**International Journal of Scientific Engineering and Research (IJSER)**
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 1, September 2013

# Removal of Black Hole Attack by Implementing Digital Signature and Trust Index Computation in Ad hoc Wireless Networks

**L. N. Jyothi Bhargavi[1], J. Girija[2]**

[1]Bangalore Institute of Technology,
V.V. Puram, Bangalore-560004, Karnataka, India

[2]Associate Professor, Computer Science Department,
Bangalore Institute of Technology, V.V. Puram, Bangalore-560004, Karnataka, India

**Abstract:** ***Ad hoc wireless networks are the infrastructure less networks. They consist of mobile nodes which move around the network within a given range. Ad hoc wireless networks are prone to attacks. Security is of utmost concern in such networks. One such threat is black hole attack. In black hole attack, a node or nodes exhibit malicious behavior by intercepting the packets and thus disclosing the confidentiality of the message being transmitted. In this paper, the black hole attack is detected and eliminated by modifying AODV protocol***.

**Keywords:** wireless networks, black hole attack, mobile nodes, AODV, RSA, trust index.

## 1. Introduction

A wireless ad hoc network is a decentralized type of wireless network. It consists of mobile nodes that move arbitrarily and thus they have no infrastructure. The nodes in the network move dynamically and join the network. This nature of the nodes makes them susceptible to malicious attacks. These attacks can be either passive attack or active attack. The passive attacks caused by malicious nodes without disturbing the network operation. The active attacks disturb the operation. The attacks take place when routing the control information and data. In ad hoc wireless networks each node acts as host as well as router [1].

Different routing protocols are used in ad hoc wireless networks to update the routing information. Proactive (or table driven), reactive (on demand) and hybrid routing protocols are used for ad hoc wireless networks. The routing attacks that affect the ad hoc wireless networks are: Attacks using Modification, Fabrication, Interruption, and Interception. In this paper we focus on Interception of the message caused by black hole attacks [2].

Ad hoc on-demand distance vector (AODV) routing, dynamic source routing (DSR ) and Destination sequence vector routing (DSDV) protocols are some of the routing protocols for ad hoc wireless networks. These protocols are affected by different security attacks. In this paper Black hole attack is detected and removed using AODV protocol.

Black hole attack is one of the severe attacks that come from misbehavior of the node. The remaining of the paper is organized as follows. The AODV protocol is described in section 2. The characteristics of the Black hole are described in section 3. Related work in section 4. Solution to black hole is in section 5. Simulation environment and results are analyzed in section 6. The last conclusion is in section 7.

## 2. Ad hoc on Demand Distance Vector Routing Protocol

Ad hoc on-Demand distance-Vector (AODV)[3] routing protocol uses on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence number to identify the most recent path. AODV works on the router request (RREQ)/route reply (RREP) query cycle. Route request packet (RREQ) is sent from source to destination node when route does already not exist between them. AODV uses a destination sequence number (DestseqNum) to determine an up-to-date path to destination. A node updating its path information only if the DestSeqNum of the current packet received is greater than the last destSeqnum stored at the node. In this case, a node unicast a RREP back to the source. If received RREQ is already processed simply they discard the RREQ and don't forward it. After receiving the RREP the source node send the data packets to the destination node. If source node later receives the RREP of greater sequence number or same sequence number with less hop count then the routing table is updated and uses the better route to destination [4].

## 3. Black hole attack

Malicious node in the network is called as black hole as shown in Figure 1. Black hole intercepts the packet and the confidentiality of the message is disclosed. In black hole attack, the malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives

RREQ, it immediately sends RREP with highest sequence number to the source before any other node sends RREP. Source node on receiving RREP with high sequence number, establishes route to black hole node and start transmitting packets assuming that the node knows the route to the sink node. Malicious node attack all RREQ messages this way and takes over all routes. In such attacks, all packets in the network are being sent to a point from where they are not forwarding to anywhere. This is called black hole, meaning which swallows all objects and matter.

