International Journal of Current Engineering and Technology
©2015 INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Investigating the Impact of Black Hole Attack on AODV with Statistical Tool-ANOVA

B.A.S Roopa Devi[†*], J.V.R Murthy[‡], G.Narasimha[‡] and S.Pallam Setty[§]

[†]Department of CSE, Pragati Engineering College, Kakinada, AP, India
[‡]Department of CSE, JNT University, Kakinada, AP, India
[§]Department of Computer Science and Systems Engineering, College of Engineering (A), Andhra University, Visakhapatnam, AP, India

Accepted 07 Jan 2015, Available online 01 Feb 2015, **Vol.5, No.1 (Feb 2015)**

Abstract

MANET is a infrastructure less network in which the communication is carried out without any physical link. However, due to the characteristics of MANET like Open Environment, Dynamic Topology and Distributed Nature, there is lot of possibility for the attacks. Among the various passive and active attacks that prevail in this dynamic network, Black Hole attack is one such dangerous active attack in MANETs. In this attack, a malicious node falsely assures that it has the shortest path to the destination even though it does not have one. This type of attack seriously damages the performance of the network and should be strictly prevented. In this paper, the impact of black hole attack on the Ad-hoc On-demand Distance Vector (AODV) routing protocol is investigated using Network Simulator (NS-2.34).The performance analysis of this active attack is measured using the QoS metrics such as Packet Delivery Ratio, Throughput, End-to-End Delay, Jitter and Packets Dropped and also proved statistically using a Stat Tool.

Keywords: *Mobile ad hoc network, AODV, Black hole attack, Security attacks, Network Simulator, ANOVA*

1. Introduction

The remarkable technology of wireless networks started in late 1970s and the interest has been growing ever since. Earlier, information sharing between various communication devices was difficult, as the users need to set up static, bi-directional links between the devices to perform various administrative tasks. In order to prevent the difficulty in maintaining these infrastructure based networks, various techniques have been determined leading to ad hoc networks. In Adhoc Networks, there is no infrastructure, which makes it easily deployable and connects the communication devices (nodes) within no time. Such interconnection between mobile nodes is called a Mobile Ad hoc Network (MANET).

Mobile ad hoc network is an autonomous and decentralized network in which any mobile node can freely move in and out of the network. These mobile nodes must act as both host and router in which both route discovery mechanism and data transmission between nodes is handled by the mobile nodes itself. These nodes have the ability to configure themselves and because of their self-configuring capability, they can form an arbitrary network when needed without the basis of any fixed infrastructure. Due to these characteristics, the network topology gets varied more frequently and hence a routing protocol must be efficient enough in delivering an ameliorated network performance. Traditional routing protocols used for wired networks cannot be employed for mobile ad hoc networks because the basic idea of such ad hoc networks is mobility with dynamic topology [Janne Lundberg *et al*, 2014]. Routing protocols plays a major role in such type of networks whose function is to transfer data packets between the mobile nodes efficiently tackling all the varying situations.

Due to their inherent characteristics and lack of any centralized administration, mobile ad hoc networks are vulnerable to different types of security attacks. These attacks include active interfering, passive eavesdropping, impersonation and denial of service [Ketan *et al*, 2014]. Since the communication among the nodes is purely based on mutual trust between nodes, malicious nodes in the network must be identified carefully and must be restricted in their behavior. Hence securing a mobile ad hoc network is necessary for basic functionality of the network. Black hole attack is one among these various attacks. In the black hole attack, a malicious node drops all the packets coming in its way without transferring them to its neighborhood node, thus degrading the network performance. Black hole attack may occur due to a malicious node which is deliberately misbehaving, as

*Corresponding author **B.A.S Roopa Devi** is working as Associate Professor; **Dr.V.R Murthy** as Professor; **G.Narasimha** as Associate Professor and **Dr. S.Pallam Setty** as Professor well as a damaged node interface. Such type of attacks must be prevented in order to obtain better performance of the network. In this paper, the performance of the AODV routing protocol is examined under black hole attack.

2. Routing protocols in MANETs

In MANETs, nodes are not familiar with the network topology in priori. Routing protocols are responsible in establishing the paths between the mobile nodes in order to transmit data between source and destination in that path. Hence a routing protocol must be efficient enough in handling various network phenomenon's and must tolerate against different security attacks. These routing protocols are broadly classified into three types based on the phenomenon in which they broadcast information.

1. Proactive or Table-Driven routing protocols
2. Reactive or On-Demand routing protocols
3. Hybrid routing protocols

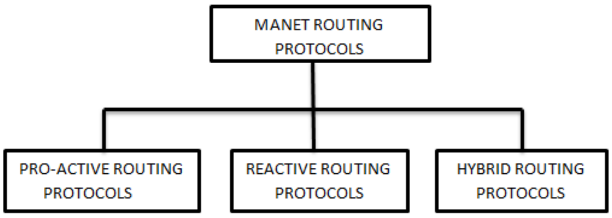


Figure 1: Routing Protocols in MANETs

2.1 Proactive routing protocols

Proactive routing protocols designed for MANETs are adopted from various traditional routing protocols available for wired networks. Proactive routing protocols attempt to maintain an up-to-date routing information from each node to every other node in the network prior to the need of data transmission. The routing information is kept in a number of different routing tables and the routing information is updated regularly responding to the changes in the network topology. Primary advantage of proactive routing protocols is the availability of routes to concern nodes at any moment. Control overhead generated by these protocols is significantly more in large networks. Examples of such networks include DSDV, OLSR, WRP etc.

