



International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network

Vimal Kumar^a, Rakesh Kumar^b

^{ab}Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology

Gorakhpur, 273010, U.P., India

{vimalmnnit16@gmail.com, rkiitr@gmail.com}

Abstract: Security is an essential component for mobile ad hoc network (MANET). In order to provide security against attacker, researchers are working specifically on the security challenges in MANETs, and many techniques are proposed for secure routing protocols within the networks. Our proposed work presents a more efficient solution for detecting a black hole attack with less communication cost in the MANET, which is particularly vulnerable compared to infrastructure-based networks due to its mobility and shared broadcast nature. As an adversary can successfully deploy black hole attack in the network. It can be seen that proposed work is more secure than the existing solutions. We also compared its performance to standard AODV routing protocol. The experimental results show that the proposed approach is better than standard AODV.

Keywords: Black hole attack, Secure AODV, Mobile Ad hoc network

1. Introduction

Mobile ad hoc network is a collection of nodes that do not depend on any infrastructure to maintain the network connection. They may act as a source, destination or as a router. It also avoids a single point of failure due to its nature of dynamic topology. The routing protocol in a mobile ad hoc network (MANET) can be categorized into three categories, namely, table-driven/proactive, on-demand/reactive and hybrid one. They provide various

applications that includes, military application, disaster relief, collaborative and distributed computing, wireless sensor network (WSN), networks of visitors at airport, health and business. Development of a security protocol in ad hoc network is not an easy task due to its unique characteristics of ad hoc wireless network, namely, shared broadcast channel, insecure operational environment, lack of central administration, lack of association between nodes, limited availability of resource and physical vulnerability. An attacker can easily deploy the security attacks due to security breaches in the network [1, 2, 3, 4]. This paper is organized in the following four sections. Section 2 presents an overview of AODV routing protocol and blackhole attack. In sections 3, we discuss related work in the area. In Section 4, we propose the detection scheme for a black hole attack. In Section 5, we describe the performance evaluation. Finally, we conclude our proposed work in Section 6.

2. Background

2.1 AODV Overview: AODV is an on-demand/reactive routing protocol. In AODV, when a route to new destination needed, a source node broadcast a route request (RREQ) packet to find a route to the destination node. A valid route can discover when a RREQ reaches a destination node either itself, or an intermediate node with a fresh route to the destination node. A fresh route is a valid route entry for the destination node whose associated sequence number is greater than sequence number of RREQ packet. A route is made available by unicast a route reply (RREP) packet to a source node. A RREP packet is unicast by a destination or an intermediate node. When a link break in a route is detected, a route error (RERR) packet is used to notify other participating nodes [5].

2.2 Blackhole Attack: A malicious node uses the routing protocol (such as AODV) to advertise itself as having the shortest path to the destination node whose packets it wants to discard/replay packets. When an attacker receives RREQ packet, then they create a reply where an extremely short route is advertised. If the malicious reply reaches to a source node before the reply from a legitimate node, a forged route has been created. Once the attacker has been able to insert itself between source and destination node, it is able to do discard/replay packets passing between them [6]

3. Related Work

Mistry et al. [7] gave a solution, which provides security to against black hole attacks by modifying standard AODV routing protocol. It uses two main parameters, namely MOS_WAIT_TIME and Cmg_RREP_Tab table to counter blackhole attack. From the experimental results show proposed solution achieves a very good rise in packet delivery ratio (PDR) with acceptable rise in throughput.

Saetang et al. [8] proposed an approach to eliminate black hole attack by using Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol. Experimental results show that proposed solution achieves throughput improvement at about 47 %.

