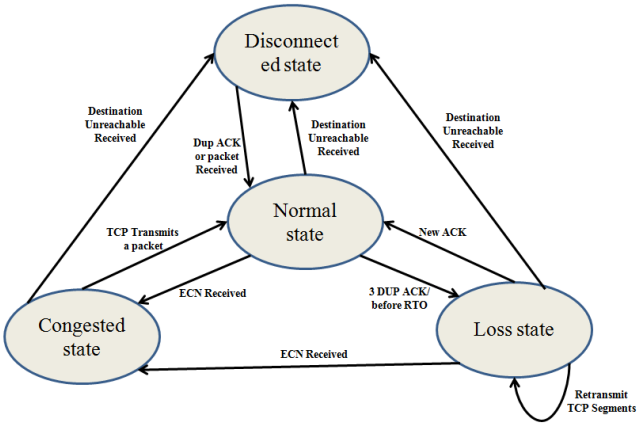

Figure 3. State diagram for ATCP.

Although the dependence on ECN to enter the congestion state in ATCP, this indicator will also determine packet loss due to DDoS attacks as network congestion.

2.2.2 TCP-WELCOME

TCP Wireless Environment, Link losses, and Congestion packet loss ModEls (TCP-WELCOME) [13] is designed to work over MANET environment to increase the throughput and decrease energy consumption in more efficient way based on measured Round Trip Time (RTT), RTO and three duplicated ACK. Traditional TCP variants are not design to handle dynamic topology with large number of link failure. TCP-WELCOME overcomes this problem by performing two operations: Loss Differentiation Algorithm (LDA) and Loss Recovery Algorithm (LRA). LDA is performed first to detect packet loss reason during data transmission as in Fig.4. The causes of packet losses in TCP-WELCOME are divided into three types: network congestion, link failure or wireless channel errors. If the RTT value increases gradually (due to the gradual increase in processing time at congested node's buffer), then packet loss is identified as network congestion as in Fig.4. If RTT remains relatively constant, then the expiration of Retransmission Time Out (RTO) or three duplicate ACK will decide whether the cause of packet loss is due to wireless channel error or due to link failure.

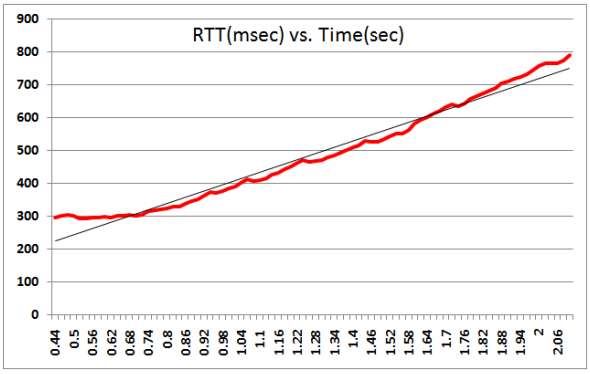

Figure 4. RTT evolution due to network congestion in MANET

RTT is measured as the summation of queuing time q(t), processing time p(t) and propagation P(t) time as in (12):

$$RTT(t) = 2\sum_{i=1}^{n}\left[q_{d,i}(t) + P_{d,i}(t) + p_{d,l}(t)\right] \qquad (1)$$

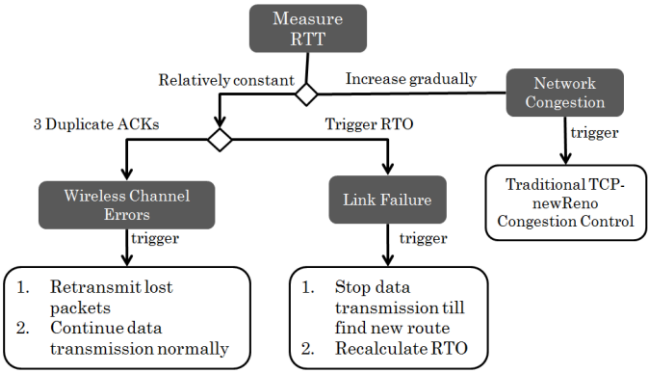

Figure 5. TCP-WELCOME LDA and LRA based on RTT, RTO and 3 duplicated ACK

LRA is performed after LDA to trigger the related recovery algorithm based on packet loss reason. TCP-WELCOME has three loss recovery algorithms which are: network congestion recovery, link failure recovery and wireless channel errors recovery.
TCP-WELCOME Shortcomings,
TCP-WELCOME implements traditional TCP New-Reno congestion technique and does not differentiate between packet loss caused by network congestion and packet loss caused by DDoS attack.