2.2 Reactive routing protocols

In this type of routing protocols, routes between the mobile nodes are not continuously maintained without any need such as in proactive routing protocols. Routes are established between the mobile nodes only when needed i.e., On-Demand. Here in reactive routing protocols, if a source node needs to send data packets to some destination, it checks whether it already has a route towards the destination to transmit data packets. If it does not find any route, then it initiates the route discovery phase to establish a new path towards the destination, through which the data packets are sent. The drawback of the reactive routing protocol is the introduction of route acquisition latency. The time taken by the data packets to reach the destination is more compared to proactive routing protocols. Reactive routing protocols include AODV, DSR, and AOMDV etc.

2.3 Hybrid routing protocols

Hybrid routing protocols exploit the strengths of both proactive and reactive routing protocols in order to deliver better performance. In hybrid routing, entire network is divided into zones so that, one protocol is used within a zone and another protocol is used between the zones. ZRP is an example of such routing protocol.

Performance of the On-demand routing protocol, AODV is determined in this paper.

Ad-hoc On-demand Distance Vector (AODV) routing protocol

AODV is an on-demand routing protocol. It does not maintain any routing information and participate in any periodic routing table exchanges prior to the necessity of communication. It finds the route between the mobile nodes only when needed (on-demand). AODV routing protocol adopts the concept of destination sequence numbers from DSDV to maintain the most recent information about the mobile nodes and the concept of on-demand route discovery and maintenance from DSR. Each entry in the routing table consists of the destination node, destination sequence number, number of hops, next hop, expiration table for the entry in the tables containing the routing information etc. AODV routing protocol makes use of various control messages such as Route Request (RREQ), and Route Reply (RREP) for establishing a path from source to destination. Header information of various control messages used in AODV is listed out in [C. E. Perkins *et al*, 2004].

Whenever a source node needs to communicate with another node for which it has no route, the process of route discovery is initiated by the source which broadcasts a RREQ packet to its neighborhood nodes. Each neighboring node either responds to the RREQ by sending Route Reply (RREP) packet back to the source node or it further transfers the RREQ packets to its neighborhood nodes after incrementing the hop count. This route discovery process is carried on until the RREQ packet reaches the destination node or an intermediate node that has a fresh enough route entry for the destination in the routing table. Once the intermediate node has a valid route towards destination, it sends a RREP packet back to the source node in the reverse path. Making use of the reply from an intermediate node rather than the destination node reduces the route establishment time and also the control traffic in the network.

Sequence numbers are used in these control packets and they serve as time stamps which are used by the nodes to compare the freshness in the routing information [Ranjeet *et al*,2012]. When a node sends any type of routing control message, it increases its own sequence number in the message. Routing information with highest sequence number is considered to have more fresh or up-to-date information. If a node receives more than one RREP, it updates its routing information, and propagates the RREP with the highest sequence number discarding others.

The source starts the data transmission as soon as it receives the first RREP, and then its updates its routing information of better route to the destination node. If at all any of the nodes in the data path moves away causing the breakage of the link, the route discovery process is reinitiated to establish a new route to the destination node, Route Error (RERR) control packet is sent to all the nodes in the network which are using this broken link for communication. Routing protocol assumes that all the nodes are cooperative in nature in broadcasting information.

3. Security attacks in MANETs

As in [H. Deng *et al*, 2002], security is a very important issue for the basic functioning of the network. MANETs are more susceptible to various attacks than wired networks due to its flexible environment. Due to its dynamic nature, the network can be accessed by both the legitimate users and malicious attackers. Since the routing protocol assumes that all the nodes in the network are cooperative in nature, malicious attackers can easily disrupt network operations by violating protocol specification. An attacker first analyses the network functioning and then launch attacks into the network which degrades the network performance. Hence these attacks must be strictly prohibited.

These attacks are basically classified into two categories – Passive attacks and Active attacks. These are further sub-classified into various kinds depending upon the type of the attack such as Denial of Service attack, Fabrication attack, Modification attack, Replay attack and Impersonation attack. Passive attacks just listen to the traffic of the network to obtain vital information. These types of attacks do not affect the functioning of the network. It is difficult to identify such type of attacks as the performance of the network does not vary. It is even not possible to detect the presence or the location of the attacker node in this case. The only way to prevent such type of attacks is through encryption. Whereas, active attacks aim to modify the transmitted data by adding random packets or attempt to interrupt the data flow from source to destination. The main purpose is to pull all packets towards the attacker for analysis or to obstruct the network communication. Black hole attack is one such attack which comes into this category. Among these two types of attacks, only active attacks can be accepted out at routing level. They can either be inner or outer. In order to combat these attacks, a secure environment should provide confidentiality, availability, authenticity, integrity and non-repudiation [Jaspal Kumar *et al*, 2013].

