Hybrid defense mechanism for DDoS and Flooding attacks in MANET

Mohan K. Mali [1], Pramod A.Jadhav [2]
[1]*M. Tech Scholar*
Dept. Of Information Technology, Bharati Vidyapeeth Deemed University College of Engg. Pune-43

[2]*Assistant Professor*
Dept. Of Information Technology, Bharati Vidyapeeth Deemed University College of Engg. Pune-43

Abstract

MANET is collection of mobile nodes that dyanamically form temprory network and are capable of communicating with each other without use of preexisting network infrastructure.due to open medium, dynamic changing network topology MANETs are vulnerable to many types of security attacks.major form of security attacks on MANET are DDoS attack and flooding attacks. DDoS attack disables normal functionality of network by consuming network resources such as bandwidth, battery power,computational power.Flooding attack consumes bandwidth of network by sending large number of packets to victim node which results in victim unable to provide services to legitimate users. In this paper we introduce adaptive DDoS detection technique for detecting DDoS attack and bandwidth control technique for controlling DDoS attack In this paper we also introduce dynamic counter based broadcast technique for detecting and controlling flooding attack. The results obtained from NS–2 based simulations of proposed technique shows that the techniques can detect and control attacks effectively.

Keywords: ***MANET, DDoS attack, Flooding attack***

1. Introduction

MANETs are multihop wireless network that does not require any preexisting infrastructure. All nodes in MANET acts as host as well as packet forwarding routers.MANETs are mainly used in disaster releif emergencies, military or civil situation where rapid deployment and dyanamic adaptation are required [1] as compared with wired network MANET provides advantages such as mobility,flexibility and no preexisting infrastructure required,but MANETs are more vulnerable to various security attacks.The major security attacks on MANET are DDoS and flooding attack. In DDoS attack available bandwidth is attacked with malicious traffic and then origional traffic restricted to flow which means that bandwidth is hacked .

We experiment with adaptive distance estimation DDoS detection technique for detecting DDoS attack,bandwidth control technique for controlling DDoS attack and dyanamic counter based technique for detecting and controlling flooding attack in network simulator NS-2 [8] . In NS-2 we evaluate them in internet-like network with typical web application traffic.We examine adaptive distance estimation DDoS detection technique in terms of throughput , packet drop rate , end to end delay,packet delievary ratio and we also examine dynamic counter based technique to determine minimum and maximum number of neighbours versus varied netework densities (i.e number of nodes on given terrian size) with different node speeds.

The rest of paper is organised as follows ,The next section discusses various security issues in MANET.Section III provides an overview of DDoS and flooding attacks in MANET.In section IV, we present proposed defence schemes against DDoS and flooding attacks in MANET. In section V, We demonstrates effectiveness of proposed techniques in a number of simulations using NS-2 . Finally, section VI provides summary of paper.

2.Security Issues in MANETs

MANETs are much more vulnerable to attack than wired networks.This is because of the following reasons [1],[2].

Open Medium:- MANET uses wireless media for transimission which introduces security flaws to network. Both active and passive attacks such as impersonation, eavesdropping message redirection and traffic analysis can be performed by an attacker.

Dynamically changing network topology:- Network topology is always changing in Adhoc networks. Therefore any static security mechanism wiil not be applicable in MANET Mobile node comes and goes

from the network, thereby allowing any malicious node to join the network without being detected.

Battery power :- Nodes in MANET have limited battery life,which is expended by packet transmission and reception.Attacker consumes battery power of other nodes present in the network.

Decentralized administration :- Nodes in MANET does not have any central base station to co-ordinate transmission and authentication of packets thus delievery of data packets from source to destination node is depends on co-operation of intermediate nodes in network. Nodes in network have higher probability of being compromised and it is difficult to detect intruding or misbehaving nodes in such mobile decentralized architecture.

Shared broadcast medium :- Wireless channel in MANET is shared broadcast medium unlike wired scenarios whereby channel can be configured to provide dedicated access to any particular user group.therefore,nodes in wireless networks are often subject to interference from neighbouring nodes within transimission and interference range.