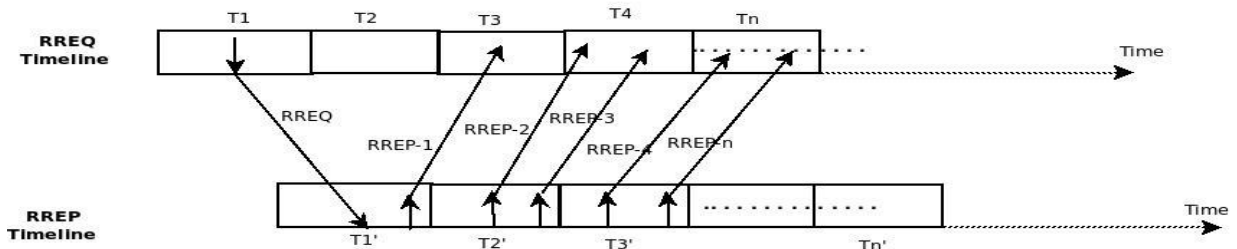
Sen et al. [9] gave a solution to detect a black hole attack in standard AODV protocol. One of the main advantages of proposed mechanism does not apply any cryptographic metrics. Instead, it protects ad hoc network by detecting and reacting to malicious activities of the intermediate nodes. Simulation results show that the technique has a significantly high detection rate with moderate network traffic hidden overhead and computation overhead.

Banerjee et al. [10] proposed an approach to protecting the mobile ad-hoc network from gray hole and black hole attack. They provide a technique to discover cooperating malicious nodes, which drop a significant fraction of packets.

Sharma et al. [11] tried to investigate the effects of blackhole attacks on mobile ad hoc network performance. Experimental results show network performance in the presence of a black hole is reduced up to 26%.

4. Proposed Methodology: The proposed solution is an enhancement of standard AODV routing protocol, which will be able to detect a black hole node in the network. In proposed approach, a coming route reply table (CRRT) added at the source node. A CRRT stores the RREP packet, which contains information about destination sequence number, next hop, hop count, originator IP address, destination IP address and lifetime. A source (S) node wants to

7



communicate with destination (D) node, they broadcast route request (RREQ) packet in the entire network.

Figure 1: RREQ packet and their corresponding RREP packets

Figure 1 shows two horizontal timelines: top line shows the times of a RREQ packet arrivals and bottom line shows the corresponding RREP packet arrivals. Time is slotted into fixed-length “observation intervals, “T1, T2,.....Tn. The corresponding observation intervals of RREP packet, T1', T2'.....Tn' are shifted to the right.

Collecting Route Replies: All incoming route replies are collected in a table namely, coming route reply table (CRRT). The entries will have fields like, source address, destination address, hop count, next hop, lifetime and destination sequence number. The route replies will be collected until an expiry time of RREP packet. This is shown in Figure 2.

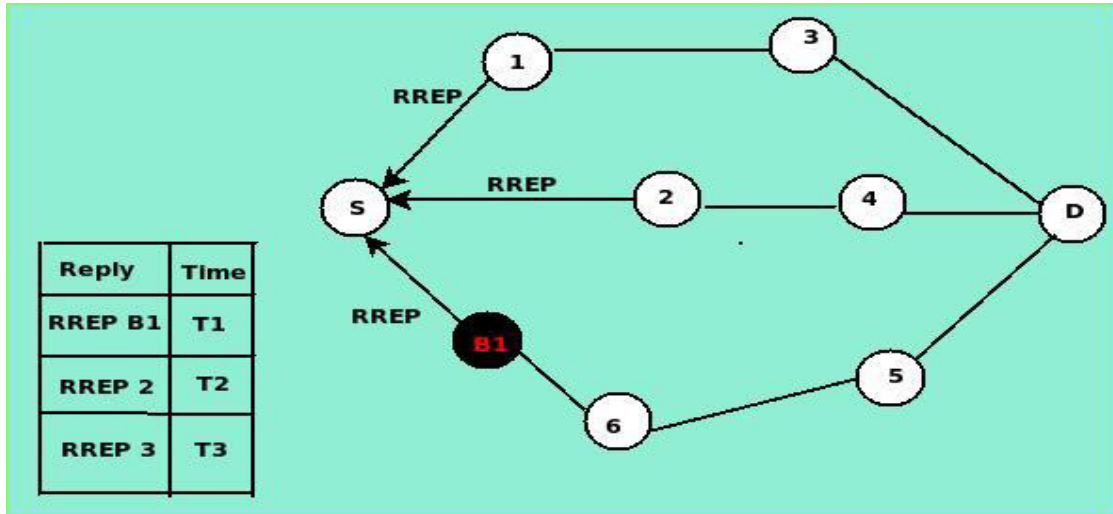



Figure 2: Collecting Route Reply

Detection Algorithm: The various notations used in the proposed algorithm is given in Table 1 while algorithm presents detection of black hole attack.

