© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Secure Routing and Intrusion Detection Analysis of Black Hole Attack on MANETsUsing NS-2

Sourabh Tilthiya, Dr. Sanjay Kumar Sharma

Department of Electronics and Communication, Research Scholar, UIT-RGPV-Bhopal, Madhya Pradesh, India

ABSTRACT

Wireless networks are gaining popularity to its peak today, as the user's wants wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It's an analogy to that of the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack others nodes and networks knowing that it has the shortest path [4]. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed.Previously the works done on security issues in MANET were based on reactive routing protocol like Ad Hoc on Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET.

Keywords: MANET, BlackHole, Routingprotocols

I. INTRODUCTION

In today's fast and rapidly growing world of technologies MANET can turn the dream of networking at any place and at time into reality. We are almost there by the way such as Bluetooth enabled mobile phones such as 3G. MANET provides lots of feature and now more and more businesses understand the advantages of usage of computer networking. Depending on the firm's size and resources it might be a small LAN containing only a few dozen computers; however in large corporations the networks can grow to enormous and complex mixture of computers and servers. A computer network is a system for communication between two system and computers. These networks may be fixed (permanent) or temporary. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless.

Infrastructure-less Networks

In any but the most trivial networks (point-to-point links), some mechanism is required for routing the packets from the source to the final destinations. This includes discovery and maintenance of routes along with associated costs. In what is called an 'infrastructure based' wireless network, the job of routing is assigned to dedicated nodes called access points (AP). Configurations of the APs are much less dynamic than there, possibly mobile, end-point nodes. APs are like base stations which keep track of nodes' associations/disassociations, authentication etc. and control the traffic flow between their clients as well as between fellow APs. The AP may also be connected to the Internet thereby providing Internet connectivity to its clients. A very attractive and promising category of wireless networks that has emerged is based on an Ad Hoc topology; these networks are called Wireless Ad Hoc Networks. The term wireless network implies a computer network in which the communication links

are wireless. The term Ad Hoc comes from the fact that there is no fixed infrastructure for forwarding/ routing the packets. Figure 1. [2] shows an infrastructure-based and an Ad Hoc wireless network.

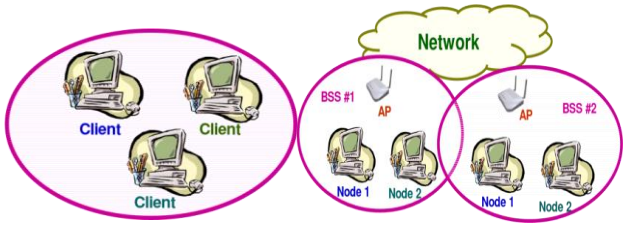


Figure 1. Ad Hoc and Infrastructure Network Topologies

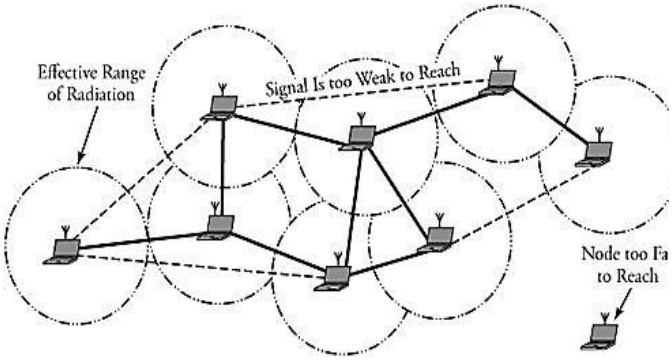


Figure 2. A Typical MANET

A typical MANETs (Mobile Adhoc Networks) is shown in Fig 2 [6]. The circles indicate communication ranges of individual nodes. In the real-world, this boundary is never likely to be a perfect circle and the links in fact can even be unidirectional in many cases – node 'A' can reach node 'B' on link 1 but node 'B' may not be able to use this link to reach node 'A'. This can happen due to the signal strengths of the two transmitters being unequal or can even be based on the transmission path.

In Ad Hoc networks, each node is willing to forward data to other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to the infrastructure-based networks in which designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make Ad Hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc. An Ad Hoc network is formed for a purpose by participating wireless nodes and is then torn off.

These networks introduced a new art of network establishment and are well suited for environments where either the infrastructure is lost or where deploying an infrastructure is not cost-effective.

II. METHODS AND MATERIAL

A. AIMS and Objectives

Aims and objectives of this thesis work are summarized as follow

- The study focus on analysis of black hole attack in MANET and its consequences.
- Analyzing the effects of black hole attack in the light of Network load, throughput and End to End delay in MANET.
- Simulating the black hole attack using Proactive and Reactive routing protocols.
- Comparing the results of both Proactive and Reactive protocols to analyze which of these two types of protocols are more vulnerable to Black Hole attack.

Previously proposed plans are suggested for counter measurement of Black Hole attack.