3. Security attacks in MANETs

A.DDoS attacks in MANETs

A DDoS attack is a distributed, large-scale attempt by malicious users to flood the victim network with a large number of packets. This consumes the victim network resources such as bandwidth, battery power, computing power, etc, which results in victim is unable to provide services to its legitimate users and network performance is greatly degrades [3],[4]

In DDoS attack, attacker discovers insecure machine connected in network. Discovered machine is infected with attack code then infected machine can further be used to discover and infect another machine in network and so on. The attacker thus gradually prepares an attack network called botnet depending on attacking code compromised machine are called zombies. Attacker sents control instructions to zombies,which in turn sends DDoS attack to victim. DDoS attack basically target victims computational resources such as bandwidth, memory, battery power, computational power etc.

Types of DDoS attack

Flooding attack :- Flooding is a Dinal of Service(DoS) attack that is designed to bring a network or service down by flooding it with large amount of traffic.Flooding attack consumes bandwidth of network by sending large number of packets to victim node which results in victim unable to provide services to legitimate users .

Ping of death attack :- In this type of attack, attacker sends large number of data packets (packet that contains more than 65536 bytes) to victim which results in victim machine to crash [5]

Smurf attack :- In this type of attack, attacker broadcasts ICMP echo request packets with victims IP address as source address and victim will be flooded with large number of ICMP echo reply packets[6].

4. Proposed work

A. Defense scheme against DDoS attack:-

The adaptive distance estimation DDoS detection technique:

The adaptive distance estimation DDoS detection technique used to detect anomalous changes of mean distance values, maximum distance values and minimum distance values based on the exponential smoothing estimation technique [11]. Distance value means number of hops required for packet to reach from source to destination. The distance information of packet can be taken from TTL value of IP header.

The exponential smoothing estimation technique predicts the mean,maximum ,minimum value of distance,mean absolute deviation(MAD),maximum absolute deviation(MaxAD) and minimum absolute deviation (MinAD) value at next time interval.Therefore, we can provide a clear scope for a legal value at the next time interval. Any values which are out of the legal scope can be considered as anomalous.

The MAD-based deviation prediction model defines the scope of normality to detect anomalous changes of the mean distance value.The MaxAD-based deviation prediction model defines the scope of normality to detect anomalous changes of the maximum distance value and The MinAD-based deviation prediction model defines the scope of normality to detect anomalous changes of the minimum distance value.Central to this technique is the computation of the distance

*1) Computing Distance:*The distance has been calculated based on the TTL field of IP header. During transit, each intermediate router deducts one from the TTL value of an IP packet. Therefore, the distance of the packet is the final TTL value subtracted from the initial value. The challenge in distance calculation is how the victim derives the initial TTL value from the final TTL value. Fortunately, most of the operating systems use only a few selected initial TTL values: 30, 32, 60, 64, 128, and 255, according to [17]. Most of the Internet hosts can be reached within 30 hops. Therefore, the initial value can be determined by choosing the smallest initial value of all the possible values which are larger than the final TTL value. For example, if the final TTL value is 100,

the initial TTL value is 128 which are the smallest of 128 and 255.

*2) Estimating Mean Distance:*The detection of anomaly relies on the description of normality and deviation. The exponential smoothing estimation model predicts the mean value of distance d_{t+1} at time t+1 using the following equation.

$$d_{t+1}=d_t + w * (M_t-d_t)$$

Here, d_t is a distance value at time t predicted at time t-1, M_t is the measured distance value at time t, w is a smoothing gain, and $M_t - d_t$ is the error in that prediction at time t.

2.1)Estimating Deviation for Mean Distance: To determine whether the current distance value is abnormal or not, mean absolute deviation (MAD) can be utilized.

$$MAD = 1/n * \sum | e_t |$$

Where, n is the number of all past errors and e_t is the prediction error at time t. However, it is not realistic to maintain all the past errors. Therefore, we use the exponential smoothing technique to calculate MAD based on the approximation equation as defined below.

$$MAD_{t+1} = r * |e_t| + (1 - r) *MAD_t$$

Where, MAD_t is the MAD value at time t. r is smoothing gain.

3)Estimating maximum distance : The exponential smoothing estimation technique is modified to apply on simulation situation based distance calculation affected by various parameters. Exponenetial smoothing estimation model predicts maximum value of distance d_{max+1} at time t+1 using following equation.

$$d_{max+1} = d_{max}+w * (M_t-d_t)$$

Here ,d_{max} is maximum distance value at time t predicted at time t-1.