Table 1: Notations

RREQ_i	Destination sequence number of RREQ packet arrivals in the i^{th} observation interval
RREP_j	Destination sequence number of RREP packet arrivals in the j^{th} observation interval
D	Difference between destination sequence number of RREQ packet arrival in the i^{th} and destination sequence number of RREP packet arrival in the j^{th} interval
DS_RREQ_i	Destination sequence number of RREQ packet at i^{th} interval
DS_RREP_j	Destination sequence number of RREP packet at j^{th} interval
Th	Threshold value
CRRT	Coming route reply table

n	Number of replies
----------	-------------------

Algorithm: Detection of black hole attack 

```

Sum = 0
for each reply[ j ] do
    All incoming route replies are stored in a CRRT
    if ( DS_RREQ < DS_RREPj)
        Di = (DS_RREQ) – (DS_RREPi)
        Sum= Sum + Di

    end if
end for
Th = Sum / n
for ( j =1; j <= n; j++) do
    if ( Th < DS_RREPi) then
        Discard RREPi form CRRT /* RREPi packet is generated by black hole node */
    else
        h_count [ ] = h_counti /* choosing route for data transmission */
        sort array h_count[] in increasing order
        hop_value = h_count[0]
        Select a route corresponding to their hop_value
    end if
end for

```

Source (S) node must use defined threshold (Th) value to verify the selected destination sequence number of replying node. If the destination sequence number is greater than or equal to defined threshold value, it is treated as black hole node. Otherwise, it is legitimate node and it establishes a route to destination node using this destination sequence number. When it generates a RREP. The proposed algorithm provides better performance and high accuracy for detecting a black hole attacks in MANETs.

5. Performance Evaluation and Simulation Results

To evaluate the performance of proposed algorithm, we used NS-2 (v-2.34) network simulator. The simulations were conducted on Intel (R) Core (TM) I₅ processor at 2.40 GHz, 3 GB of RAM running Ubuntu 12.04 Linux. We use the IEEE 802.11 algorithm at the physical/data link layer. We use standard AODV reactive routing algorithm at network layer. Finally, user datagram protocol (connection-less) is used at the transport layer. The terrain area is 800m X 501m with 21 numbers of nodes varying from 10 to maximum 90 with varying speed from 10 m/s to 90 m/s.

Performance Metrics: The metrics used to evaluate performance of proposed approach:

Packet Delivery Ratio (PDR): It is defined as the total number of packets received by the destination node and total number of packets originated by source node.

Throughput: It is defined as the total number of packets or data bits successfully delivered at the destination in a given simulation time.

Simulation Results: We used the performance metrics to validate the proposed algorithm against black hole attack and the results shown in

obtained are Figures 3-6.

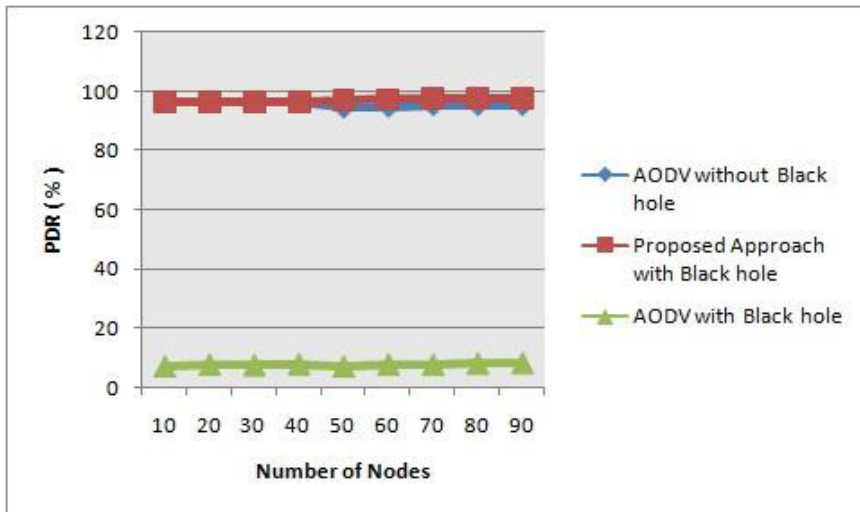


Figure 3: PDR (%) Vs Mobility (m/s)

