Available Online at www.ijecse.org ISSN- 2277-1956

Efficient Techniques to Detect the Various Attacks in Ad-Hoc Network

Rakesh Kumar Sahu [1] , Dr. Narendra S. Chaudhari [2]
[12] *Department of Computer Science & Engineering*
[12] *Indian Institute of Technology, Indore, India*
[1] *Email- rakeshsahubl@yahoo.co.in*
[2] *Email- nsc183@gmail.com*

Abstract- This paper is mainly focused on Denial of Service (DoS) attack, where a server or a node cannot give service to the other nodes as it is under an attack. There are various attacks in the Ad hoc network but our paper is mainly focused on two types of DoS attacks viz SYN-Flooding and Worm-Hole attacks. How we can detect any one of attacks is addressed in this paper. We have discussed the CPU and memory utilization during the attack. We have given two separate algorithms for each attack and also suggest how to get rid of this type of attacks .

Keywords – SYN-Flooding Attack, Warm-hole Attack, TCP/IP, Denial of Service (DoS).

I. Introduction

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of nodes, which are client terminals (individual user PCs) and one or more servers. The clients are connected to these servers. They are linked by communication systems, some of which might be private, such as within a company means these may be open to public access. And the moment it opens to public the network security issue arises. And network security is a complicated subject because every day new challenges are being faced by researchers and looking their solution to make network intact and least vulnerable. Some of these attacks may be active attacks like Denial of Service attack (DoS) [1]. In this category of attack one attack is SYN-Flooding attack, where a node(s) become disrupt and cannot serve to any other node of the network. All bandwidth and disk space consume by the attacker node. This attack exploits the TCP vulnerability of the network [2]. The other kind of DoS attack is Black-Hole attack.The Black-hole attack is one of the burning issues to be addressed efficiently. The Black-hole attack is one of the attacks in Ad hoc network mainly for proactive and reactive routing protocols such as AntNet, AntHocNet and ARA. The efficiency, throughput reliability etc. of the network is depended on the various parameters of the network. These parameters have to be observed during the network operational. The values of these experimental parameters are based on the different weaknesses in some feature of a system that makes a threat possible. The attack may be mounted if the system is weak at any point of view. But the case is not exactly fit over here as Black-hole attack is not weakness of the system. It is due to the disloyalty of a node which makes the node malicious within the network. These malicious nodes can carry out both Passive and Active attacks against the network. In passive attacks a malicious node only eavesdrop upon packet contents, while in active attacks it may imitate, drop or modify legitimate packets. A typical example of particularly devastating security active attack is known as a wormhole attack. In which, a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. This active attack can affect network routing, data aggregation and clustering protocols, and location-based security systems. Finally, the active attack can be launched even without having access to any cryptographic keys of the Ad hoc network. We are giving below different types of possible attacks in the Ad hoc network their assumptions, protocols and philosophy.

Table I. Summary of different proposed solution

Proposal name	Approach	Assumption	Philosophy
Dynamic learning system using DPRAODV [5]	DPRAODV	Multiple black hole	Single nonblack hole node detects
Cooperative black hole node detection using DRI and cross checking [6]	AODV	Cooperative black hole	Single nonblack hole node detects
Black hole node detection using two different solutions [7]	AODV	Multiple Back hole nodes	Single as well as multiple non-Black hole detection
Distributed and cooperative mechanism [8]	AODV	Distributed and cooperative	Cooperative detection
Detecting Black hole Attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection [9]	AODV	multiple Black hole nodes	Single non-Black hole detects
Single black hole node detection [10]	AODV	Single Black hole	Single non Black hole detects
Prevention of Black hole Attack using fidelity table [11]	Enhancement of AODV	Multiple Black hole	Multiple non Black hole detects
Detection of black hole using DRI and Cross checking [12]	Modified version of AODV	Multiple Black hole	Multiple non Black hole detects

II. Proposed Algorithm

A. Detection of SYN-Flooding Attack –

The model is based on the network traffic analysis by different tools available in linux based system. We have taken some data from the real network after the SYN Flooding attack is mounted.