3.1)Estimating Deviation for maximum distance : To determine whether current distance value of packet is normal or not find maximum absolute deviation (MaxAD) as follows

$$MaxAD = 1/n * \sum | M_{et} |$$

where n is number of all past errors and M_{et} is maximum prediction error at time t, however it is not realistic to maintain all the past error. therefore we use exponential smoothing technique to calculate MaxAD based on approximation equation as defined below :

$$MaxAD_{t+1} = r * |Me_t| + (1 - r) *MaxAD_t$$

where $MaxAD_t$ is MaxAD value at time t and r is smoothing gain.

4)Estimating minimum distance : The exponential smoothing estimation technique is modified to apply on simulation situation based distance calculation affected by various parameters. Exponenetial smoothing estimation model predicts minimum value of distance d_{min+1} at time t+1 using following equation.

$$d_{min+1} = d_{min}+w * (M_t-d_t)$$

Here ,d_{min} is minimum distance value at time t predicted at time t-1.

4.1)Estimating Deviation for minimum distance : To determine whether current distance value of packet is normal or not find minimum absolute deviation (MinAD) as follows

$$MinAD = 1/n * \sum | M_{et} |$$

where n is number of all past errors and M_{et} is minimum prediction error at time t, however it is not realistic to maintain all the past error. therefore we use exponential smoothing technique to calculate MinAD based on approximation equation as defined below :

$$MinAD_{t+1} = r * |Me_t| + (1 - r) *MinAD_t$$

where $MinAD_t$ is MinAD value at time t and r is smoothing gain.

TABLE "SYMBOLS USED IN THE ALGORITHMS"

Parameters	Description
thr	Adjustable threshold parameter
p	Packet
γ	Time interval of detection
Avg	Current average distance value
MaxDist	Current maximum distance value
MinDist	Current minimum distance value
MAD	Current Mean Average Distance value
MaxAD	Current Mean maximum Distance
MinAD	Current Mean minimum Distance
AvgP	Predicted average distance value
MaxP	Predicted maximum distance value
MinP	Predicted minimum distance value
MDP	Predicted MAD value
MaxDP	Predicted MaxAD value
MinDP	Predicted MinAD value

Adaptive distance based DDoS detection algorithm :

After receving packet p ;
If (interval < *γ*)
{ Add d of packet p with old d;
}
Else
{Calculate Avg;
Calculate MaxDist;
Calculate MinDist;
Calculate MAD;
Calculate MaxAD;
Calculate MinAD;
Predict AvgP;
Predict MaxP;
Predict MinP;
Predict MDP;//for average

```
  Predict MaxDP;// for max
  Predict MinDP;// for min
}
If ((Avg >(AvgP + thr* MDP))OR (Avg <(AvgP - thr* MDP)))
{Set anomaly flag;
}
Elseif ((MaxDist >(MaxP + Maxthr* MaxDP))OR (MaxDist <( MaxP -Maxthr* MaxDP)))
{Set anomaly flag;
}
Elseif ((MinDist >(MinP + Minthr* MinDP))OR (MinDist <( MinP -Minthr* MinDP)))
{Set anomaly flag;
}
Else
{Forward packet;
}
```

The Bandwidth control DDoS control technique:

To drop attack packets relatively, a distance-based attack traffic rate limit control will be triggered in the source-end edge network after receiving an alert message from the defense system of the victim-end edge network. The operation of defending against DDoS attack is as follows.

Alert messages between a victim end and a source end includes three types: Request messages, Update messages, and Cancel messages. These messages are used in different phases of defeating a DDoS attack.

Request messages: Once DDoS attack is detected victim provides suggested rate limit value to a source end by sending request message.

Update messages: If attack traffic still increases then victim sends an update message to the source end again. Based on the requirements in the message, the source-end defense system will decrease the rate limit value exponentially. After the traffic at the victim end has returned to normal for a while, an update message sent to the source end asks it to increase the rate limit value linearly.

Cancel messages: Finally, if the defense system has not found any anomalous changes in the victim end since the update message, a cancel message is sent to remove the rate limit at the source end.