2.2.3 Dynamic End-To-End Congestion Avoidance Protocol (TCP-DCM)

The Dynamic End-To-End Congestion Detection protocol for MANET (TCP-DCM) is an across layer protocol that depends on the feedback from the network layer during the route request to dynamically select the lowest congested end-to-end path from source to destination as in [14].
This protocol performs much efficient than other TCP variants over MANET due to its ability to dynamically change the route path based on values of RTT, RTO and three duplicate ACK.
TCP-DCM performs two steps: first step: during routing at the network layer, destination node chooses three valid paths, if possible, with the lowest cost and sends them to source node inside Route-Reply message. Second step: source node select the major path which have the minimum RTT value and store the remaining minor path(s).
TCP-DCM has the ability to launch the suitable recovery algorithm based on the cause of packet loss as in TCP-WELCOME with much efficient and more dynamic way over MANET.
Packets drop at victim node due to DDoS attack in MANET are difficult to distinguish from packets drop due to network congestion. We will show in section 5, how our Protected dynamic proposed mechanism in TCP-PDCM has the ability to reduce the effect of DDoS attack.

3. Related Work

In this section I will present the recent research in developing mechanisms to detect and prevent DDoS attack that exploits the TCP shortcomings.

Barbhuiya et al. [15] Proposed a mechanism to solve the distributed denial of service attack caused by low rate TCP flows that exploit the shortcomings of TCP. Low rate TCP flows created by DDoS attacker degrade the overall performance of Transmission Control Protocol by overwhelming the resources buffers, this incorrectly treated as congestion. The proposed mechanism verifies the authenticity by randomly reducing bytes from randomly selected TCP segments, this prevent attackers from determining segment size.
Alenezi et al. [16] Proposed a new mechanism to detect DDoS attack that use TCP flooding based. This mechanism depends on monitoring the Congestion Window (CWND) metric, which is an integral part of TCP/IP stack. This metric provides the best estimation to distinguish between both legitimate and illegitimate users. Manipulating the value of this metric by the attacker is difficult. They also propose a new detection metric, the cumulative sum (CUSUM), which differentiates between normal traffic and malicious traffic by comparing the current mean of traffic with the expected mean. If the value of CUSUM exceeds the threshold, then the current traffic is caused by DDoS attack.
Ren et al. [17] classify DDoS attack of multimedia application over MANETs into four categories. . After that they propose defense schemes which includes the detection of RTS/CTS packets, signal interference frequency and retransmission time and response stage.

4. Problem Definition

TCP is a congestion dependent protocol, which use Congestion Window (CWND) to control the amount of traffic between sender and receiver. In order to provide end-to-end congestion control over dynamic environment such as MANETs, adapted TCP variants apply loss differentiation mechanisms to detect causes of packet loss, if packet loss diagnosed as congestion, then TCP updates CWND based on receiving packet's ACK from destination node.

The major shortcoming of available TCP variants over MANETs is the assumption that negligibility in available bandwidth which cause packet drop is due to network congestion, thus triggering congestion mechanism will solve the problem. However, this assumption is completely incorrect, which gives illegitimate attacker, in case of DDoS attack, unfair advantage. On the other hand, the defense mechanisms used in intermediate nodes such as DROPTAIL, Random Early Detection (RED) and Active Queue Management (AQM) have no preferential treatment of both legitimate and illegitimate packets, which leads to overall performance degradation.

In this paper, our proposed dynamic end-to-end congestion avoidance technique used in TCP-PDCM shows the best performance under DDoS attack of all other TCP variants over MANETs.