3.1 Black hole attack

A Black hole attack is a denial of service type of attack, where a malicious node attracts all the data packets by falsely claiming that it has the shortest and fresh enough route towards the destination. Once the source node chooses that path to transfer data, the malicious node absorbs all the data without forwarding them to the destination. To be more elaborate, when a source nodes needs to communicate with some destination node, it initiates the route discovery process by sending route request (RREQ) packets. In black hole attack, a malicious node initially waits till the nodes broadcast RREQ packets. Once the RREQ packet is received by the malicious node, it immediately responds with a false route reply (RREP) packet with highest sequence number, indicating that it has the fresh route towards the destination. The source node believes that the destination node is behind the malicious node and ignores all the RREP packets received from other nodes, even if it is from actual destination. Then the source node transmits the data packets through the path containing the malicious node trusting that these packets will reach the destination. Once the data packets reach the black hole node, it does not forward the data packets further and simply drops them. Thus, a black hole node pretends to have fresh routes to all the destinations in the network requested by all the nodes and absorbs the networks data traffic. This type of attack never forwards any data packets.

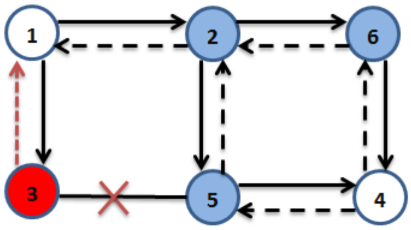


Figure 2: Black hole attack in MANET

In figure 2, source node 1 wants to send data packets to the destination node 4 in the network. Here node 3 is a malicious node which acts as a black hole. When the source node initiates the route discovery process, the malicious node responds to the RREQ packet immediately with a false or malicious RREP having higher modified sequence number, though it do not have any route to the destination. Since the reply from the malicious node first reaches the source node, it updates its routing table accordingly. Then it starts broadcasting the data packets through node 3, which do not forward the data packets to its neighboring node.

4. Simulation Setup

In order to analyze the performance of AODV under blackhole attack, network simulator NS-2.34 is used. NS-2.34 uses the collaborative environment for simulation making use of discrete event simulation. Here various quantitative metrics like packet delivery ratio, average end-to-end delay, normalized routing load and jitter are estimated under blackhole attack. The performance of the network is determined with the following network parameters summarized in Table 1.

Table 1: Simulation Parameters

Parameters	Values
Simulator	NS – 2.34
Network Dimensions	1500m x 1500m
Simulation Time	200 sec
Node mobility model	Random waypoint
Routing protocols	AODV
Application	UDP,TCP
Traffic type	Constant Bit Rate (CBR)
No. of nodes	20, 40, 60, 80, 100
Speed of node	5 – 30 m/s in steps of 5
Pause Time	0 sec
Physical Layer	IEEE 802.11b
MAC Protocol	IEEE 802.11
Transmission rate	100 kbps
Packet size	512 kb

5. Performance Evaluation

In this paper, the effect of black hole attack is determined by considering the quantitative metrics such as packet delivery ratio, average end-to-end delay, normalized routing load and jitter. However, the network performance is evaluated with and without attack. In both these cases, the following metrics are considered to evaluate the performance under varied node mobility and node density.

1) Packet Delivery Ratio: Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. It represents the maximum throughput that the network can achieve. A high packet delivery ratio is desired in any network.

$$PDR = \frac{Total\ no.\ of\ received\ packets}{Total\ no. of\ packets\ sent}$$

2) Average End-to-End Delay: The packet end-to-end delay is considered as the average time a packet takes to traverse the network. This is the time from the generation of a packet by the source, till its reception at the destination's application layer and is expressed in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. The end-to-end delay is therefore a measure of the how well a routing protocol adapts to the various constraints in the network and represents the reliability the routing protocol.

$$EED = \sum \frac{(Received\ time - sent\ time)}{Total\ data\ packets\ received}$$

3) Normalized Routing Load: Normalized Routing Load is the ratio between the total number of routing packets sent to the number of data packets delivered. This metric is used to evaluate the scalability of the network.

$$NRL = \frac{no.\ of\ routing\ packets\ sent}{no. of\ data\ packets\ received}$$

4) Jitter: Jitter is the variation in the time between packets arrival, caused by network congestion, timing drift, or route changes. A network with constant delay has no variation (or jitter). Hence jitter should be minimum for a routing protocol to perform better.

5.1 Impact of black hole attack with varied node densities

In order to determine the impact of the black hole attack on the AODV routing protocol, its performance is determined including an attacker node and by varying the total number of nodes, various metric values are determined which are discussed in this section.

