IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Detection and Prevention of Black Hole Attacks in Manets Using NTP Method

Arshdeep Singh[1], Er. Harshdeep Trehan[2], Er. Varinderjit kaur[3], Dr. Naveen Dhillon[4]

P.G. Student, Department of CSE, RIET, Phagwara[1]

Asst Prof, Department of CSE, RIET, Phagwara[2]

HOD, Department of CSE, RIET, Phagwara[3]

Principal of RIET, Phagwara[4]

Abstract: A mobile ad hoc network (MANET) is an accumulation of wireless mobile nodes which are having the capability for communicating with one another with having no central base station and network infrastructure. Whenever the source node sends the messages of route request in the network the node which is malicious after getting the request of message creates a route reply to the source. In this novel approach is presented in which black hole attack is prevented by using NTP method. Firstly nodes are deployed in the network and the source node sends route request to the destination node and after those first two replies are selected by source and compares them and if sequence number is very high, the node will be considered as malicious node. In this research work, fact considered is that the black hole never sends the message of route request in the network. The number of request packets that are forwarded will be zero. As source node gets many replies from the nodes and it will compare the time. As the time of black hole is less than all other nodes and number of forwarded request packets is zero also, so that malicious path will not be chosen by source node.

Keywords: MANETs, RREP, RREQ, black hole, AODV, NTP.

I. INTRODUCTION

In today's quick and quickly developing universe of technologies, MANET can turn the dream of networking at any time and place into reality. We are just about there by the route, for example, Bluetooth empowered mobile phones like 3G. MANET gives loads of highlight and now more and more organizations comprehend the benefits of utilization of computer networking. Contingent upon the resources and size of firm, it may be small LAN having just a couple of computers; however in expansive organizations the network can develop to complex and tremendous mixture of servers and computers. A computer network is a framework for communication and between two computers and system. These networks may be temporary or permanent. A mobile (mobile ad hoc network) is a self-designing network of mobile devices having no infrastructure joined by wireless.[1]

A mobile adhoc network (MANETS) is a group of mobile nodes which are wireless and having the capability to correspond with one another having no settled network infrastructure or any focal base station. Early research accepted a cooperative and friendly environment of wireless network. Subsequently, they concentrated on issues, for example, multihop routing and wireless channel access. Since mobile nodes are not controlled by some other controlling element, they have unlimited connectivity and mobility to others. Network and routing management are done helpfully by one another nodes. Because of transmission power which is limited, multi hop design is required for one node to communicate with other via network. In this multi-hop design, every node acts as a host and additionally as a router that forwards packets for different nodes that might not be inside of a range of direct communication. Every node takes part in a protocol of discover of ad hoc route which discovers out multi hop routes via mobile network between any two nodes. These mobile nodes without infrastructure in ad hoc networks make routes dynamically among themselves to shape own wireless networks on the fly.[2]

Mobile networks are normally open to attack to physical security threats and information that wired networks which are fixed. Providing security of wireless ad hoc networks is especially troublesome for numerous reasons incorporating vulnerability of nodes and channels, topology which is changing dynamically, infrastructure less etc. The wireless channel is accessible to malicious attackers as well as to legitimate users of network. A malicious attacker can rapidly turn into a router and break operations of network by deliberately not taking after the specifications of protocol.

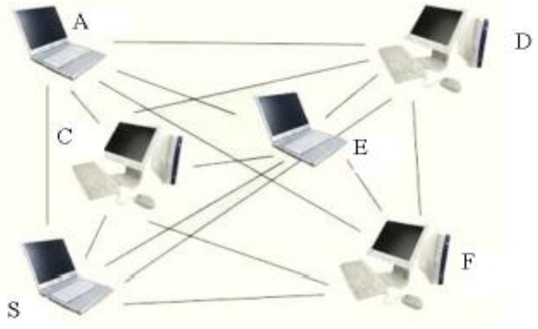


Fig. 1 Mobile Ad hoc network .[3]