Bandwidth control algorithm:

1.On hearing anomaly flag set;
2. Initialization of sending rates of source end routers;
   Ratelimit = (lowerloadlimit + upperloadlimit) / 2;
3 Initialize configurable small constant C;
4 Multicast current rate limit information to source end routers;
5 Monitor current traffic rate at victim end;
6 If currenttrafficvictim >= upperloadlimit Then
   6.1 Set constant as lowerloadlimit;
   6.2 Find difference between current traffic at victim end and constant c;
   6.3 Calculate decrease rate factor by taking quotient factor of small constant c and difference
       calculated in previous steps 6.2.
   6.4 For (each node i at distance d)
      6.4.1 Find drop rate for node i;
      6.4.2 Find rate limit for node i;
   6.5 End for;
7 Else
  7.1 If currenttrafficvictim <= upperloadlimit then
     7.1.1 Find difference between current traffic at victim end and previous traffic at victim
           End;
     7.1.2 If difference calculated in previous step 7.1.1 is less than configurable small constant
          Then 7.1.2.1 remove threshold;
     7.1.3 Else
          7.1.3.1 Keep upperloadlimit value in constant c;
          7.1.3.2 Keep current traffic at victim as previous traffic rate at victim end;
          7.1.3.3 Calculate increase rate factor;
          7.1.3.4 Calculate rate limit for node i;
     7.1.4 End if;
  7.2 Else
     7.2.1 Break;
  7.3 End if;
8 End if;

B. Defense scheme against flooding attack

Dynamic counter based broadcast Technique:

In dynamic counter-based broadcast technique counter c is used to keep track of number of times the broadcast packet is received. If node has already received same broadcast packet more than c times, it will not rebroadcast packet. A counter threshold is decided based on neighboring information. That is in low density area has a different threshold than a medium or high density area, we call them c1, c2 and c3, respectively. Whenever c is greater than or equal to the threshold, then rebroadcast is inhibited. The algorithm works as follows. On hearing a broadcast packet m at node X, the node rebroadcasts the packet according with following conditions:

i) If number of neighbours of node X is less than minimum number of neighbours, n1 then node X has low degree and counter based threshold value is set at c1.

ii) if the number of neighbours of the node X is greater than or equal the minimum number of neighbours, n1 and the number of neighbours of node X are less than or equal to maximum numbers of neighbours, n2 then X

has a medium degree and the counter based threshold value is set at c2 such that c 1< c2.
iii) If the number of neighbours of the node X is greater than maximum number of neighbours, n2 then node x has high degree and counter based threshold value is set at, c3, where c 1< c 2< c3.

Dynamic counter based broadcast Algorithm:

Main broadcast function is to deal with a specific packet and decide to rebroadcast it or not according to neighborhood information
1 On hearing a broadcast packet m at node X
2 Get the Broadcast ID from the packet; n1 Minimum numbers of neighbours and n2maximum Number of neighbours;
3 Get degree n of node X (number of neighbours of node X);
4 **If** n < n1 **then**
4.1 **low density area**
4.2 Node X has a low degree: the low Threshold value (threshold = c1);
5 **Else If** n ≥ n1 **and** n ≤ n2 **then**
5.1 **Medium density area**
5.2 Node X has a medium degree: the Medium threshold value (threshold = c2);
6 **Else If** n> n2 **then**

6.1 **high density area**
6.2 Node X has a high degree: the high Threshold value (threshold = c3);
7 **End if**
8 **counter = 1**
9 **While (not hearing a message) Do**
9.1 Wait for a random number of slots.
9.2 Submit the packet for transmission and wait until the transmission actually start
10 **End while**
11 Increment c
12 **If (c < threshold)**
12.1 Goto step 9
13 **Else**
13.1 exit algorithm
14 **End if**
End

5. Simulation and results

In this section we study performance of network when it's subject to DDoS and flooding attack. We use NS-2 simulator [8] to evaluate proposed techniques. NS-2 is widely recognized packet level discrete event simulator. It's implemented in C++ to support fast and relatively large scale simulations. The common parameters that we have used in our simulation are given in table 2.

Table2. "Summary of the parameters used in the simulation experiments".