Figure 3 shows the effect to the Packet Delivery Ratio (PDR) measured for the standard AODV protocol when node mobility is varying. It is measured that Packet Delivery Ratio of standard AODV is dramatically drop by 94.1 % when there is black hole nodes in the network, but Packet delivery Ratio increases by 96.3 % when our proposed algorithm is used in the presence of a node.

used in the black hole

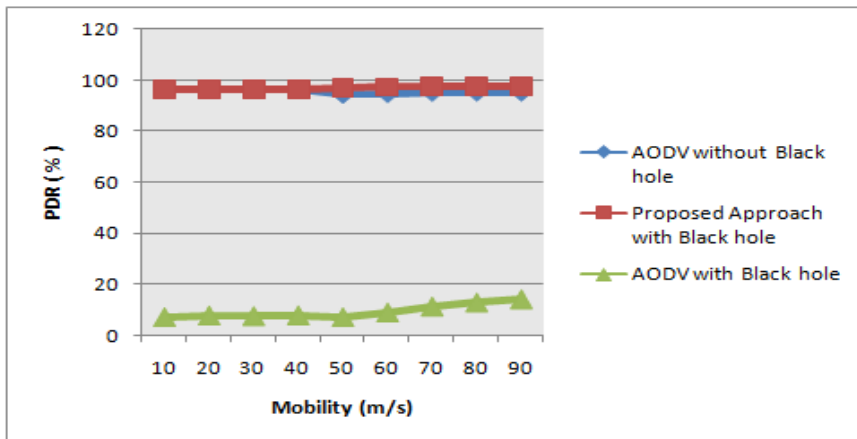
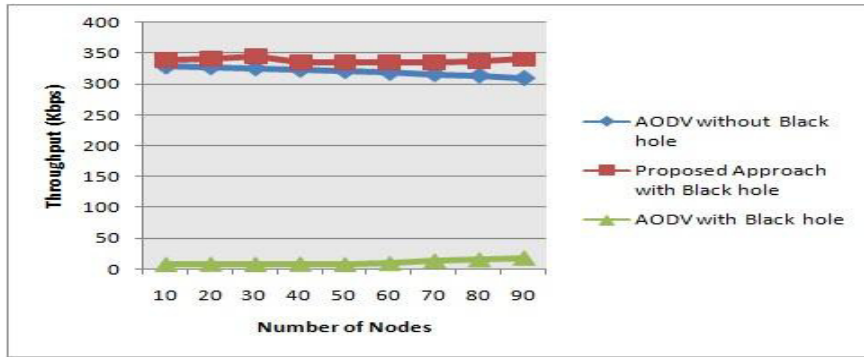


Figure 4: PDR (%) Vs Number of nodes

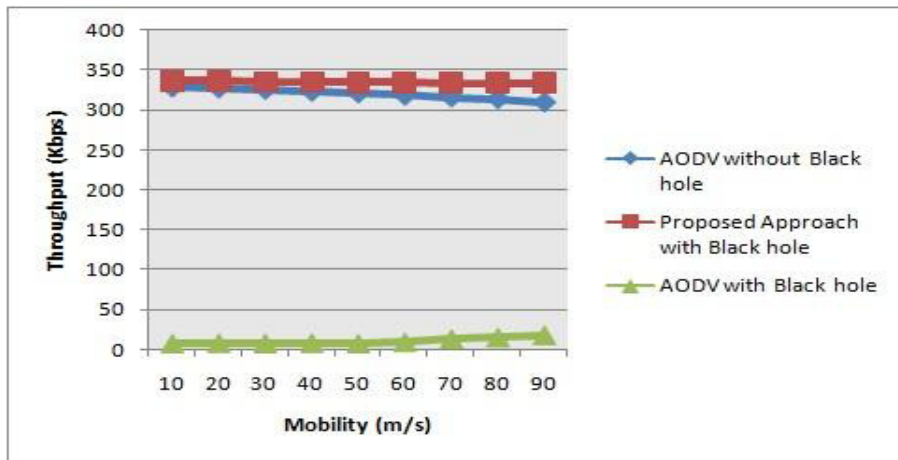
Figure 4 shows the effect to PDR the standard protocol when nodes are the network. It that PDR 95.2 in the black hole network, but algorithm increases by 97.4.