DOI 10.17148/IJARCCE.2016.5278

The protocols of routing in MANETs are essentially categorized into divisions: Proactive and Reactive routing protocols and another category is Hybrid routing protocols. Proactive routing protocols are likewise known as protocols of table driven which keep up the lists of all conceivable destination nodes in a table and intermittently changes messages of routing, with a specific end goal to keep the data in the table of routing correct and up-to-date. At the point when transmission is needed from one node to other node, the knowledge of route is available and can be utilized. The instances of Proactive Protocols are OLSR (Optimized Link State Routing Protocol), DSDV (Distributed Sequenced Distance Vector Protocol). Then again, Reactive Protocols, for example, DSR and AODV protocols are protocols of on demand i.e. appeal to procedure of determination of route on demand only. At the point when there is requirement of route, some kind of procedure of discover of route is utilized, in light of the fact that these protocols accept participation between two packets for forwarding of packet, a malicious node might prompt attack of routing in the network that disturbs the operations of normal routing in MANET. Thus dynamic and decentralized nature of MANET might prompt different attacks in the network that can demolish or partition the network. [4]

Normally, there are two main attacks in the MANETs, first one is Active attack and second is Passive attack. In active attack, interloper can destroy or alter the data which is originally present. But in passive attack, the interloper quietly listen the channel of communication with no destroying and alteration in packets of data. Because of fast deployment and insignificant arrangement, MANETs are appropriate for situations of emergency such as hospitals, military, and rescue operations of Natural disasters. Accordingly transfer of information between two nodes must need security. In any case, active attacks such as Black hole attack, Worm hole attack and Rushing attack have incredible influence on the network's performance.[4]

II. BLACK HOLE ATTACK

In Black hole attack, a node which is malicious utilizes its protocol of routing so as to promote itself for having the path which is shortest to the destination node or to the packet it needs to capture. This antagonistic node promotes its accessibility of routes which are fresh regardless of checking its table of routing. Along these lines, node of attacker will dependably have the accessibility in giving reply to the request of route and hence capture the packet of data and hold it. In the protocol dependent upon flooding, the reply of malicious node will be gotten by node which is requesting before the gathering of reply from the genuine node; consequently a forged and malicious is made. At the point when this route is build up, now it's up to the node whether forward all the packets to the address which is unknown or drop every one of the packets.[5]

A problem of black hole implies that a node which is malicious uses the protocol of routing for claiming itself of being the path which is shortest to the destination node, however declines the packets of routing yet does not forward packets to its nearby nodes. Suppose a node "M" which is malicious. When node "A" transmit a RREQ packet, other nodes "M", "D" and "B" get it. The node "M" being malicious does not check up with its table of routing for the route requested to "E" node. Thus it promptly sends back packet of RREP, guaranteeing a route to the destination. "A" node gets the RREP from "M" in front of the RREP from "D" and "B". "A" node accepts that route via "M" is the route which is shortest and forwards any packet to the destination via it. At the point when "A" node transmits data to "M", it acts like a "Black hole".[6]

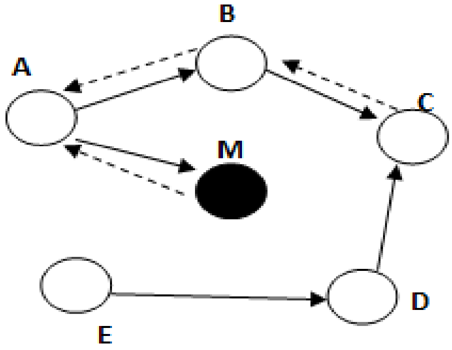


Fig. 2 Black Hole Attack in AODV protocol [6]

III. TYPES OF BLACK HOLE ATTACKS

There are many types of black hole attacks which are discussed below: [7]

1. Based on Number of Malicious Nodes

(i) Single Blackhole: In this type, there is just a solitary node which is malicious which is in charge of controlling the entries of routing table of source node and accordingly putting itself into the path in between two nodes which are communicating.

(ii) Co-operated Blackhole: In co-operative attacks, there are nodes of multiple attackers which co-operates with one another to dispatch an attack which is collaborative and expand the scope of topologies which are distorting.