There some systematic approach applied :

- ◦ Port Scanning.
- ◦ Identification of Ports (eg. Vulnerable Ports).
- ◦ Mount Syn-Flooding.
- ◦ Run Tool.
- ◦ Collect Data.
- ◦ Analysis of Data.

For analysis of data we have employed the following algorithm (figure 1.) as well as we used some tools which are described in figure 3 and figure 4.

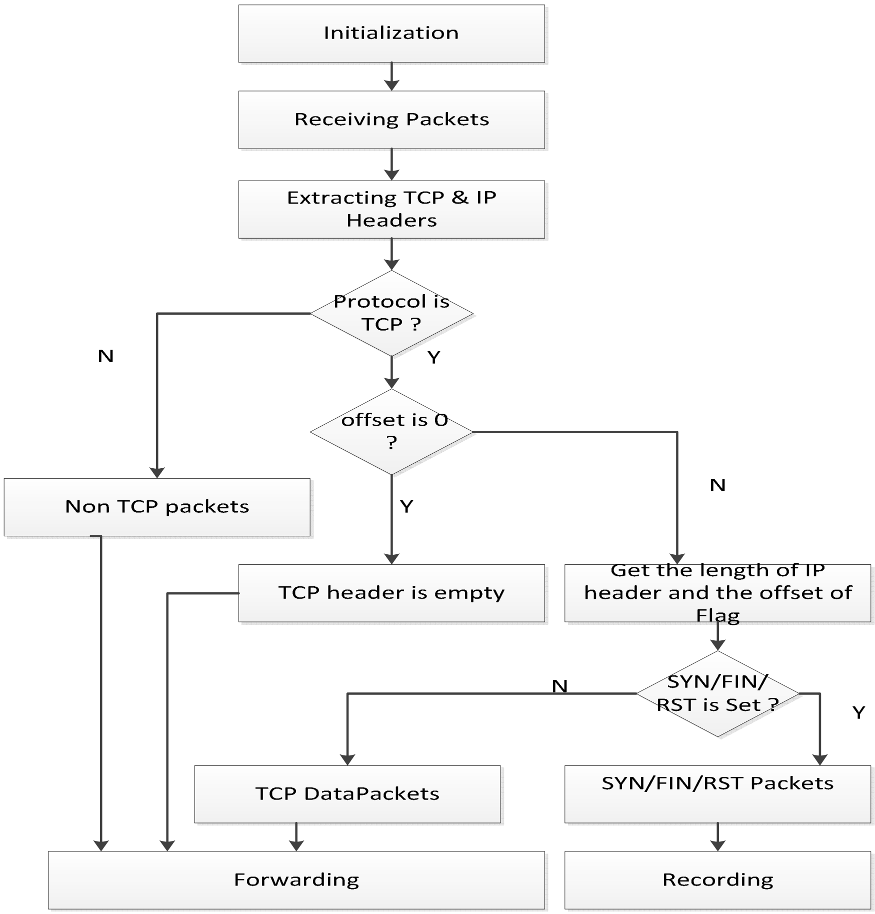


Figure1. Shows how TCP packets are identified and analyzed.

B. Detection of Warm-Hole Attack

There are several simple techniques to detect an warm-hole attack in a network [3]. But We have applied this technique which is based on promiscuous mode.

Monitoring Neighbours

In this security model, nodes go into promiscuous mode immediately after sending a packet to their neighbour. They monitor to check if the neighbour is transmitting it to the intended sender or dropping it. This can be found by istening to the packet header of the retransmission. If the destination is not transmitting to the intended destination or if the packet is simply dropped, then the source counts this as a drop. Hence every node in the network keeps track of the number of packets that are sent and dropped for each of its neighbours. This information is stored periodically for different intervals. For each neighbour, a node monitors the number of packets dropped *Dp* and packets sent *Sp* to it in that interval. I – 1, I – 2, I – 3, etc., are various intervals for which the observations are made.

With the trust information available through neighbour monitoring, it is simple to detect the wormhole. The algorithm for detection of Wormhole is run during the routing phase. The procedure for wormhole detection is described by means of a flowchart given in Figure. 2.