Parameters	**value**
Transmitter range	250 meters
Topology size	600m × 600m, 800m × 800m and
Number of nodes	10,20,40,60,80,100,120
Maximum speed	2 and 20 m/s
Bandwidth	2Mbps
Hello' packet size	12 bytes
Routing protocol	AODV[11]
Antenna model	Omni antenna
Radio Propagation	Propagation /two ray ground
Interface queue	Drop tail/priqueue

A. Simulation implementation and evaluation for DDoS attack

The performance of our proposed scheme against DDoS attack is analyzed in MANET with and without defense scheme.To evaluate performance of our proposed techniques following performance matrices are used.

Throughput: - Throughput is the number of packets transmitted per unit time

Packet drop rate: - Packet drop rate is ratio number of packets dropped to the total number of packets sent.

End to End delay: - End to End delay is the delay experienced by a packet from the time it was sent by the source till the time it was received at the destination.

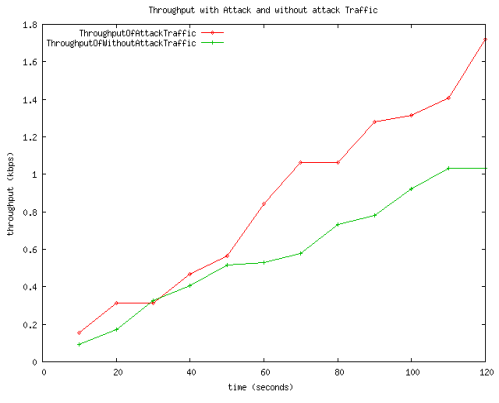

Figure 1." Throughput with and without attack traffic versus time"

As shown in Figure 1 at the initial stage there is minar difference between throughtput of attack traffic and legitimate traffic but as time increases and attck coes in

picture then our proposed approach works on attack and filters traffic using bandwidth control mechnism and hence attack traffic throughput increses.

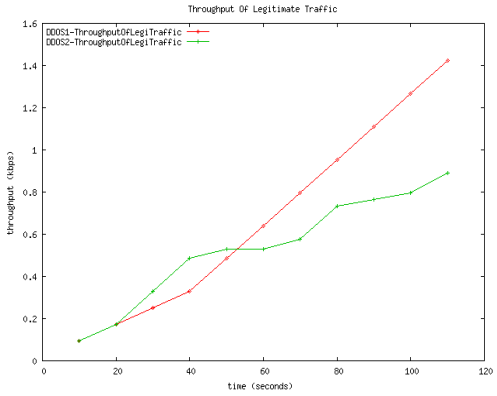

Figure 2. "Throughput of legitimate traffic versus time"

Figure 2 shows in existing system throughtput of legitimate traffic is consistently increses where as throughtput of legitimate traffic in proposed approach is decreses because of various control mechnisms applied at source and destination end.

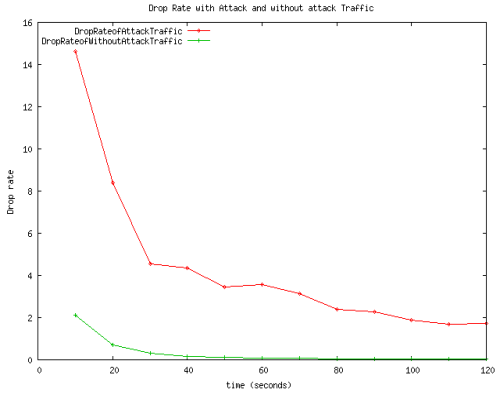

Figure 3. "Drop Rate with and without attack traffic versus time"

Figure 3 Shows the Packet Drop Rate with and without attack traffic versus time, it indicates at initial stage more percentage of attack traffic is delivered to destination but when time increases then proposed approach works on traffic and drop rate slowely decreases and drop rate without attack traffic given cinsistency with minar changes.