2. Based on Position of Attacker

(i) Internal Blackhole: Internal blackhole attack happens when the nodes which are malicious are portion of the network itself i.e. they are available in the topology which they are deforming.

(ii) External Blackhole: In External Blackhole attack, the node which is malicious is an outer element physically yet it send up one of the inner nodes to demonstrate itself being the part of the network and send it to the intermediate nodes which are nearby which is piece of active communication and after that the source will overhaul its table of routing with the accessible freshest route and the entire communication of data will be handed off the through the node which is malicious.

3. Based on Control Packet Manipulated

(i) RREQ based Blackhole: In this attack, the aggressor puts on a show to rebroadcast RREQ in the direction of other nodes. Just hop count is set to be the least so that

DOI 10.17148/IJARCCE.2016.5278

another nodes can create their route via this node which is malicious and hence an aggressor can mightily turn out to be the route's part.

(ii) RREP based Blackhole: In this attack, the aggressor can create RREP message which is fake after getting the RREQ from source or even by parodying the communication which active. It generally changes hop count to 1 and sequence number of destination to the value which is higher.

IV. NTP METHOD

At the time when source node sends messages of route request in the network to the node at destination, the node which is malicious after getting message of request creates a reply of route to the source declaring shortest path to destination. Black hole node is detected in this method. Number of packets of request sent by specific node and the number of packets of request received by it are checked. The number of request of packets forwarded will be zero for black hole. This node will be put in the suspected list by source node. As source node gets numerous replies from nodes and also from node having black hole, the comparison will be done by source node as per the received replies by it. As the black hole node replies very fast, so the time will be less than rest of nodes. Hence the time is less and the numbers of packets of request sent are zero also. The source node will not forward information via that path and it will select some other path for sending the information. [8]

V. MOTIVATION

Mobile Ad-hoc networks are independent and decentralized wireless systems. MANETs comprise of mobile nodes that are free to move in and out in the network. The main issue in MANET is Cooperative Black hole attack which is very serious issue. The primary issue to security is mobility. The main aim of this research work is to detect and prevent black hole attack in MANETs by using NTP method. A Black Hole attack scrambles the route by forging a routing message, and then, further either eavesdrops or drop the packets, posing a possible threat to safety properties.

The research work is based on following objectives:

1. To analyze the performance of the network under black hole attack.
2. To detect the malicious black hole nodes in the network using sequence number comparison method.
3. Improving the performance of the network using NPT scheme.
4. Comparison of NPT and sequence number control method (SNCM) on the basis of parameters.

The parameters which are considered in this research work are throughput, packet delivery ratio and detection rate.

VI. PROPOSED SCHEME

In our research work, a technique is proposed which will detect and prevent the malicious nodes in the network using sequence number comparison method.

The algorithm of detection of black hole is as given below:

```
1.  NR: Number of packets (RREQ) received by node.
NF: Number of packets (RREQ) forwarded by node.
N: Total number of nodes.
For i = 1: N
    Ratio = NF/NR
    If (ratio == 0)
        Malicious = Node i
    End
End
2. Malicious set of nodes detected in previous step that did not forward RREQ packets
tR: time taken by node to reply to packet
for i= 1:m
    if ($t_i < t_D$)
        Node confirmed as black hole
          End
End
```