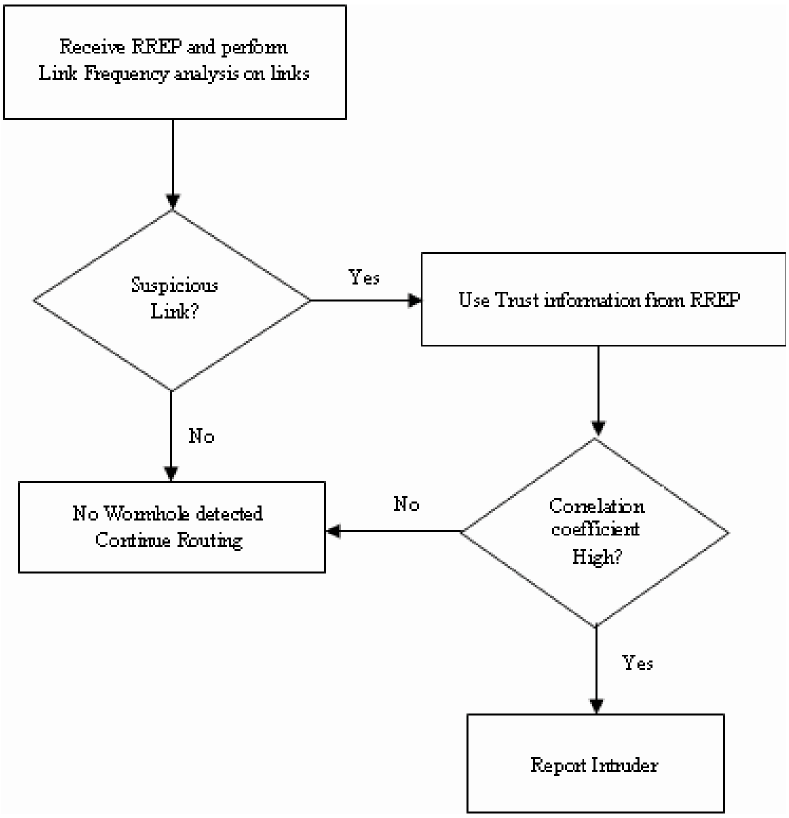
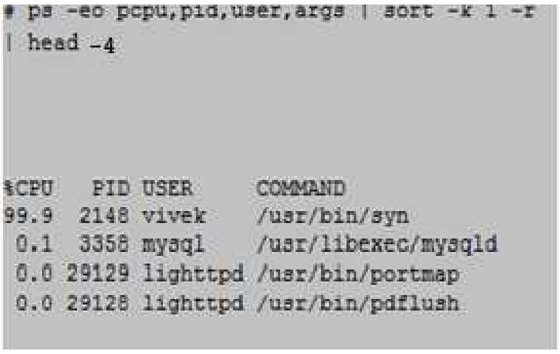

Receive RREP and perform Link Frequency analysis on links
Suspicious Link?
Yes
Use Trust information from RREP
No
No Wormhole detected Continue Routing
No
Correlation coefficient High?
Yes
Report Intruder

Figure 2. Algorithm for detecting the Warm-Hole attack

III. Experiment and Result

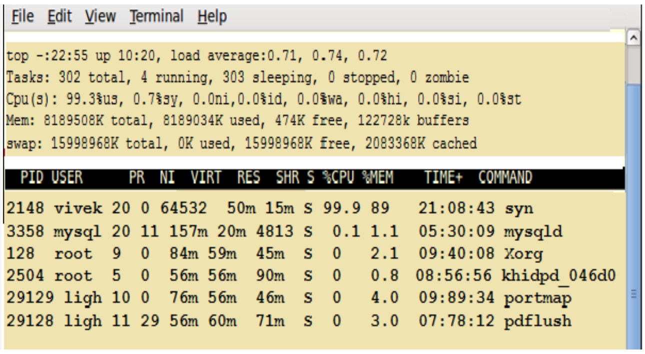
A. *Experiments & Result for SYN-Flooding Attack –*