shows the measured for AODV number of varying in is measured drops by presence of a node in the proposed

Figure 5: Throughput Mobility (m/s)

Figure 5 shows to Throughput standard protocol when mobility is in the network. measured that Throughput of



(Kbps) Vs the effect of AODV node varying It is standard

AODV is dramatically drop by 310.13 kbps when there is a black hole node in the network, but Throughput increases by 333.9 kbps when our proposed algorithm is used in the presence of a black hole node.

Figure 6: Throughput (kbps) Vs Number of Nodes

Figure 6 shows the effect to Throughput of standard AODV protocol when number of nodes is varying in the network. It is measured that Throughput of standard AODV drops by 314.32 kbps in the presence of black hole node in the network, but Throughput increases by 336.14 kbps when our proposed algorithms used in the presence of a black hole node.

6. Conclusion

Black hole attack is one of most important issues in mobile ad hoc networks (MANETs). It can be seen that Packet Delivery Ratio and Throughput of standard AODV protocol decreases due to the presence of black hole node in the network. However, the overall performance of standard AODV protocol can vary dramatically when the network conditions change. Experimental results show that the proposed algorithm achieves a very good rise in Packet Delivery Ratio and Throughput. , we believe that proposed algorithm is an efficient solution for detection the black hole node in the network.

Acknowledgements: This research work is partially funded by the Technical Quality Improvement Programme Phase –II (TEQIP-II).

References

1. Claude Castelluccia, Nitesh Saxena, Jeong Hyun Yi. Robust self-keying mobile ad hoc networks. In: Proceedings of Elsevier Computer Networks, 2001, pp.143-161.
2. Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao. Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks. In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2010, pp.162-167.
3. Patroklos G. Argyroudi, Donal O Mahony. Secure Routing for Mobile Ad Hoc Networks. In: Proceedings of IEEE Communications Surveys and Tutorials, 2005, Third Quarter, Vol. 7, pp.2-21.
4. Yiu-Chun Hu, Adrian Perrig. A survey of secure wireless ad hoc routing. In: Proceedings of IEEE Security and Privacy, 2004, pp.28-39.
5. Lidong Zhou, Zygumt J. Haas. Securing Ad Hoc Networks. In: Proceedings of IEEE Network, Computer Communications, 211, pp.24-30.
6. Latha Tamilselvan, V Sankaranarayanan. Prevention of Co-operative Blackhole Attack in MANET. In: Journal of Networks, 2008, Vol. 3, No. 5, pp.13-20.
7. Nital Mistry, Devesh C Jinwala, Zaveri. Improving AODV Protocol against Blackhole Attacks. In: Proceedings of the IMECS 2010, Hongkong.
8. Watchara Saetang, Sakuna Charoenpanyasak. CAODV Free Blackhole Attack in Ad Hoc Networks. In: International Conference on Computer Networks and Communication Systems (CNCS 2012), 2012, pp.63-58.
9. Jaydip Sen, Sripad Koilakonda, Arijit Ukil. A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks. In: Proceedings of IEEE International Conference on Intelligent Systems, Modelling and Simulation, 2011, pp.338-343.
10. Sukla Banerjee. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. In: Proceedings of the World Congress on Engineering and Computer Science 2008, San Francisco, USA.
11. Sheenu Sharma, Roopam Gupta. Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks. In: Journal of Engineering Science and Technology, 2009, Vol. 4, No. 2, 243 – 250.