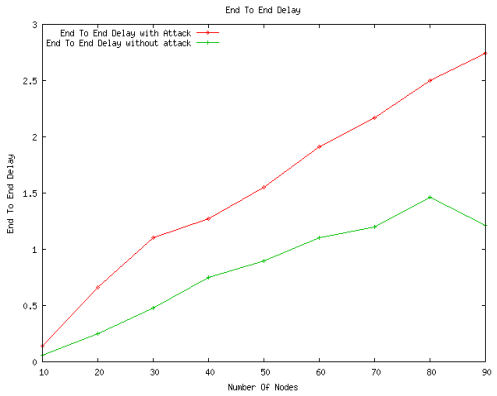

Figure 4. "Impact of End to End Delay versus Number of Nodes"

Figure 4 shows Impact of End to End Delay Versus Number of Nodes, it indicates when attack traffic comes in existance it altimatly affects on delivery time of traffic at destination causing delay hence end to end delay increases with attack traffic. The difference between end to end delay with and without attack traffic is increases as simulation time increases.

B.Simulation implementation and evaluation for flooding attack

We have different the network density (i.e the number of nodes on a given terrain size) and have measured the minimum and maximum number of neighbours over the whole nodes in the network. For a given number of nodes, three terrain sizes have been considered: 600m × 600m, 800m ×800m and 1000m ×1000m.

Figures 5 and 6 shows the minimum and maximum number of neighbours after averaging over the whole network nodes when the nodes move at the maximum speed of 2m/s. Various network densities resulting from a combination of different network sizes (from 20 to 120 nodes) and terrain sizes (600m×600m, 800m×800m,and 1000m×1000m) have been examined. **A summary of the minimum and maximum number of neighbours is listed in Table ?.** The results show that as expected the high density area is, the higher the maximum number of neighbours is at a given node and the low density area is, the lower is the minimum number of neighbours at a given node. As the network size increases so does the minimum and maximum number of neighbours. For example, in a terrain size of 1000m × 1000m when the network size is 50 nodes, a typical node has the minimum number of neighbours equals to 4, the maximum number of neighbor to 17. When the network size is doubled to 100 nodes, a typical node has the

minimum number of neighbour's equals to 7, the maximum number of neighbour to 34.
Figures 7 and 8 provides further results on the minimum and maximum number of neighbours
(averaged over the whole network) after repeating the above simulation experiments where the node speed is set at 20 m/s.

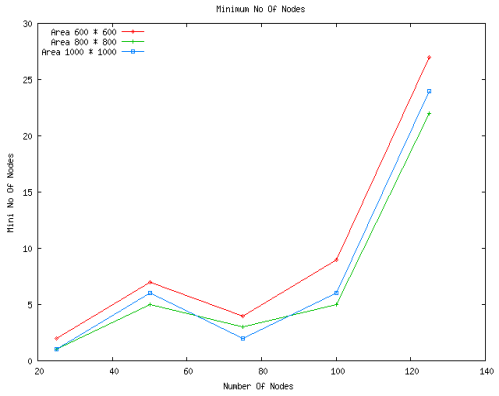

Figure 5. "Minimum number of neighbours vs. network size with a node speed of 2 m/s"

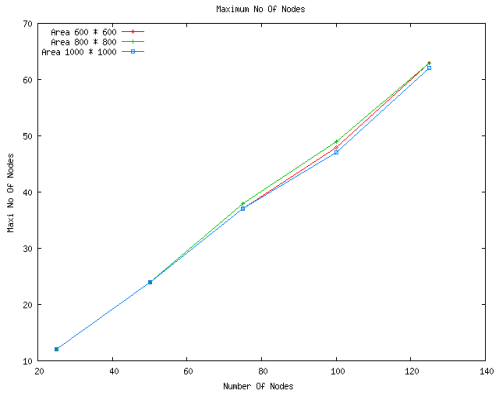

Figure 6. "Maximum number of neighbours vs. network size with a node speed of 2 m/s"

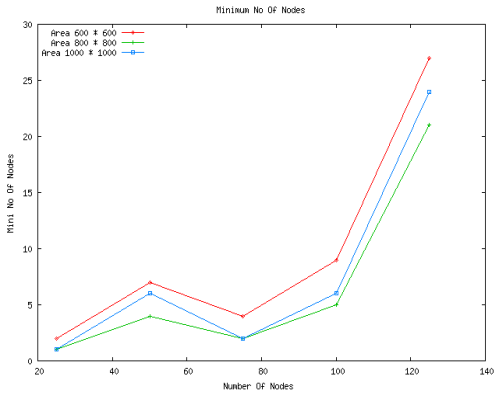

Figure 7. " Minimum number of neighbours vs. network size with a node speed of 20 m/s"

