ISSN:0975-9646
Shekhar Tandan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1513-1516

A PDRR based detection technique for blackhole attack in MANET

Shekhar Tandan and Praneet Saurabh

Computer Science and Engineering Dept., RGPV Bhopal, Gyan Ganga College of Technology, Jabalpur

***Abstract*— An Ad hoc network is the network with no fixed infrastructure. There is no central administrator so any node can come and move in and outside of the network in a dynamic manner. This makes it more dynamic and complex which makes it more prone to attacks. They can attack either active or passive. Some effects of malicious nodes are Denial of service, Routing table overflow, Impersonation, Energy consumption, Information disclosure etc.**

A blackhole attack node attracts all packets by falsely claiming a fresh route to the destination node and absorbs them without forwarding them to destination.

In this paper a mechanism based on PDRR is proposed to detect the blackhole attack in MANET with AODV protocol. An introduction of blackhole in MANET with QUALNET 5.0 is done, after applying the detection technique result reflects the performance degradation.

This paper is intended for audience having prior knowledge about network routing protocols and its related quantitative performance metrics.

***Keywords*— Ad hoc Network, Blackhole Attack, AODV, QualNet 5.0, Detection Technique.**

INTRODUCTION

Ad hoc network has no predefined structure and no any fixed topology. All nodes can move freely in network. There is no any centralized control to control transmission and movement of nodes. All the nodes in network participate in network management task, Hence network management is done in distributed manner. Each node in the network works both as router and host. As all nodes are movable so this changes topology of the network dynamically, which brings more challenges in security of Ad hoc network

BLACK HOLE ATTACK

A black hole node that attracts all the packets by falsely claiming that it has valid route to destination node. [8]

It disturbs the routing protocol by deceiving other nodes about the routing information. A black hole node works in the following scheme: once receiving RREQ messages, the attacker replies RREP messages directly and claims that it is the destination node or had valid route to destination node. Under these circumstances, the source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message.

AODV(AD HOC ON-DEMAND DISTANCE VECTOR)

AODV is reactive protocol Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network.

When a route to a new destination is needed, the node broadcasts a RREQ to find a route to the destination. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator. A route can be determined when the RREQ reaches a node that offers reach ability to the destination (e.g., the destination itself).

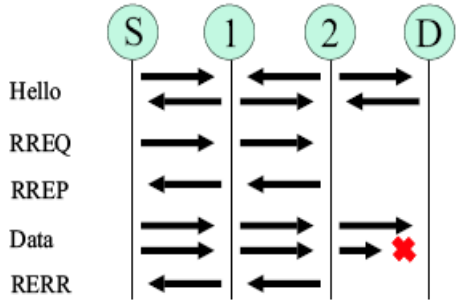

Figure 1: AODV Protocol Messaging

The route is made available by unicasting a RREP back to the origination of the RREQ. For nodes monitoring the link status of next hops for active routes, when a link break in an active route is detected, the broken link is invalidated and a RERR message is typically transmitted to notify other nodes that the loss of that link has occurred. The RERR message indicates the destination that is no longer reachable by way of the broken link.

RELATED WORKS

Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Ali[1] discuss about the existing MANET Routing Protocols in paper author highlight the important routing matrices required in evaluating the performance of the protocol in terms of reliability and efficiency. In paper they discuss some of the factor which affects the routing algorithm like such as variable wireless link quality, propagation path loss, fading; multi-user interference, power expended and topological changes become important issues. In paper discuss about the proactive DSDV, WRP, CGSR, reactive SSR, AODV, RDMAR, Hybrid routing Protocol like, ZRP.

Jiwen CAI,Ping YI,Ye TIAN,Yongkai ZOHU,Ning LIU [8] has proposed & simulated some of the attacks for DSR protocol using NS2.

Ioannis Broustis Gentian Jakllari Thomas Repantis Mart Molle[2] discuss the performance of routing protocols for large scale mobile adhoc network larger throughput lower end to end delay fewer lost data packet. They perform the simulation on DSR, TORA, AODV, LAR in the paper discuss result derived from extended simulation and compare the efficiency of the above four protocols using NS-2 and Qualnet.

Satoshi Kurosawa, Hidehisa Nakayama[3] has been analyzed the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. After analysis he prospsed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

Md. Anisur Rahman, Md. Shohidul Islam[4] compared the performance of two prominent on-demand reactive routing protocols for mobile ad hoc networks: DSR and AODV, along with the traditional proactive DSDV protocol. A simulation model with MAC and physical layer models have been used to study interlayer interactions and their performance implications. The On-demand protocols, AODV and DSR perform better than the table-driven DSDV protocol.

Lidong Zhou[5] studied the threats an ad hoc network faces and the security goals to be achieved. After that he identified the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication.