We have carried out some experiments to evaluate the performance of the network using some tools like ps, iostat, netstat, vmstat etc [8] [14]. We need to know which process is monopolizing the CPUs utilization, which is identified by the following combination of commands as:



```
# ps -eo pcpu,pid,user,args | sort -k 1 -r
| head -4

%CPU   PID USER     COMMAND
99.9  2148 vivek    /usr/bin/syn
 0.1  3358 mysql    /usr/libexec/mysqld
 0.0 29129 lighttpd /usr/bin/portmap
 0.0 29128 lighttpd /usr/bin/pdflush
```



```
top -:22:55 up 10:20, load average:0.71, 0.74, 0.72
Tasks: 302 total, 4 running, 303 sleeping, 0 stopped, 0 zombie
Cpu(s): 99.3%us, 0.7%sy, 0.0ni,0.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 8189508K total, 8189034K used, 474K free, 122728k buffers
swap: 15998968K total, 0K used, 15998968K free, 2083368K cached

 PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
2148 vivek 20 0 64532  50m 15m s 99.9 89   21:08:43 syn
3358 mysql 20 11 157m 20m 4813 s  0.1 1.1  05:30:09 mysqld
128  root  9  0  84m 59m  45m  s  0   2.1  09:40:08 Xorg
2504 root  5  0  56m 56m  90m  s  0   0.8 08:56:56 khidpd_046d0
29129 ligh 10 0  76m 56m  46m  s  0   4.0  09:89:34 portmap
29128 ligh 11 29 56m 60m  71m  s  0   3.0  07:78:12 pdflush
```

Figure 3. : output of ps command

Figure 4. : Output of top command

As shown in figure 3, tool runs on each machine, it gives the network information shows in figure 4, says that SYN process (SYN Flooding attack) is consuming the almost all CPU bandwidth (99.9%) and make feel other processes in hanged condition. This Monopolizing process is known and who is executing this process is identified called attacker node, and the node which is showing this data is the victim machine.

The server node is busy in responding the SYN/ACK packet to the sender machine and other processes get very less CPU time. The CPU utilization can be seen in graphical representation in figure 5. The size of these packets has been verified by using tcpdump tool and find out that the each packet is of similar in all kinds. It also give strengthen in our verification of attack. Likewise we also apply the iostat, netstat & vmstat tools to counter verification of SYN Flooding attack. Some of the results we have tried to show in the following figures and graphs.