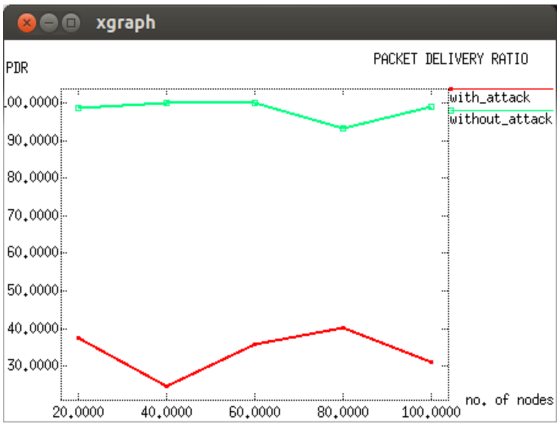


Figure 5.1: No. of nodes vs PDR

From Figure 5.1, we observe a drastic change in the packet delivery ratio when the network is analyzed in the presence of black hole attack. This happens because the number of packets delivered greatly reduces as all packets traversed in attacker's way, will be dropped. From figure 5.2, when we analyze the network with varying node density from 0-60 nodes, end to end delay remains same. After 60 nodes, in the presence of attack as the black hole node send RREP message immediately with minimum hop count and maximum sequence number, this implies that delay for the packets from source to destination is reduced. From figure5.3, in the presence of attack, the data packets received greatly reduces and hence normalized routing load increases; but as the node density increases NRL remains almost same. From figure 5.4, as the number of nodes increases over 40 nodes, jitter in the network increases indefinitely as the attacker nodes presence creates routing changes and congestion in the network when compared to no attack scenario.

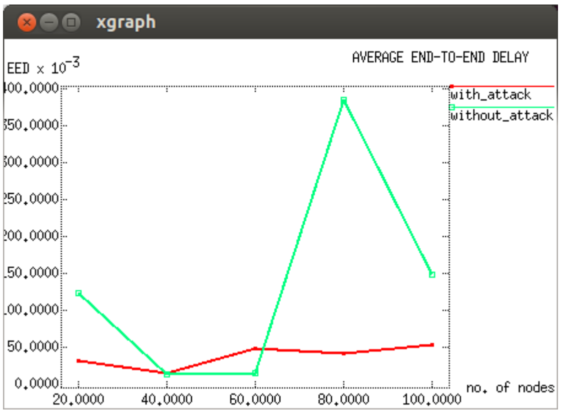


Figure 5.2: No. of nodes vs EED

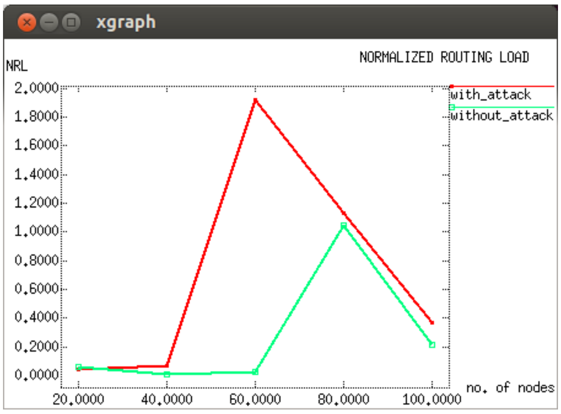


Figure 5.3: No. of nodes vs NRL

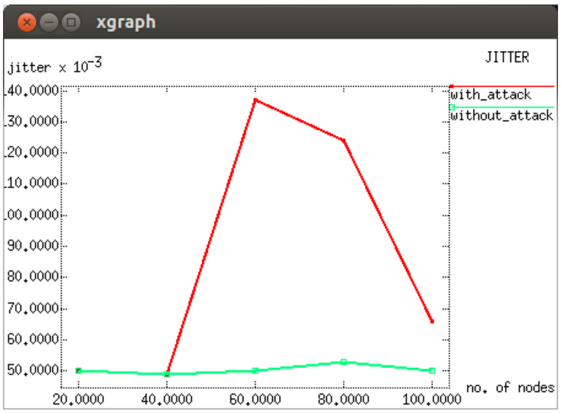


Figure 5.4: No. of nodes vs Jitter

6. Statistical Tool-ANOVA

Analysis of variance (ANOVA) is the method used to compare continuous measurements to determine if the measurements are sampled from the same or different distributions. It is an analytical tool used to determine the significance of factors on measurements by looking at the relationship between a quantitative response variable and a proposed explanatory factor. This method is similar to the process of comparing the statistical difference between two samples, in that it invokes the concept of hypothesis testing. Two-way ANOVA is used in the instance that the variance depends on two factors. There are two cases in which two-way ANOVA can be employed:

- Data *without replicates*: used when collecting a single data point for a specified condition
- Data *with replicates*: used when collecting multiple data points for a specified condition (the number of replicates must be specified and must be the same among data groups)