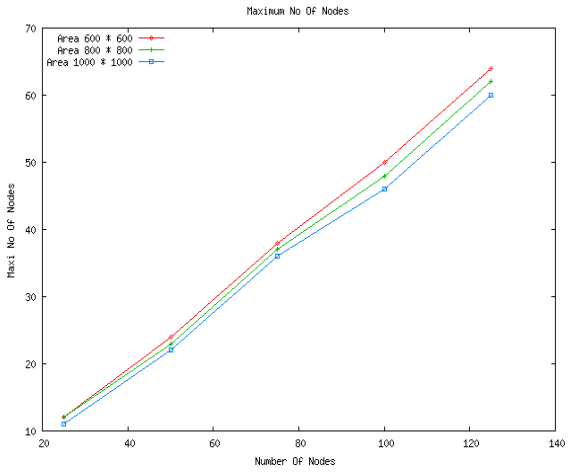

Figure 8. "Maximum number of neighbours vs. network size with a node speed of 20 m/s"

6. Conclusions

As the use of MANETs increases, the security is becomes critical issue. In this paper, we have discussed the various security issues and security attacks in MANET and proposed a defense schemes against DDoS and flooding attacks in MANET. We have also simulated some DDoS attacks in MANET, with and without defense schemes and understand the effects of such attacks on performance of network.
In this paper, we have also shown minimum and maximum number of neighbours for given node using dynamic counter based broadcast technique. It's concluded that among all network attacks, DDoS and flooding attacks are most harmful threats to network functionality and MANETs are even more vulnerable to those attacks.

7. References

[1] Hwee-Xian Tan,Winston K.G.Seah "Framework for statistical filtering against DDoS attacks in MANET."Proceddings of second international conference on embedded software and systems,2005.
[2] Nishu Garg, R.P.Mahapatra. "MANET Security Issues". IJCSNS.International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.
[3](2000)CERT.[Online].Available:http://www.cert.org/advisories/CA-2000-01.html
[4] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state of the art," Computer Journal of Networks, vol. 44, no. 5,pp. 643-666, Apr.2004.
[5] Wang H.,Zhang D. and Shin K."Detecting syn flooding attacks,in IEEE infocom".

[6]Maha Abdelhaq,Sami Serhan,Rred Alsqour and Rosilah Hassan(2011) IEEE sponsored international conference on Electrical Engifneering and informatics.
[7 VINT Project U. C. Berkeley/LBNL, "NS2: network simulator," Available at http://www.isi.edu/nsnam/ns, 2006
[8] K. Fall and K. Varadhan. The ns manual, the VINT project. http://www.isi.edu/nsnam/ns/ns-man.html.
[9] C-K. Toh. Ad hoc mobile wireless networks, protocols and systems, Prentice-Hall, New York,2002.
[10] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-service attack detection techniques," IEEE Internet Computing, vol. 10, no. 1, January 2006, pp. 82–89.
[11] Yonghua You; Zulkernine, M. ; Haque, A. Detecting Flooding-Based DDoS Attacks. IEEE International Conference on Communications 2007,ICC 07. June 2007, Page(s): 1229-1234
[12] Y. Kim, J.-Y. Jo, and K. K. Suh, "Baseline profile stability for network anomaly detection," in Proceedings of the 3rd International Conference On Information Technology: New Generations, 2006, pp. 720–725.
[13] J. Jung, A. Berger, and H. Balakrishnan, "Modeling TTL-based internet caches," in Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, pp. 417–426.
14[14] T. Gil and M. Poleto, "Multops: a data-structure for bandwidth attack detection," in Proceedings of 10th Usenix Security Symposium, 2001, pp.23–38.
[15] J. Jiang and S. Papavassiliou, "Detecting network attacks in the internet via statistical network traffic normality prediction," Journal of Network and System Management, vol. 12, no. 1, 2004, pp. 51–72.
[16] S. Lee, H. Kim, J. Na, and J. Jang, "Abnormal traffic detection and its implementation," Advanced Communication Technology, vol. 1, February 2005, pp. 246–250.
[17] The Swiss Education and Research Network,"Default TTL values in TCP/IP,"Available at http://secfr.nerim.net/docs/fingerprint/en/ttldefault.html, 2002.