5. Proposed Mechanism in TCP-PDCM

TCP is not designed to handle security issues over dynamic environment such as MANETs. However, TCP-DCM [12] present a dynamic end-to-end congestion avoiding mechanism that handles congested nodes in a more efficient way. As we mentioned in section 2.2.3, it is difficult to differentiate between the packet drop at congested nodes and packet drop at victim nodes. The mechanism used in the Protected Dynamic end-to-end Congection avoidance TCP for MANETs (TCP-PDCM) not only improve the performance of TCP on network congestion, but also provide a dynamic technique to decrease the impact of DDoS attack over MANET.

In TCP-PDCM each path has a congestion threshold. If the RTT value exceeds the congestion threshold as in equation (2), then source node will check its minor paths after notifying the network layer, to select another path with lower value of RTT.

$$\text{cong\_thresh} = RTT_{\min} * \alpha \qquad (1.7 < \alpha < 1.95) \quad (2)$$

The entire operations of TCP-PDCM during the gradual increase in RTT value is shown in Figure 6.

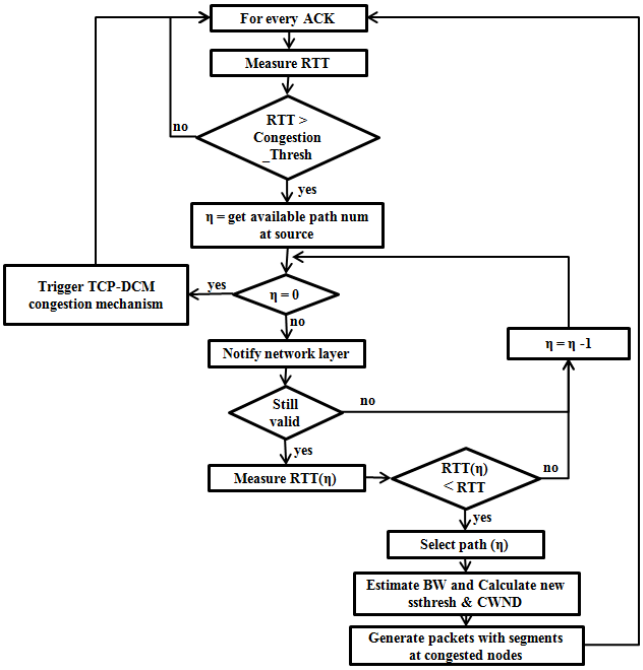

Figure 6. TCP-PDCM dynamic operations while gradual increase in RTT value.

DDoS attack in MANET is different in patterns due to dynamic topology of nodes. However, there are two patterns that success to launch a DDoS attack: self whisper attacking and SYN flooding attacking. In both patterns, attackers create congested nodes near the victim or the victim itself to prevent the legal services.

5.1. Self Whisper Attacking

In self whisper attacking, attacking nodes send packets to each other to increase the number of congested nodes and overhead in the network. TCP-PDCM strength the structure by dynamic avoiding the congested nodes.

In order to explain the mechanism used, suppose three malicious (M1,M2,M3) want to launch a DDoS self whisper attacking pattern by sending packets to another attacker M4 as in Figure 7.

Both M1 and M2 reach M4 with minimum number of congested nodes, in this example, no congested nodes as the following: Path 1: M1-N2-N5-M4 , Path 2: M2-N6-N3-M4. Attacker M3 want also to reach M4, so there are two paths from M3 to M4 which are: path 3.1: M3-N4-N5-M4 and path 3.2: M3-N7-N1-M4. The mechanism used in TCP-PDCM will force the selection of path 3.2 to avoid creating congestion at node N5.

No suppose sender S1 want to communicate with receiver R1. The path: S1-N4-N1-R1 will be selected as shown in Figure 7.