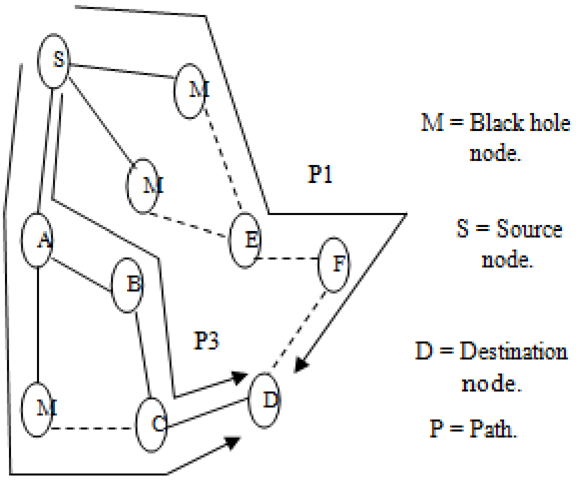


**Figure 1:** Example of black hole attack.

## 4. Related work

The authors in [4] have discussed a solution to black hole attack by modifying the AODV protocol. Here the RREP received at the source node is compared with the threshold value. If the sequence number is within the threshold value then the RREP is coming from valid node. If the sequence number in RREP is greater than threshold value then such node will be detected as malicious. This solution has increased delay. The authors in [1] discuss an approach in which the requesting node waits for the responses including the next hop details, from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated *next-hop-node* or not. If any repeated *next-hop-node* is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited in. The solution adds a delay and the process of finding repeated next hop is an additional overhead. In [5] authors propose a protocol that modifies the behavior of the original AODV by introducing a data structure referred as trust table at every node. This table is responsible for holding the addresses of the reliable nodes. The RREP is extended with an extra field called trust field. In order for a node to be added to the trust table of another node, it needs firstly to pass the behavioral analysis filter. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node. RREP is overloaded with an extra field to indicate the reliability of the replying node. The value of the trust field is initialized to zero by the replying node and might be modified by its previous hop during the trip of the RREP. The value of the trust field could be modified either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exist in the trust table. Upon the RREP is received by the source node, it decides whether to send the data or to wait for further route. In case the trust field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route. Although the proposed method gives reliable routes but it consumes high network delay. Authors in [6] suggest a solution to detect the black hole attack. This process does not change the normal working of the AODV. Here the process continues to accept RREP packets and calls a process called Compare_Pkts which compares the destination sequence number of the two packets. If the difference in the sequence numbers is significantly high, then an alert message containing node identification is generated and broadcasted to the neighboring nodes. Thus the malicious nodes are identified and excluded from the communication path. But this solution increases the network delay and cannot detect co-operative black hole nodes.

All solutions discussed above increase the delay considerably. They also involve additional overhead either on the intermediate nodes or destination node or both. Mobile nodes in MANETS suffer from limited battery life, processing power and storage. Therefore it is necessary to design a protocol such that it successfully detects and eliminates black hole attack with reduced overhead and delay.

## 5. Proposed solution to black-hole attack

In the proposed solution digital signature concept is implemented and trust index for the links is calculated by modifying the AODV protocol to detect black hole attack. RSA algorithm [7] is used to implement the digital signature concept. At source the RREQ is encrypted and forwarded to neighboring nodes. Only the node which knows the key to decrypt will decrypt correctly and generates RREP and sends it to source based on decrypted RREQ. Source checks if the RREP has come from valid node and computes the trust index of the link from which RREP has come from. Link to valid node gets high trust index where as the link to black hole gets low trust index. Based on the computed trust index, source node establishes route to the sink. If it has come from a valid node, then it establishes route to the sink. During packet transmissions when a node in the communication path becomes black hole, then the source determines an alternative path to the sink based on trust index of the links calculated. Black holes are excluded from the path. Links with low trust index are avoided in the path for transmission. Trust index of the link is calculated based on the number of correct transmissions among total number of transmissions through the link. The proposed solution is implemented as follows:

ISSN (Online): 2347-3878
Volume 1 Issue 1, September 2013

Step 1: Select two large prime numbers p and q such that p!=q.
Determine n = p*q
Determine Φ (n) = (p-1)*(q-1)
Determine e such that gcd (e,n)=1
Determine d.

Step 2: Construct RREQ.

Step 3: Encrypt RREQ. To encrypt using following
For i =0 till i<e
C=C*M mod n
Where C=1 (set initially) cipher text
M=RREQ constructed.

Step 4: Forward RREQ to the neighboring nodes.