Rajan Shankaran, Vijay Varadharajan, Michael Hitchens [6] presented a scheme for providing security services for routing of control messages in an ad-hoc network. Our focus is on on-demand routing protocols for ad-hoc networks, specifically the Dynamic Source Routing Protocol.

PROPOSED WORK & METHODOLOGY

In this paper an implementation of black hole in wireless network is presented and the analysis is performed using AODV protocol with variation in pause time and speed of node with a simulator QualNet 5.0. The performance metric is packet drop ratio (PDRR). After analysis of result effect of black hole attack in network is observed and also analysed how detection technique helps to detect them.

All simulation has been performed with QualNet 5.0[7] simulator.

SIMULATION ENVIRONMENT

In this paper work all the simulation work is performed in Qualnet wireless network simulator version 5.0. The movement proceeds for a specific amount of time or distance, and the process is repeated a predetermined number of times. We choose Min speed = 10 m/s, Max speed = 50m/s, and pause time = 10s to 50s.

All the simulation work was carried out using TCP variants (Reno, Lite, Tahoe) with DSR routing protocol .Network traffic is provided by using File Transfer Protocol (FTP) application. File Transfer Protocol (FTP) represents the File Transfer Protocol server and client.

Wireless network which we have used have following values for different parameter:

Mobility model Random Way Point
Minimum speed 0 mps
Maximum speed 10 mps, 20 mps, 30mps, 40 mps, and 50 mps
Pause time 10s, 20s, 30s, 40s, 50s.
Simulation Time 200s

Terrain
Coordination 1500 * 1500 m

Connection
FTP (File transfer protocol): 41 (client) to 1 (server)
Item size 512(byte)

Radio/physical layer parameters:
Radio type: 802.11b Radio
Data rate: 2Mbps
Packet reception model: Bit error rate (bpsk.ber)

MAC Protocol: 802.11
Routing Protocol: AODV
Transport Protocol: TCP
Node: 50
Node Placement: Random
Seed: 1

DETECTION TECHNIQUE AND ALGORITHM

This work proposes a technique works on a parameter Packet Drop Ratio (PDRR).It calculates PDRR also verifies it.

Threshold detection technique compares calculated packet drop ratio (PDRR) against a Threshold value. Threshold value is a maximum packet drop ratio value without blackhole attack. Under the normal case i.e. without attack Packet Drop Ratio (PDRR) must always be less or equals to threshold value. Under attack case packet drop ratio will be more than the threshold value. Thus algorithm compares calculated packet drop ratio with a pre specified threshold .

Algorithm for Detection of Blackhole attack

Step1:[Calculate packet delivery ratio (PDR) for all the experiments.]
PDR←pktrv/100.0;
Step2:[Computation of Packet Drop Ratio(PDRR)]
PDRR←1-PDR;
Step3:[Maximum PDRR value for AODV without blackhole attack is chosen as a threshold.(here 0.05)]
THRESHOLD←MAXIMUM(PDRR without attack)
Step4: [Check PDR of current simulation if less than threshold then system is free from attack. Otherwize there is blackhole attack.]

```
if ( PDRR > THRESHOLD ) then
    Message("System is under Blachole Attack");
otherwise
    Message("System is free from Attack");
```

RESULT ANALYSIS AFTER APPLYING DETECTION ALGORITHM

After applying the detection technique the following results obtained shown in table for both the cases
i) variation in pause time, and ii) variation in node speed.

TABLE I
VARIATION IN PAUSE TIME

Pause Time (Sec.)	With Blackhole		Without Blackhole	
	PDR (%)	PDRR (%)	PDR (%)	PDRR (%)
10	0.85	0.15	0.96	0.04
20	0.86	0.14	0.95	0.05
30	0.86	0.14	0.99	0.01
40	0.79	0.21	0.98	0.02
50	0.78	0.22	0.98	0.02

TABLE III
VARIATION IN NODE SPEED

Pause Time (Sec.)	With Blackhole		Without Blackhole	
	PDR (%)	PDRR (%)	PDR (%)	PDRR (%)
10	0.87	0.13	0.98	0.02
20	0.89	0.11	0.99	0.01
30	0.86	0.14	0.98	0.02
40	0.77	0.23	0.98	0.02
50	0.84	0.16	0.99	0.01

A) ANALYSIS OF PDRR FOR AODV WITH BLACKHOLE ATTACK AND WITHOUT ATTACK WITH VARIATION IN PAUSE TIME

After analyzing fig.2 it is observed that for AODV without attack PDRR is initially 4% for pause time 10, It is maximum 5% for pause time 20. PDRR is lowest for pause time 30 and for remaining pause time it is 2%.
For AODV with attack PDRR is initially 15% for pause time 10, It is 14% for pause time 20 and 30. For other pause time it is increasing. Packet drop is maximum for pause time 50.