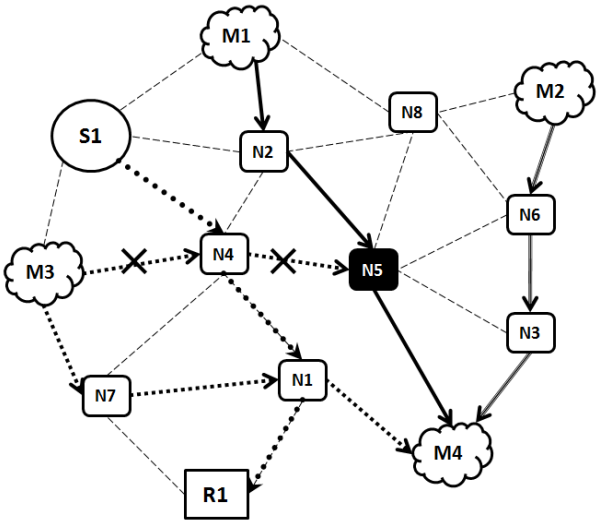

Figure 8. A DDoS self whisper attacking model with legitimate TCP connection between S1 and R1 nodes.

Note that N1 node is not congested node before the connection. As the number of nodes in MANET increase the ability of this mechanism to mitigate the impact of DDoS attack will increase.

5.2. SYN Flooding Attacks

In SYN flooding attacking, attacking nodes send packets to a single victim. In order to mitigate this attacking type of DDoS, Destination node simply ignores the ACK from source node and act as ACK received. In the case of legitimate nodes, duplicated ACK will receive to the Destination node. However, ACK from malicious nodes will not receive. Destination records the number of not received ACKs form each source, if that number exceeds a threshold, then source node will be reported as malicious node. Destination node not only prevents any malicious nodes from any future RouteReply messages, but also sends alarm message to neighbor nodes to do the same.

The pseudo code for TCP-PDCM for preventing SYN flooding DDoS attacks is as follows:

```
ID_NODE_STATUS=unknown
 For each SOURCE_NODE
  If ID_NODE_STATUS not malicious
   If message = request_TCP_ CONNECTION
    Increment NUM_TCP_SOURCE_ID_TRIES
    Send SYN_ACK to source
    Do establish the connection //no wait for source ACK
   END
```

```
 If message = Source ACK
 //source complete normal Three-Way Handshake
    Decrement NUM_TCP_SOURCE_ID_TRIES
     If NUM_TCP_SOURCE_ID_TRIES = 0
       NODE_STATUS = TRUST
     END
   END
   If NUM_TCP_SOURCE_ID_TRIES > TRIES_Thresh
    NODE_STATUS= malicious
    Send one hop Alarm Message to neighbors
    Notify network layer to record SOURCE_ID as malicious
    END
 END
END
```

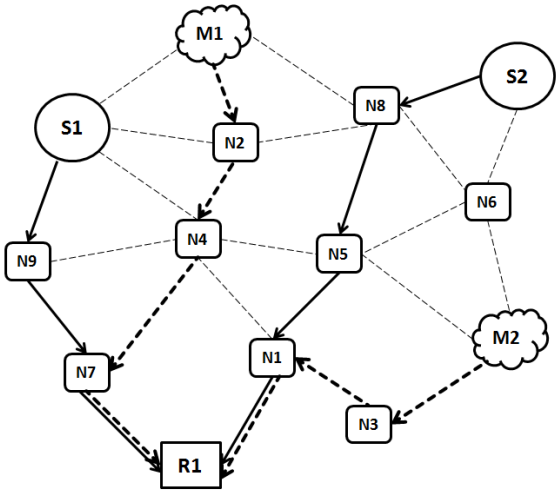

Figure 8. DDoS SYN flooding attacks.

Suppose we have a MANET with two legitimate nodes S1 and S2, and two malicious nodes M1 and M2 as shown in Figure 8.

Both M1 and M2 will start SYN flooding attack to destination R1. Destination R1 acts as ACK received success fully from all sources, therefore no incomplete there-way handshake operations overwhelm the destination's queue. In the case of legitimate sources, a duplicate ACK will receive to destination, this guarantee that source is trusted. However, malicious nodes will not send any ACK to complete the three-way handshake operations. If number of incomplete three-way handshake operations of a certain source exceeds a threshold, then destination node record that source as malicious node and send alarming messages to one hop surrounding nodes.