Step 5: On receiving RREQ, if it is a valid node,

(i). Decrypt RREQ using the following
For i =0 till i<d
M = M*C mod n
(ii). Construct RREP based on RREQ
(iii). Encrypt RREQ as in Step 3
(iv). Forward RREP to source

Step 6: If RREQ is received by a black hole then black hole node,

(i). Generate RREP
(ii). Forward to source

Step 7: Check RREP at source on receiving RREP. This is done as follows:

(i). Decrypt the received RREP as in step 5.
(ii). If the RREP had come from a valid node, then RREP will be decrypted correctly. Set flag as 0 to indicate that RREP has come from a valid node.
(iii). Else, this means RREP has come a black hole. Set flag as 1 to indicate that RREP has come from a black hole.

Step 8: Compute the trust index of the link from which RREP has come from using the following formula:

Trust index = correct transmissions/total transmissions

Step 9: Establish connection from source to sink.

(i). Select the path based on the trust index of the links computed.
(ii). Exclude the black hole from the communication path.
(iii). Avoid links with the low trust index.
Step 10: if a node becomes black hole during transmission, repeat steps from 6 to 9.

## 6. Simulation of Black Hole Attack

We have done the simulation in NS2 [8]. We have made 5 nodes as black hole with a terrain area of 800 X 800. The simulation was carried with 10 nodes to 50 nodes with 5 nodes incrementing. The following parameters were considered for simulation.

**Table 1:** Simulation parameters

| *Parameters used* | *Values* |
|---|---|
| Simulator NS2(2.35) | |
| Simulation time | 1 ms |
| Number of nodes | 10 to 50 |
| Routing protocol | AODV |
| Traffic model | CBR |
| Terrain area | 800 X 800 |
| Black hole nodes | 5 |

The simulation was done to analyze the performance of the networks for various parameters. Different metrics are used to evaluate the performance of the network under black hole attack. We have considered the following metrics to analyze the performance of our solution.

- **Delay:** It is the time taken for the packets to transmit from source to destination.
- **Overhead:** This gives the ratio of routing related transmissions (RREQ, RREP, and RERR) to data transmission in a simulation.
- **Throughput:** It is the average rate of successful message delivery over a communication path.

We have got the following results after simulation.

**Table 2:** Delay under attack and after elimination of attack.

| *Nodes* | *Under attack* | *After elimination of attack* |
|---|---|---|
| 10 | 0.89 | 0.798 |
| 15 | 0.88 | 0.803 |
| 20 | 0.833 | 0.77 |
| 25 | 0.833 | 0.745 |
| 30 | 0.798 | 0.703 |
| 35 | 0.765 | 0.691 |
| 40 | 0.722 | 0.655 |
| 45 | 0.707 | 0.632 |
| 50 | 0.691 | 0.619 |

**Table 3:** Overhead under attack and after elimination of attack

| *Nodes* | *Under attack* | *After elimination of attack* |
|---|---|---|
| 10 | 5.92797 | 6.27744 |
| 15 | 5.82907 | 5.96962 |
| 20 | 5.92684 | 5.97883 |
| 25 | 5.92615 | 5.95469 |
| 30 | 5.93036 | 5.96976 |
| 35 | 5.92624 | 5.91307 |
| 40 | 5.92684 | 5.91341 |
| 45 | 5.92684 | 5.91345 |
| 50 | 5.92684 | 5.92187 |

**Table 4:** Throughput under attack and after elimination of attack

| *Nodes* | *Under attack* | *After elimination of attack* |
|---|---|---|
| 10 | 41.14 | 126.47 |
| 15 | 39.75 | 193.22 |
| 20 | 41.14 | 216.08 |
| 25 | 41.14 | 225.79 |
| 30 | 74.76 | 193.22 |
| 35 | 41.14 | 216.08 |
| 40 | 41.14 | 225.76 |
| 45 | 41.14 | 225.76 |
| 50 | 41.14 | 256.49 |

We have used Xgraph to analyze the result obtained. We can see in Figure 2 the delay being increased slightly for the solution. There is significant reduction in the overhead for the solution in Figure 3. Throughput has been increased significantly for the solution in Figure 4.