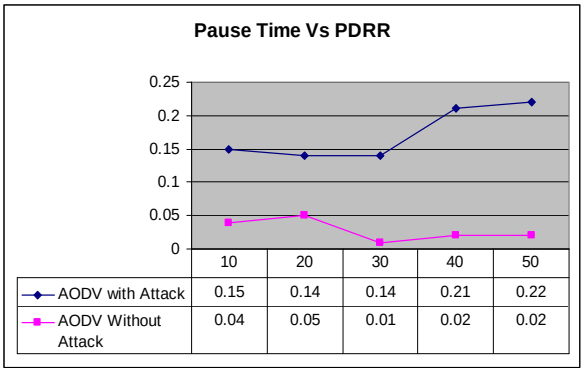

Fig.2. Pause time Vs PDRR

From above Fig.2 it is estimated that PDRR effect in AODV without attack are less and for AODV with attack changes by increasing or decreasing the pause time. There is much PDRR in case of AODV with Attack.

B) ANALYSIS OF PDRR FOR AODV WITH BLACK HOLE ATTACK AND WITHOUT ATTACK WITH VARIATIONS IN NODE SPEED.

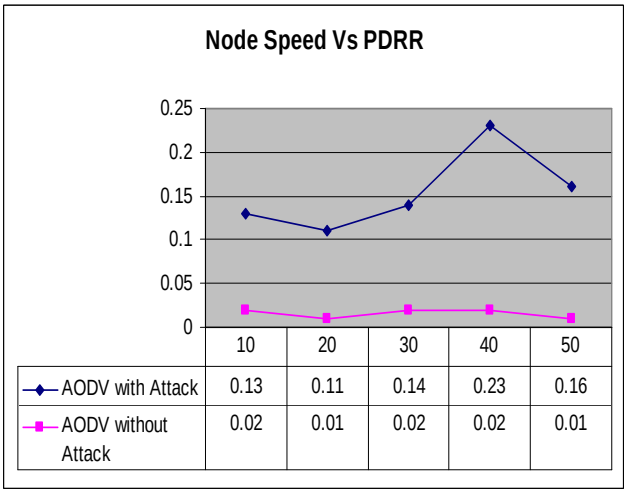

Fig.3: Node Speed Vs PDRR

For AODV without attack PDRR is 2% for node speed 10, 30, and 40.For node speed 20 and 50 it is 1%. For AODV with attack PDRR is initially 13% for node speed 10.It is minimum 11% for node speed 20 and maximum 23% for node speed 40.
From above Fig.3 it is estimated that PDRR effect in AODV without attack are less and for AODV with attack changes by increasing or decreasing the node speed. There is much PDRR in case of AODV with Attack.
After observing the results it is found that the under attack case system has PDRR always greater to threshold. Hence detection is supported.

.

CONCLUSIONS

This paper presents a detection analysis with black hole attack by using AODV routing protocol in different scenario. This analysis is performed in wireless ad hoc network.
After completion of all simulation results were analyzed in graph. It is observed that AODV without attack gives better result in all situations.After observing the results it is found that under attack case system has more packet drop ratio it is always greater to threshold. Hence detection is supported.

FUTURE WORK

The work can be extended by nitty-gritty study of routing protocols in a fault tolerant approach with proper simulation set up with parallel real time environment for mobile and wireless ad hoc networks.
This paper is for introduction and detection of blackhole attack as a part of future work, this work can be extended for implementation of prevention technique for blackhole attack.
As part of future work it can simulate Routing protocols by using other protocols with the help of other different parameters in wide network

REFERENCES

[1] Existing MANET Routing Protocols and Metrics used Towards the Efficiency and Reliability- An Overview Shafinaz Buruhanudeen, Mohamed Othman, Mazliza Othman, Borhanuddin Mohd Ali Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, 14-17 May 2007, Penang, Malaysia 1-4244-1094-0/07©2007 IEEE.

[2] Charles E.Perkins. Ad hoc Networking, Addison-Wedey, 2001

[3] 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, Vol.5, No.3, PP.338–346, Nov. 2007

[4] Md. Anisur Rahman, Md. Shohidul Islam, Alex Talevski, "Performance Measurement of Various Routing Protocols in Ad-hoc Network", International MultiConference of Engineers and Computer Scientists 2009 Vol I.

[5] Lidong Zhou, Zygmunt J. Haas "Securing Ad Hoc Networks", IEEE network, special issue on network security, November/December, 1999.

[6] Rajan Shankaran, Vijay Varadharajan, Michael Hitchens, "Securing the Ad Hoc Dynamic Source Routing Protocol" IEEE 2006 .

[7] Scalable Network Technology, "QualNet5.0 simulator" tutorial and QualNet Forum http://www.scalable-networks.com/forums/

[8] Jiwen CAI,Ping YI,Ye TIAN,Yongkai ZOHU,Ning LIU "The simulation and comparison of routing attack on DSR protocols" IEEE 2009