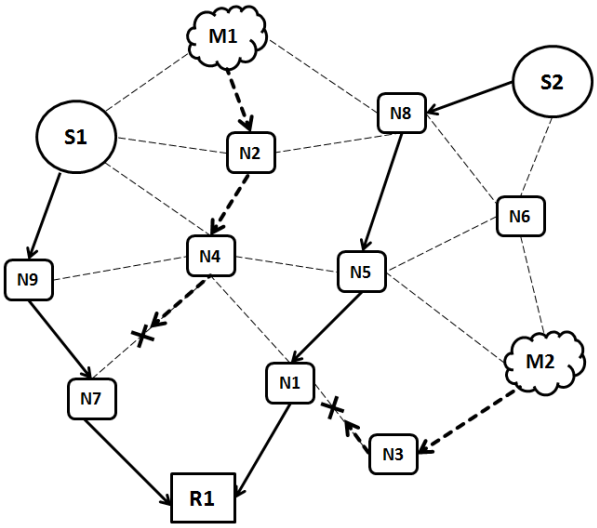

Figure 9. operations of TCP-PDCM to prevent DDoS SYN flooding attack**s.**

All hops that receive the alarming message will not only prevent malicious node from any future RouteReply messages in routing process, but also discard all messages from that malicious node as in figure 9.

6. Validation and Simulation Results

The proposed mechanism was constructed and evaluated in Network Simulator NS 2.34, which is a free discrete event based simulator. NS 2 is written in C++ object oriented language [20]. NS2 also support and provide a free source code for different variants of TCP and different routing protocols over MANET.
In this paper, the size of MANET environment is 1000*1000 with randomly distributed nodes of two types: legitimate nodes and attacking nodes. Legitimate nodes number is 60. The attacking nodes are 4,8,12. We also generate 8 TCP connections between random Legitimate sources and destinations. Interface queue length is 50 packets with type of DROPTAIL for queue management.
The evaluation of DDoS attack is performed in two parts: self whisper attacks and SYN-flooding attacks. Each DDoS attacks pattern is evaluated by the overall average of five scenarios; each scenario has 50 random patterns of different moving directions and random speed ranges in (0-20)m/s. packet size is 1460 bytes.

Table 1. Simulation parameters.

MANET Parameter	Value
Value x	1000
Value y	1000
Simulation time	150s
Speed	(0-20) m/s
Routing protocol	DYMO
Mobility	Random
legitimate Connections	8
Number of nodes	60
Packet size	1460
Data Rate	1 Mbps
Traffic Type	Constant Bit Rate (CBR)
MAC Protocol	Mac/802_11

The results of data processing and analysis is performed by using AWK scripting language as in [19].
In order to validate the performance of TCP variants under DDoS attack, the throughput metric are used which is the number of successful received packets with respect to time as in equation (3).

$$\text{Throuputs(bits/s)} = \frac{\text{ReceivedPackets} * \text{PacketSize} * 8}{\text{TotalPeriod}} \quad (3)$$

6.1. Self Whisper Attacks

In self whisper attacks, varying number of malicious nodes 4,8 and 12 sending packets to each other in order to create congested nodes as much as possible.

Table 2. Average throughput (kbps) for a DDoS self whisper attacking model.

	Number of DDoS attackers			
TCP Protocols	0	4	8	12
ATCP	357.1	293.4	152.5	56.2
WELCOME	405	324.6	178	43.8
DCM	427.9	395.7	298.2	167.5
PDCM	425.1	397.7	302.6	189.8

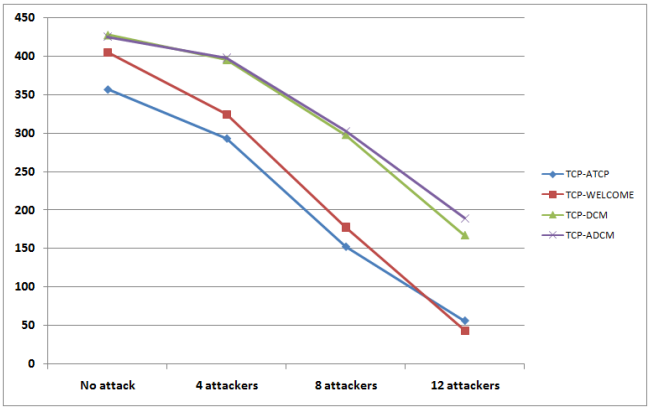

Figure 10. Average throughput (kbps) for a DDoS self whisper attacking model.