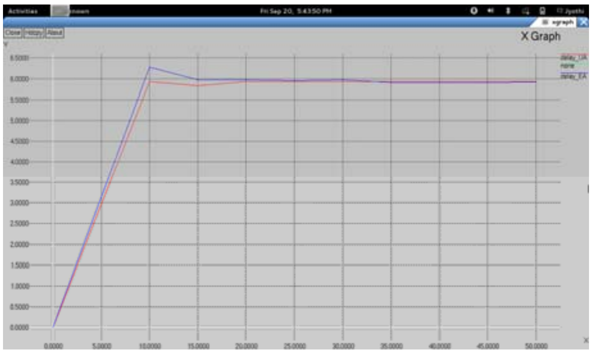


**Figure 2:** Delay v/s number of nodes

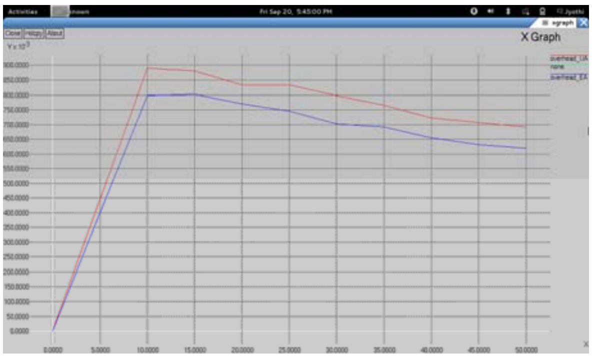


**Figure 3:** Overhead v/s number of nodes

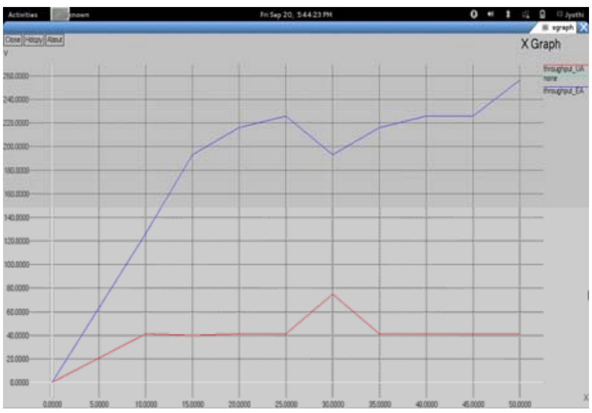


**Figure 4:** Throughput v/s number of nodes

## 7. Conclusion

In this study we analyze the effects of blackhole in ad hoc wireless networks. We have implemented a modified AODV protocol that simulates the behaviour of a blackhole in NS-2. In this method we have used digital signature and trust index computation to provide security in AODV against blackhole attack that causes the interception and confidentiality of the ad hoc wireless networks. The solution detects the blackhole nodes and excludes them from the communication path. From the graphs illustrated in results we can see that the performance of the solution. Our solution detects and eliminates the black hole attack with very little increase in delay and significant reduction in overhead and increase in throughput. Though the solution increases the delay, but this increase is negligible. Though the algorithm is implemented and simulated with AODV routing algorithm, we believe that the solution can also be used by other routing algorithm as well.

## References

[1] Latha Tamilselvan, Dr. V. Sankarayanan, "Prevention of Black hole Attack in MANET". The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless2007) India, 2007 IEEE.

[2] Mohammad O. Pervaiz, Mihaela Cardien Jie wu "Routing Security in Ad Hoc wireless Networks", Network Security, 2005 Springer.

[3] Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.

[4] A. Vani, and D. Sreenivasa Rao, " Removal of black hole attack in ad hoc wireless networks to provide confidentiality Security service", International Journal of Engineering Science and Technology (IJEST) Vol. 3, No. 3, March 2011

[5] Songbai Lu; Longxuan Li ; Kwok-Yan Lam ; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack ," Computational Intelligence and Security, 2009. CIS ' 09. International Conference on, vol .2, no., pp.421-425, 11-14 Dec. 2009.

[6] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A counter measure to Black hole attack on AODV-based Mobile Ad-Hoc Networks" International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 2011.

[7] Introduction to algorithms, Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, Eastern Economy Edition, 3rd edition.

[8] ns-2:http://www.isi.edu/nsnam/ns/

## Author Profile

**L. N. Jyothi Bhargavi** is a student of M.Tech (Computer Science and Engineering) in Bangalore Institute of Technology . Currently

pursuing her final semester, her area of interests includes Computer networks, Information security.

**J. Girija** B.E, M.Tech, is an Associate Professor, Computer Science and Engineering Department in Bangalore Institute of Technology. Her areas of interest include Selfish nodes in ad hoc networks, Information security, Artificial Intelligence, Image processing and Natural Computing.