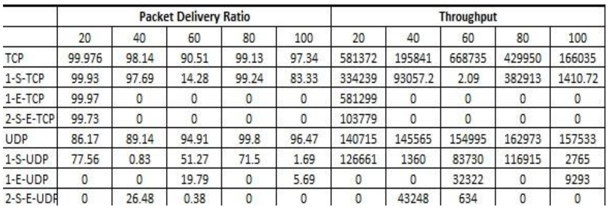
The F-statistic is the ratio of two variance estimates: the variance between groups divided by the variance within groups. The larger the F-statistic, the more likely it is that the difference between samples is due to the factor being tested, and not just the natural variation within a group. A standardized table can be used to find $F_{critical}$ for any system. $F_{critical}$ will depend on alpha, which is a measure of the confidence level. Typically, a value of alpha = 0.05 is used, which corresponds to 95% confidence. If $F_{observed} > F_{critical}$, we conclude with 95% confidence that the null hypothesis is false.

The F-Test is the ratio of the sample variances. The F-statistic and the corresponding F-Test are used in single-factor ANOVA for purposes of hypothesis testing.

- Null hypothesis (H_o): all sample means arising from different factors are equal
- Alternative hypothesis (H_a): the sample means are not all equal

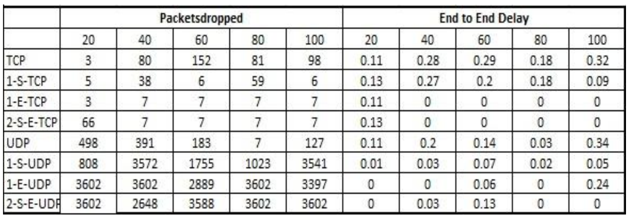
6.1 Statistical Evaluation- Results

The QoS metrics like Packet Delivery Ratio, Throughput, End-to-End Delay, Jitter, Packets Dropped are analyzed using the Statistical Tool ANOVA and it is observed that the F critical value for all the metrics is greater than the F-Statistic value when compared with and without attack, from which it is obvious that there is significant impact of black hole attack on MANET environment.



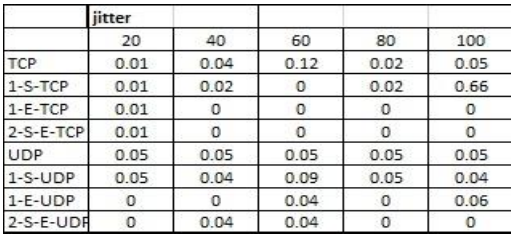
	Packet Delivery Ratio					Throughput				
	20	40	60	80	100	20	40	60	80	100
TCP	99.976	98.14	90.51	99.13	97.34	581372	195841	668735	429950	166035
1-S-TCP	99.93	97.69	14.28	99.24	83.33	334239	93057.2	2.09	382913	1410.72
1-E-TCP	99.97	0	0	0	0	581299	0	0	0	0
2-S-E-TCP	99.73	0	0	0	0	103779	0	0	0	0
UDP	86.17	89.14	94.91	99.8	96.47	140715	145565	154995	162973	157533
1-S-UDP	77.56	0.83	51.27	71.5	1.69	126661	1360	83730	116915	2765
1-E-UDP	0	0	19.79	0	5.69	0	0	32322	0	9293
2-S-E-UDP	0	26.48	0.38	0	0	0	43248	634	0	0

Figure 6.1: Packet Delivery Ratio & Throughput



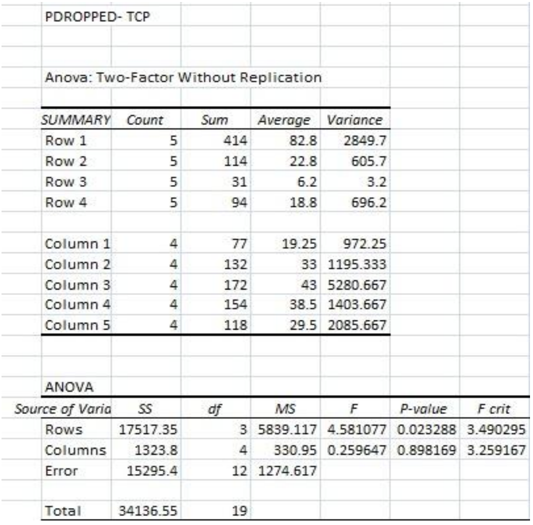
	Packetsdropped					End to End Delay				
	20	40	60	80	100	20	40	60	80	100
TCP	3	80	152	81	98	0.11	0.28	0.29	0.18	0.32
1-S-TCP	5	38	6	59	6	0.13	0.27	0.2	0.18	0.09
1-E-TCP	3	7	7	7	7	0.11	0	0	0	0
2-S-E-TCP	66	7	7	7	7	0.13	0	0	0	0
UDP	498	391	183	7	127	0.11	0.2	0.14	0.03	0.34
1-S-UDP	808	3572	1755	1023	3541	0.01	0.03	0.07	0.02	0.05
1-E-UDP	3602	3602	2889	3602	3397	0	0	0.06	0	0.24
2-S-E-UDP	3602	2648	3588	3602	3602	0	0.03	0.13	0	0