Simulation results in Figure 10 show that the performance of both ATCP and TCP-WELCOME degrades under the impact of this type of DDoS attacks. One the other hand, the impact of DDoS attacks on TCP-DCM and TCP-PDCM is mitigated by its dynamic mechanism which avoid creating congested nodes. The overall throughput at legitimate nodes results in TCP-PDCM are better than other TCP variants under self whisper attacks.

6.2. SYN Flooding Attacks

In DDoS SYN-flooding attacks, malicious nodes try to flood the destination node with incompleted three-way handshake attack. The mechanism used in TCP-PDCM mitigates this attack by detecting and preventing malicious nodes from proceeding in the attack.

Table 4. Average throughput (kbps) for a DDoS SYN flooding attacking model.

	Number of DDoS attackers			
TCP Protocols	0	4	8	12
ATCP	357.1	119	45.2	23.9
WELCOME	405	157.3	75.8	64.1
DCM	427.9	179.7	69.3	50.1
PDCM	425.1	398.8	344.6	325.4

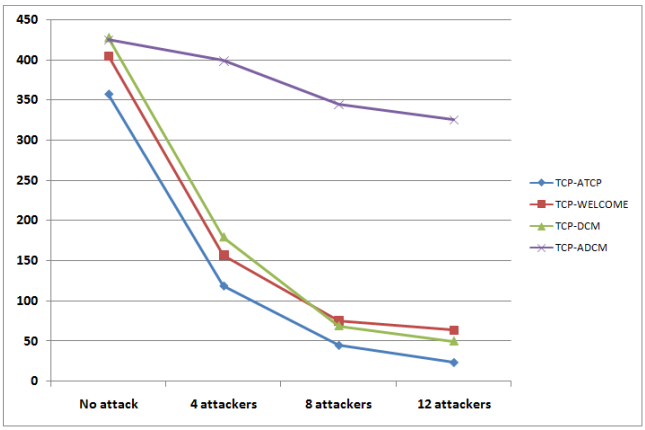

Figure 11. Average throughput (kbps) for a DDoS SYN flooding attacking model.

Simulation results in Figure 11 show that the performance of TCP-PDCM is much better under SYN flooding than other TCP-PDCM variants in the average overall throughput. This is due to the mechanism used in TCP-PDCM that detect the malicious nodes and mitigate their future attack by recording them as malicious nodes.

7. Conclusion

TCP is not originally designed to handle the impact of DDoS attack over MANET environment. Developing an effective and creative solution to minimize the effect of DDoS attack is an important challenge, because the availability of DDoS attacking tools makes it possible to launch an attack.
Simulation results show that TCP-PDCM, has the ability to mitigate the effect of DDoS attacks through its dynamic avoiding end-to-end congestion, which provide flexible and dynamic solution and increase the overall performance over MANET. Other TCP variants show no ability to handle the DDoS attacks.

7. CONCLUSION

TCP is not originally designed to handle the impact of DDoS attack over MANET environment. Developing an effective and creative solution to minimize the effect of DDoS attack is an important challenge, because the availability of DDoS attacking tools makes it possible to launch an attack.

Simulation results show that TCP-PDCM, has the ability to mitigate the effect of DDoS attacks through its dynamic avoiding end-to-end congestion, which provide flexible and dynamic solution and increase the overall performance over MANET. Other TCP variants show no ability to handle the DDoS attacks.

REFERENCES

The main references are international journals and proceedings. All references should be to the most pertinent and up-to-date sources. References are written in Vancouver style. Please use a consistent format for references – see examples below (9 pt):