The **flowchart** of the proposed methodology is as shown below-

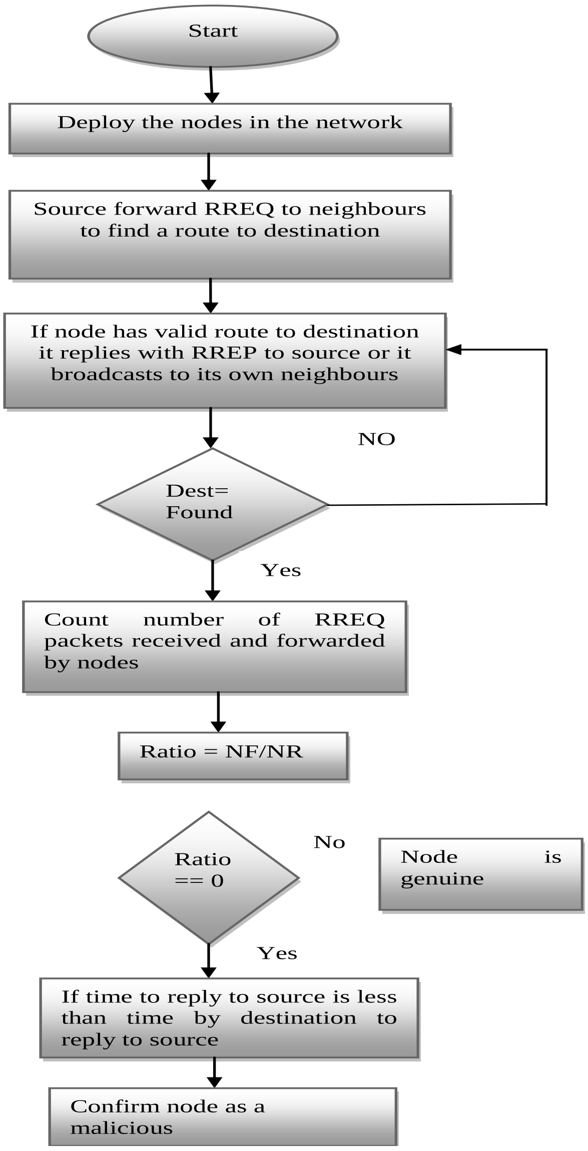
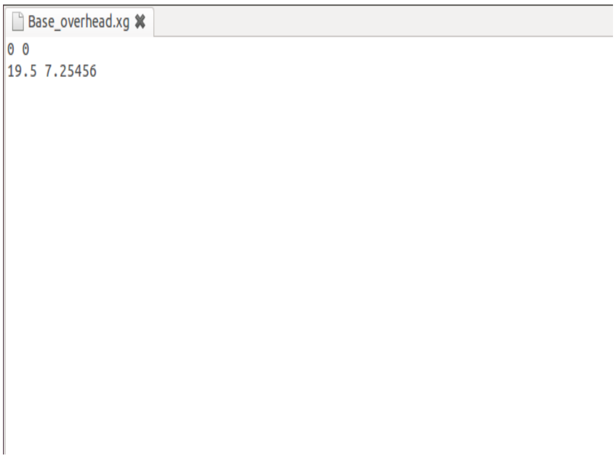

Start
Deploy the nodes in the network
Source forward RREQ to neighbours to find a route to destination
If node has valid route to destination it replies with RREP to source or it broadcasts to its own neighbours
NO
Dest= Found
Yes
Count number of RREQ packets received and forwarded by nodes
Ratio = NF/NR
No
Node is genuine
Ratio == 0
Yes
If time to reply to source is less than time by destination to reply to source
Confirm node as a malicious

Fig.3: Flowchart of proposed method

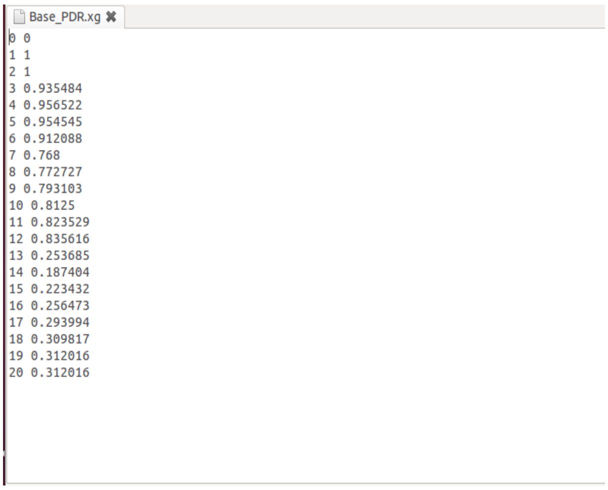
VII. RESULTS AND DISCUSSIONS

The main aim of this research work is to propose an approach of black hole attack prevention by using NTP method. The parameters considered are throughput, packet delivery ratio and overhead.