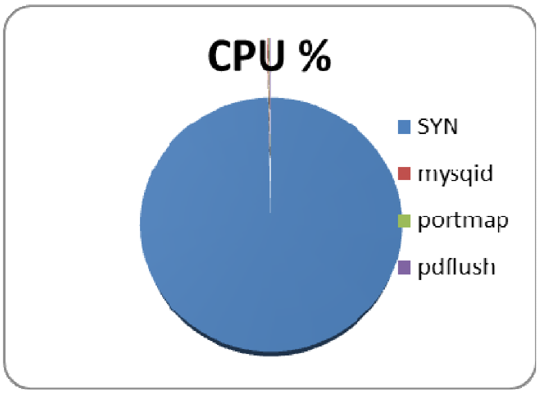


Figure 5. : Shows CPU% utilized by each process

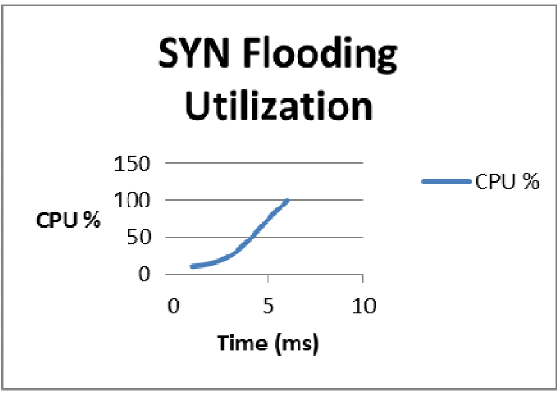


Figure 6. : Shows CPU utilization with time scale

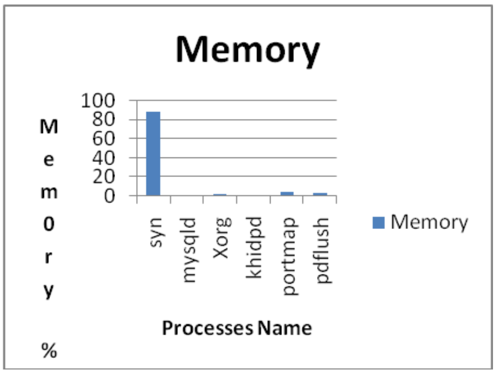


Figure 7. : Shows memory occupied by each process

B. Experiments & Result for Warm-Hole Attack

The performance of DaW was evaluated against existing method of link frequency analysis.. We have implemented both Link Frequency analysis and DaW on DSR routing protocol. Nodes monitor their neighbor by going into promiscuous mode. Each interval spans over a period of 20 seconds and at any time a maximum of 5 intervals are observed and are used for trust evaluation. The size of the interval and the number of intervals observed both are variables and can be changed based on the available resources.

Precision of Alarms

The results of the simulations in terms of the total number of alarms raised and the genuine alarms out of them are tabulated. The precision is defined as follows:

Precision of alarms= (Number of alarms for worm holes/Total number of alarms)%

The total number of alarms might include apart from genuine wormhole [4]. The precision is decided by the proportion of genuine wormholes detected. Based on the simulations, the graph of Precision of Alarms versus the number of nodes is plotted in Figure 8.

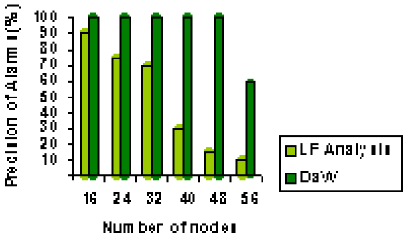


Figure 8. : Precision f Alarms

IV.CONCLUSION

This paper is basically focused on detection of two types of denial of service attacks Syn-Flooding and Warm-hole attack. Under the Syn-Flooding attack in the network we found that how memory and CPU utilization are abruptly increased. It is clearly depicted that approximately 99% CPU utilization is acquired by this attack. And the memory utilization is also considerable. Therefore Syn-flooding badly affects the memory and CPU utilization of the victim node and other nodes could not get any chance to connect with this victimized node. In the second analysis (for warm-hole attack) for the detection of the warm-hole attack we have proposed monitoring neighbours technique which is very efficient technique. We have also addressed various types of attacks their occurrence in protocol, philosophy etc. for the Ad-hoc network

V. REFERENCE

[1] Stevens, and W. Richard, “TCP/IP illustrated, Vol(1),” Machinery Industry, pp. 174-190, 2005.

[2] Juniper Networks, “Denial of service and attack protection,” white paper, Juniper Networks 2006.

[3] Y.-C. Hu, A. Perrig, D. B. Johnson, “Wormhole Attacks in Wireless Networks” Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.

[4] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, in *proceedings of INFOCOM*, 2004.

[5] Payal N. Raj and Prashant B. Swadas, “DPRAODV: A dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[6] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks,” International Conference (ICWN’03), Las Vegas, Nevada, USA, 2003, pp 570-575.

[7] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjjin Park, “Black Hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference, 2004, pp 96-97.

[8] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, PAKDD 2007 International Workshop, May 2007, Nanjing, China, pp 538–549.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, “Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security, Volume 5, Number 3, 2007, pp 338–346.

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[11] Latha Tamilselvan and V Sankaranarayanan, “Prevention of Black hole Attack in MANET”, Journal of networks,Volume 3, Number 5, 2008, pp 13-20.

[12] Bo Sun Yong, Guan Jian Chen and Udo W. Pooch,“Detecting Black-hole Attack in Mobile Ad Hoc Networks”, The Institution of Electrical Engineers (IEE) ,Volume 5, Number 6, 2003, pp 490-495.