Figure 6.2: Packets Dropped & End to End Delay



	jitter				
	20	40	60	80	100
TCP	0.01	0.04	0.12	0.02	0.05
1-S-TCP	0.01	0.02	0	0.02	0.66
1-E-TCP	0.01	0	0	0	0
2-S-E-TCP	0.01	0	0	0	0
UDP	0.05	0.05	0.05	0.05	0.05
1-S-UDP	0.05	0.04	0.09	0.05	0.04
1-E-UDP	0	0	0.04	0	0.06
2-S-E-UDP	0	0.04	0.04	0	0

Figure 6.3: Jitter



PDROPPED- TCP

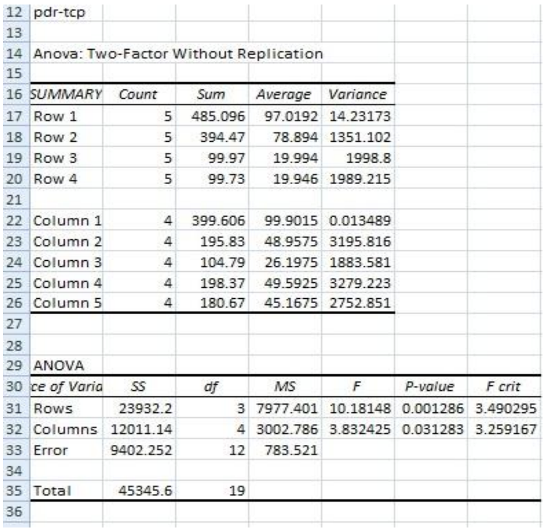
Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	414	82.8	2849.7
Row 2	5	114	22.8	605.7
Row 3	5	31	6.2	3.2
Row 4	5	94	18.8	696.2
Column 1	4	77	19.25	972.25
Column 2	4	132	33	1195.333
Column 3	4	172	43	5280.667
Column 4	4	154	38.5	1403.667
Column 5	4	118	29.5	2085.667

ANOVA

Source of Varia	SS	df	MS	F	P-value	F crit
Rows	17517.35	3	5839.117	4.581077	0.023288	3.490295
Columns	1323.8	4	330.95	0.259647	0.898169	3.259167
Error	15295.4	12	1274.617			
Total	34136.55	19				

Figure 6.4: Statistical Evaluation of Packets Dropped-TCP



pdr-tcp

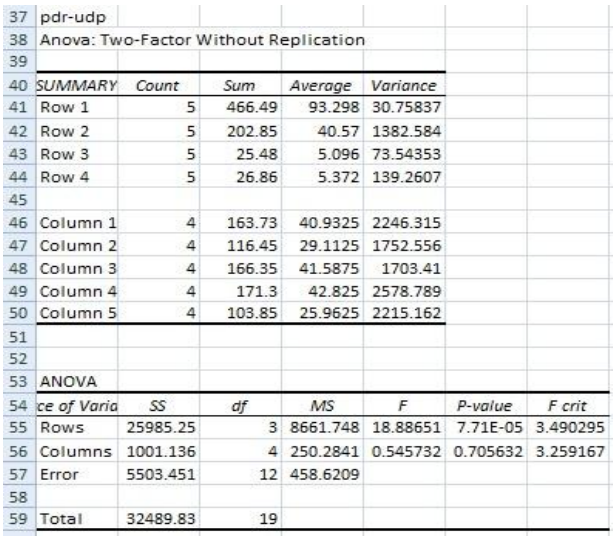
Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	485.096	97.0192	14.23173
Row 2	5	394.47	78.894	1351.102
Row 3	5	99.97	19.994	1998.8
Row 4	5	99.73	19.946	1989.215
Column 1	4	399.606	99.9015	0.013489
Column 2	4	195.83	48.9575	3195.816
Column 3	4	104.79	26.1975	1883.581
Column 4	4	198.37	49.5925	3279.223
Column 5	4	180.67	45.1675	2752.851

ANOVA

ce of Varia	SS	df	MS	F	P-value	F crit
Rows	23932.2	3	7977.401	10.18148	0.001286	3.490295
Columns	12011.14	4	3002.786	3.832425	0.031283	3.259167
Error	9402.252	12	783.521			
Total	45345.6	19				