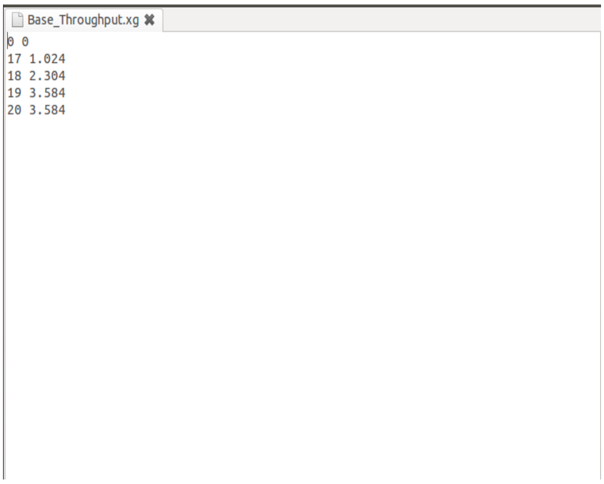
```
0 0
19.5 7.25456
```

Fig. 4: Overhead of base paper



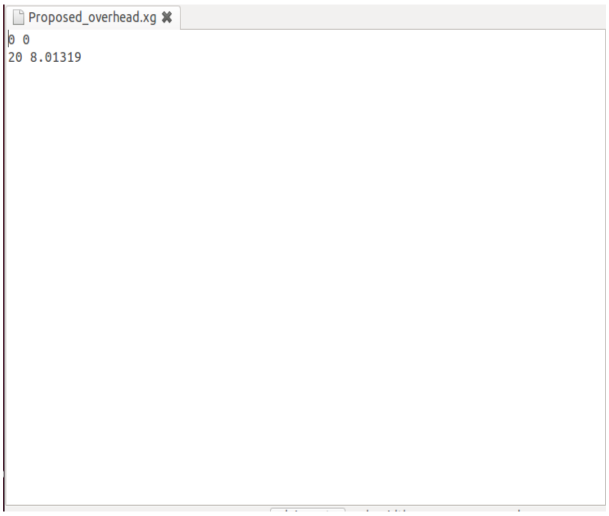
```
0 0
1 1
2 1
3 0.935484
4 0.956522
5 0.954545
6 0.912088
7 0.768
8 0.772727
9 0.793103
10 0.8125
11 0.823529
12 0.835616
13 0.253685
14 0.187404
15 0.223432
16 0.256473
17 0.293994
18 0.309817
19 0.312016
20 0.312016
```

Fig.5: Packet Delivery ratio of base paper



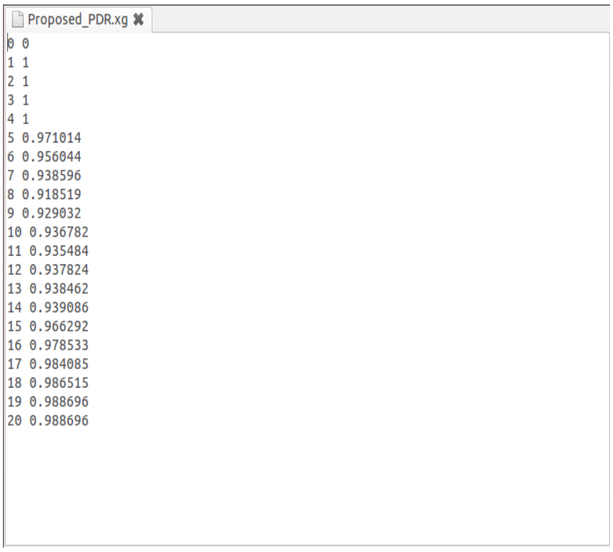
```
0 0
17 1.024
18 2.304
19 3.584
20 3.584
```