[1] Haina Hu, Lin Yao, "Improvement for Congestion Control Algorithms under DDoS Attacks", Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference, Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference, 11-13 Dec. 2009, Page(s):1-4.
[2] Kumar, K.D. , Ramya, I. , Masillamani, M.R., "Queue Management in Mobile Adhoc Networks (Manets)", Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom), Hangzhou, 18-20 Dec. 2010.
[3] Esraa Alomari, Selvakumar Manickam, B.B.Gupta , Shankar Karuppayah, Rafeef Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art ", International Journal of Computer Applications (0975 – 8887) Volume 49– No.7, July 2012, Page(s):24-32.
[4] Ismail, D., Johor ; Jaafar, M., "Mobile ad hoc network overview", Applied Electromagnetics, 2007. APACE 2007. Asia-Pacific Conference, Melaka, 4-6 Dec. 2007.
[5] Karthik Pai, Nagesh H.R., Abhijit Bhat, "Detection and Performance Evaluation of DoS/DDoS Attacks using SYN Flooding Attacks", International Conference on Information and Communication Technologies (ICICT- 2014).
[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security, Signals and Communication Technology 2007, pp 103-135.
[7] Anuj K. Gupta, Harsh Sadawarti2 and Anil K. Verma, "IMPLEMENTATION OF DYMO ROUTING PROTOCOL ", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol.1, No.2, May 2013, page(s):49-57.
[8] Sukant Kishoro Bisoyi, Sarita Sahu, "Performance analysis of Dynamic MANET Ondemand (DYMO) Routing protocol", Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010.
[9] Ahmad Al Hanbali, Eitan Altman, Philippe Nain, "A survey of TCP over ad hoc networks", IEEE Communications Surveys & Tutorials, 2005, Page(s): 22-36.
[10] Hao Yang, Haiyun Luo, an Ye ; Songwu Lu, "Security in mobile ad hoc networks: challenges and solutions", Wireless Communications, IEEE (Volume:11 , Issue: 1), Feb 2004, Page(s):38-47.
[11] V.Kaviyarasu, S.Baskaran, "Security in MANET Against DDoS Attack", International Journal of Computer Trends and Technology (IJCTT) – volume 7 number 1– Jan 2014.
[12] Jian Liu and S. Singh, "ATCP: TCP for mobile ad hoc networks", Selected Areas in Communications, IEEE Journal on (Volume:19 , Issue: 7), Jul 2001, Page(s):1300-1315.
[13] Seddik-Ghaleb, Y. Ghamri-Doudane, and S. M. Senouci, "TCP WELCOME TCP Variant for Wireless Environment, Link losses, and Congestion packet loss ModEls," in First International Communication Systems and Networks and Workshops, COMSNETS 2009.
[14] Rushdi A. Hamamreh, Mohammed J. Bawatna, "Protocol for Dynamic Avoiding End-to-End Congestion in MANETs", Journal of Wireless Networking and Communications, Vol. 4 No. 3, 2014, pp. 67-75. doi: 10.5923/j.jwnc.20140403.01.
[15] Barbhuiya, F.A., Gupta, V., Biswas, S., Nandi, S, "Detection and Mitigation of Induced Low Rate TCP-Targeted Denial of Service Attack", Software Security and Reliability (SERE), 2012 IEEE Sixth International Conference, Gaithersburg, MD, 20-22 June 2012, Page(s):291-300.
[16] Mohammed Alenezi and Martin J. Reed, "Denial of Service Detection Through TCP Congestion Window Analysis", World Congress on Internet Security (WorldCIS-2013), Page(s):145-150.
[17] Wei Ren, Hai Jin, Tenghong Liu, "Congestion Targeted Reduction of Quality of Service DDoS Attacking and Defense Scheme in Mobile Ad Hoc Networks", Proceedings of the Seventh IEEE International Symposium on Multimedia (ISM'05), 2-14 Dec. 2005.

[18] Monika Aggarwal, Pankaj Kapoor, "Investigation on DDOS Attacks Over MANET", IJSRD - International Journal for Scientific Research & Development, Vol. 2, Issue 04, 2014, page(s):417-422.
[19] Neeraj Bhargava1, Ritu Bhargava, Anchal Kumawat, Bharat Kumar, "Performance of TCP-Throughput on NS2 by Using Different Simulation Parameters", International Journal of Advanced Computer Research, Volume-2, Number-4, December-2012, Page(s):323-327.
[20] Amey Shevtekar and Nirwan Ansari, "Is It Congestion or a DDoS Attack?", IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 7, JULY 2009,Page(s):546-548.
[1] NS-2 network simulator, URL: http://www.nsnam.org/