Figure 6.5: Statistical Evaluation of Packet Delievery Ratio-TCP



pdr-udp

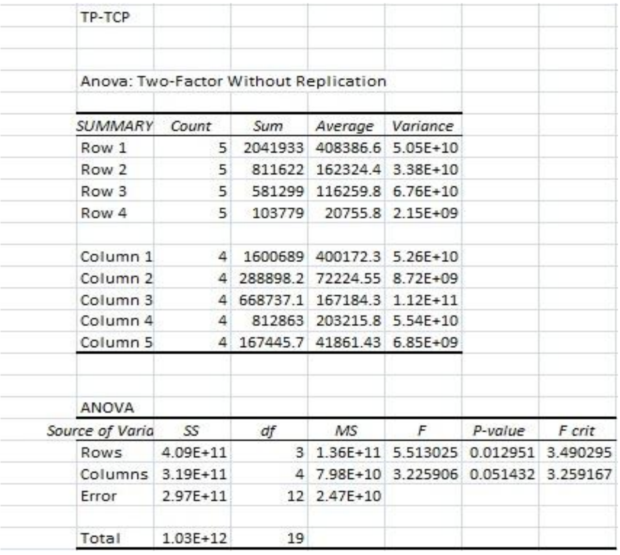
Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	466.49	93.298	30.75837
Row 2	5	202.85	40.57	1382.584
Row 3	5	25.48	5.096	73.54353
Row 4	5	26.86	5.372	139.2607
Column 1	4	163.73	40.9325	2246.315
Column 2	4	116.45	29.1125	1752.556
Column 3	4	166.35	41.5875	1703.41
Column 4	4	171.3	42.825	2578.789
Column 5	4	103.85	25.9625	2215.162

ANOVA

ce of Varia	SS	df	MS	F	P-value	F crit
Rows	25985.25	3	8661.748	18.88651	7.71E-05	3.490295
Columns	1001.136	4	250.2841	0.545732	0.705632	3.259167
Error	5503.451	12	458.6209			
Total	32489.83	19				

Figure 6.6: Statistical Evaluation of Packet Delievery Ratio-UDP



TP-TCP

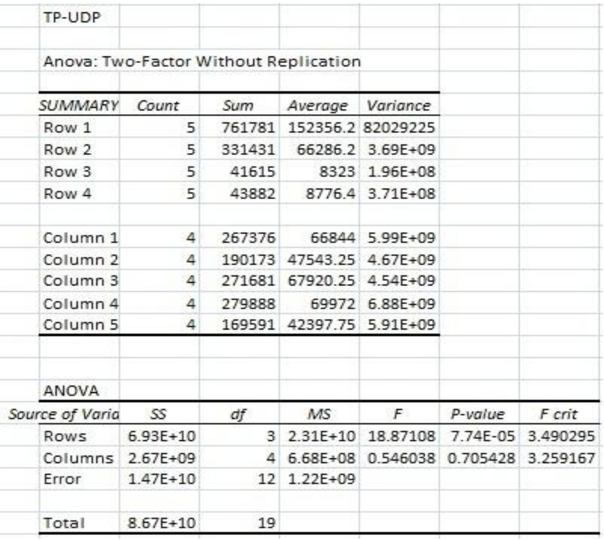
Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	2041933	408386.6	5.05E+10
Row 2	5	811622	162324.4	3.38E+10
Row 3	5	581299	116259.8	6.76E+10
Row 4	5	103779	20755.8	2.15E+09
Column 1	4	1600689	400172.3	5.26E+10
Column 2	4	288898.2	72224.55	8.72E+09
Column 3	4	668737.1	167184.3	1.12E+11
Column 4	4	812863	203215.8	5.54E+10
Column 5	4	167445.7	41861.43	6.85E+09

ANOVA

Source of Varia	SS	df	MS	F	P-value	F crit
Rows	4.09E+11	3	1.36E+11	5.513025	0.012951	3.490295
Columns	3.19E+11	4	7.98E+10	3.225906	0.051432	3.259167
Error	2.97E+11	12	2.47E+10			
Total	1.03E+12	19				

Figure 6.7: Statistical Evaluation Throughput -TCP



TP-UDP

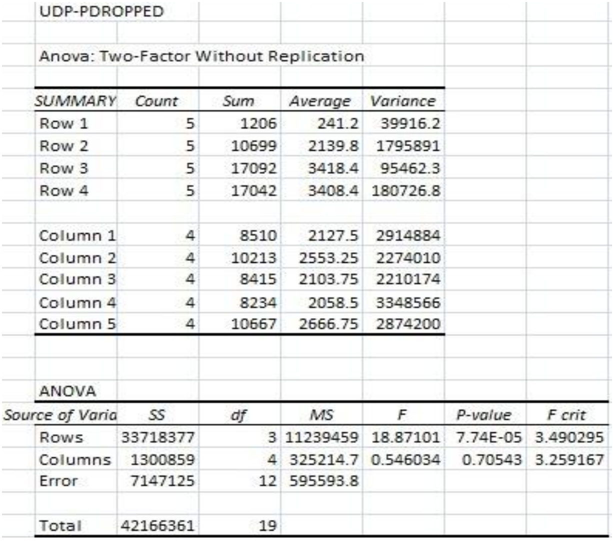
Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	761781	152356.2	82029225
Row 2	5	331431	66286.2	3.69E+09
Row 3	5	41615	8323	1.96E+08
Row 4	5	43882	8776.4	3.71E+08
Column 1	4	267376	66844	5.99E+09
Column 2	4	190173	47543.25	4.67E+09
Column 3	4	271681	67920.25	4.54E+09
Column 4	4	279888	69972	6.88E+09
Column 5	4	169591	42397.75	5.91E+09