Fig. 6: Throughput of base paper



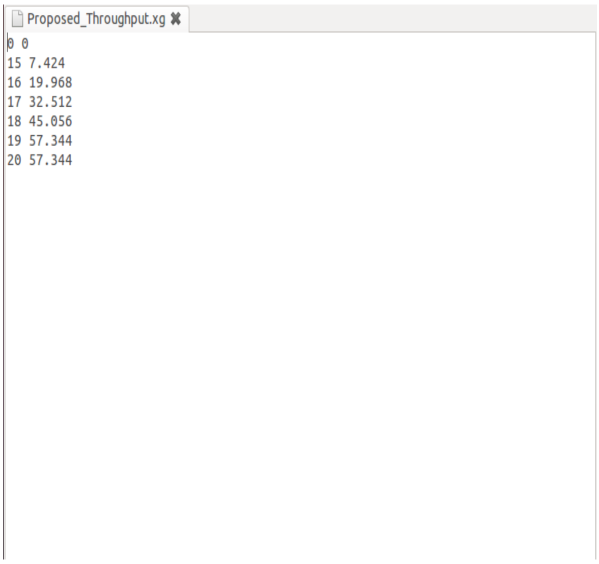
```
0 0
20 8.01319
```

Fig. 7: Proposed overhead



```
0 0
1 1
2 1
3 1
4 1
5 0.971014
6 0.956044
7 0.938596
8 0.918519
9 0.929032
10 0.936782
11 0.935484
12 0.937824
13 0.938462
14 0.939086
15 0.966292
16 0.978533
17 0.984085
18 0.986515
19 0.988696
20 0.988696
```

Fig. 8: Proposed Packet Delivery ratio



```
0 0
15 7.424
16 19.968
17 32.512
18 45.056
19 57.344
20 57.344
```

Fig. 9: Proposed throughput

DOI 10.17148/IJARCCE.2016.5278

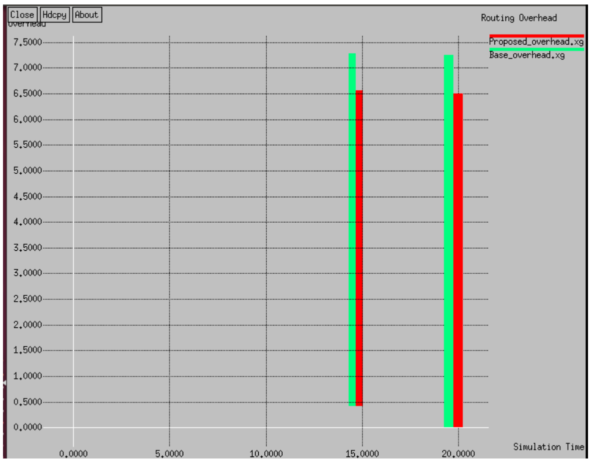


Fig. 10: Overhead graph

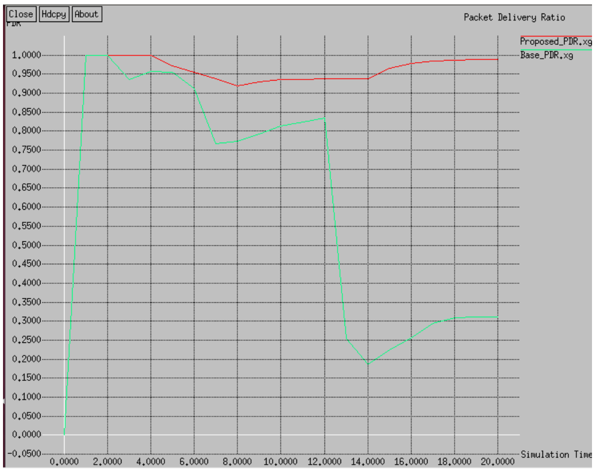


Fig. 11: Packet Delivery ratio graph

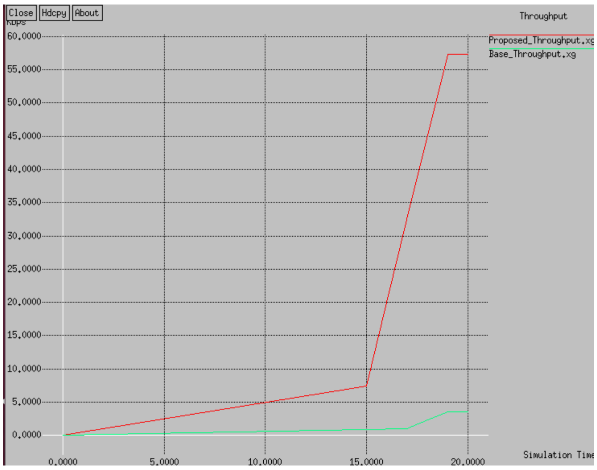


Fig. 12: Throughput graph

Table 1: Comparison table of parameters considered

Parameters	Base paper		Proposed	
(Simulation Time)	15	20	15	20
Overhead	7.3	7.25	6.6	6.5
Packet Delivery ratio	0.22	0.31	0.96	0.98
Throughput	0.7	3.58	7.4	57.34

VIII. CONCLUSION & FUTURE SCOPE

The main aim of this research is to propose a technique for detecting and preventing black hole attack in MANETs. A black hole attack is a node which is malicious that replies falsely for any RREQ having no active route to a particular destination and declines all its packets. A novel approach is proposed for detecting and preventing the black hole attack and the parameters considered in this approach are throughput, packet delivery ratio and overhead. This technique provided better results than the techniques which are already available.

REFERENCES

[1] Harjeet Kaur, Manju Bala, Varsha Sahni, “Study of Blackhole Attack using Different Routing Protocols in MANET”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 7, July 2013.

[2] Antony Devassy, K. Jaynthi, “Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting”, International Journal of Modern Engineering Research (IJMER), Vol. 2, Issue 3, pp. 1017-1021, May-June 2012

[3] Amol A. Bhosle, Tushar P. Thosar, Snehal Mehatre, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol. 2, No. 1, February 2012.

[4] Rashmi, Ameeta Seehra, “A Novel Approach for Preventing Black-Hole Attack in MANETs”, International Journal of Ambient Systems and Applications (IJASA), Vol. 2, No. 3, September 2014.

[5] Himani Yadav, Rakesh Kumar, “A Review on Black Hole Attack in MANETs”, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp. 1126-1131, May-June 2012.

[6] Jaspinder Kaur, Birinder Singh, “Detect and Isolate Black hole attack in MANET using AODV Protocol”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 3, Issue 4, February 2014.

[7] Neetika Bhardwaj, Rajdeep Singh, “Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs”, International Journal of Application or Innovation in Engineering & Management”, Vol. 3, Issue 5, May 2014.

[8] D.L. Mills, “Internet Time Synchronization: the Network Time Protocol”, University of Delware.

[9] Gurnal Singh, Gursewak Singh, “Detection and Prevention of Black Hole Using Clustering in MANET using NS2”, International Journal of Engineering and Computer Science, Vol. 3, Issue 8, pp. 7420-7430, August 2014.

[10] Disha G. Kariya, Atul B. Kothle, Sapna R. Hede, “Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method”, International Journal of Emerging Technology and Advanced Engineering, Vol.2, Issue 1, Januray 2012.

[11] Pooja Jaiswal, Dr. Rakesh Kumar, “Prevention of Black Hole Attack in MANET”, International Journal of Computer Networks and Wireless Commuincation (IJCNWC), Vol. 2, No. 5, October 2012.

[12] Nitesh A. Funde, P.R. Pardhi, “Detection & Prevention Techniques to Black & Gray Hole Attacks in MANET”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.

[13] Fan-Hsun Tsang, Li-Der Chou, Han-Chieh Chao, “A Survey of Black Hole attacks in wireless mobile and ad hoc networks”, Springer, 2011.

[14] Ekta Barkhodia, Parulpreet Singh, Gurleen Kaur Walia, “Performance Analysis of AODV Using HTTP traffic under Black Hole Attack in MANET”, Computer Science & Engineering: An International Journal (CSEIJ), Vol. 2, No. 3, June 2012.