ANOVA

Source of Varia	SS	df	MS	F	P-value	F crit
Rows	6.93E+10	3	2.31E+10	18.87108	7.74E-05	3.490295
Columns	2.67E+09	4	6.68E+08	0.546038	0.705428	3.259167
Error	1.47E+10	12	1.22E+09			
Total	8.67E+10	19				

Figure 6.8: Statistical Evaluation Throughput -UDP



UDP-PDROPPED

Anova: Two-Factor Without Replication

SUMMARY	Count	Sum	Average	Variance
Row 1	5	1206	241.2	39916.2
Row 2	5	10699	2139.8	1795891
Row 3	5	17092	3418.4	95462.3
Row 4	5	17042	3408.4	180726.8
Column 1	4	8510	2127.5	2914884
Column 2	4	10213	2553.25	2274010
Column 3	4	8415	2103.75	2210174
Column 4	4	8234	2058.5	3348566
Column 5	4	10667	2666.75	2874200

ANOVA

Source of Varia	SS	df	MS	F	P-value	F crit
Rows	33718377	3	11239459	18.87101	7.74E-05	3.490295
Columns	1300859	4	325214.7	0.546034	0.70543	3.259167
Error	7147125	12	595593.8			
Total	42166361	19				

Figure 6.9: Statistical Evaluation Packets Dropped – UDP

Figures 6.1, depicts the values obtained for the Packet Delivery Ratio & Throughput, Fig 6.2 shows Packets Dropped & End to End Delay values , Fig 6.3 depicts the values of Jitter.

Figures 6.4-6.9 illustrates the statistical evaluation of the QoS metrics for both TCP and UDP,where the F value is greater than the Fcriticial value which contradicts the null hypothesis.Hence,it is also proved statistically using the ANOVA STAT tool that there is significant impact of black hole attack on MANET environment as stated above.

Conclusion

In this paper, Impact of Black Hole Attack on AODV in MANET, considering various simulation parameters listed above has been analyzed. This dynamic network, MANET is examined for QoS metrics like packet delivery ratio, average end-to-end delay, normalized routing load and jitter with varying node densities in the deployed network. The simulation results signify that the performance of network in the presence of black hole attack is predominantly decreasing in packet delivery ratio as the attacker nodes discards all the data packets traversing its path. Jitter increases as the attacker nodes increase congestion in the routes discovered, end to end delay decreases in the presence of attack, as the attacker nodes send RREP message immediately with minimum hop count and maximum sequence number. These changes in metrics conclude that network performance is degraded predominantly in the presence of black hole attack.

References

Ketan Sureshbhai Chavda (2014) A Performance analysis of AODV under Black hole attack in MANET, IJTCSE, Vol.1, No.2, pp. 82-87.

Jaspal Kumar, M. Kulkarni, Daya Gupta (2013) Effect of Black hole Attack on MANET routing protocols, IJCNIS, Issue 5, pp. 64-72.

Ranjeet Suryawanshi, Sunil Tamhankar,(2012) Performance Analysis and Minimization of Black hole attack in MANET, IJERA, Vol. 2, Issue-4,pp. 1430-1437.

Punardeep Singh, Er. Harpal Kaur, Satinder Ahuja (2012) Brief Description of Routing Protocols in MANETs and Performance and Analysis (AODV, AOMDV, TORA), IJARCSSE, Vol. 2, Issue. 1.

Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao(2010),Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks,IEEE International Symposium on Parallel and Distributed Processing with Application.

Anuj K. Gupta, Harsh Sadawarti (2009),Secure Routing Techniques for MANETs, International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201, Article No. 74, Vol.1 No. 4, pp. – 456-460.

R. H Rashid Khokhar , Md. A. Nagdi(2009), A Review of Current Routing Attacks in Mobile Ad Hoc Networks, International Journal of Computer Science and Security, pages 18-29.

K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer,(2005) Authenticated routing for ad hoc networks, IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610.

M. A. Shurman, S. M. Yoo, and S. Park (2004), Black hole attack in wireless ad hoc networks. proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97.

C. E. Perkins, E. Beliding Royer, S. Das (2004) Ad hoc On-demand Distance Vector (AODV) routing, IETF Internet Draft, MANET working group.

B. Dahill, B. N. Levine, E. Royer, and C. Shields,(2002),A secure routing protocol for ad hoc networks,‖ in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87.

Y. Hu, A. Perrig and D. Johnson, Ariadne(2002), A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02.

H. Deng, W. Li, and D. P. Agarwal (2002) Routing security in ad hoc networks, IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75.

Nital Mistry, Devesh C Jinwala, Mukesh Zaveri (2000) Improving AODV Protocol against Black hole Attacks,Proceedings of the international multi conference of engineer and computer science vol. 2.

C. E. Perkins and E. M. Royer (1999)Ad Hoc On-Demand Distance Vector Routing Proc. 2nd IEEE Workshop. Mobile Computing System and Apps. New Orleans, LA, pp. 90–100.

ns-2, Network simulator, http:// www.isi.edu/ nsnam/ns