B. Black Hole Attack in MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in MANET" on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile ad hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

Black hole attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

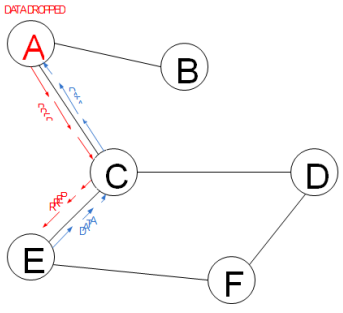
This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the

chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value
   - is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest
   - available node which belongs to the active route. This can also be send directly to the data source node if route is available.
   -
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing
   - table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.



C. Intrusion Detection AODV (IDAODV)

In this chapter we propose and discuss IDAODV, an Intrusion Detection mechanism for Wireless Mobile Ad Hoc Networks. IDAODV is based on State Transition Analysis Technique, which was initially developed to model host-based and network-based intrusions in a wired network environment.

Of all the routing protocols proposed for MANETs, AODV has been very popular and has become an Internet standard. This also has been the reason for AODV becoming more and more vulnerable to attacks. The AODV routing protocol was described. Our IDS has been designed on top of this protocol.

✓ **Problem Statement/ AODV Routing Attacks**

AODV presents many opportunities to attackers. We first identify a number of misuse goals that an inside attacker may want to achieve [32]. The misuse goals can be one or more of the following:

Route Disruption: Route Disruption means either breaking down an existing route or preventing a new route from being established.

Route Invasion: Route invasion means that an inside attacker adds itself into a route between two endpoints of a communication channel.

Node Isolation: Node isolation refers to preventing a given node from communicating with any other node in the network. It differs from Route Disruption in that Route Disruption is targeting at a route with two given endpoints, while node isolation is aiming at all possible routes.

Resource Consumption: Resource consumption refers to consuming the Communication bandwidth in the network or storage space at individual nodes. For example, an inside attacker may consume the network bandwidth by either forming a loop in the network.

Details of IDAODV: We now describe the details of the design and implementation of the proposed IDAODV. IDAODV detects attacks against the AODV routing protocol in Wireless Mobile Ad Hoc Networks. The components of IDAODV are discussed in the following sections.

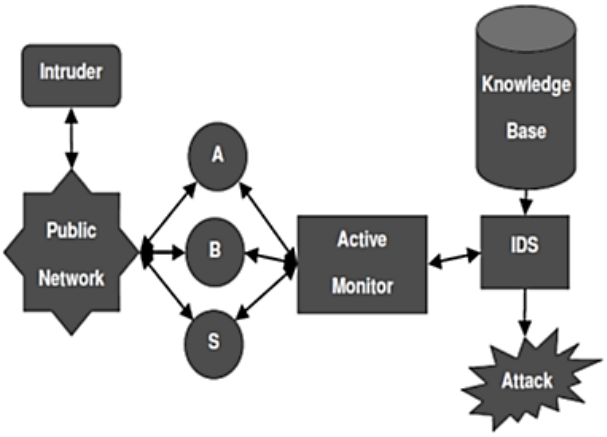


Figure 4. Architecture of IDAODV

✓ **Assumptions**

The following assumptions have been made for the algorithms.

1. ∀ **Pi, Pj∈ P, Pi ⊄Pj**
   e.g. if P_1 = {A, B, C} and P_2 = {A, B, C, D}, remove P_1
2. ∀ **Pi, Pj∈ P, Pi[|Pi| - 1] ∉Pj, |Pj|**
   e.g. if P_1 = {A, B, C} and P_2 = {A, B, D, E}, remove C from P_1
3. ∀ **Pi ∈ P, |Pi| > 1**

✓ **Algorithm 1: Detection of Routing Packets Dropped**

- Check a path from the farthest node to the nearest
- ∀ p ∈ P, check p[|p|]
- If an ACK is received ∀ v ∈ p and v ≠ p[|p|], v is *Good*
- Otherwise, check p[|p| - 1]
- If an ACK is not received from p[i+1] but received from p[i], 0 ≤i< |p|, select p[i]

✓ **Algorithm 2: Node Selection**

If p[i] is responsive but p[i+1] is not, there are three possibilities:

- p[i] is *Bad*
- p[i+1] is *Lost*
- The link p[i+1] → p[i] is broken

- Search next shortest path, p_a, to p[i+1] without going through p[i]
- If p[i+1] is responsive, check p[i] over p_a→ p[i+1] → p[i]. If p[i] is responsive, p[i] is *Bad*. Otherwise p[i+1] → p[i] is broken

✓ **Simulation**

The experiments were simulated using NS-2. The following section details the simulation environment, metrics and the results.

✓ **Simulation Environment**

- **Grid Size:** 1000x1000 Meters
- **Packet Traffic:** 10 Constant Bit Rate (CBR) Traffic connections were generated simultaneously. Four nodes were the sources for two streams each, and two nodes were the sources for a single stream each. Destination nodes only receive one CBR stream each.
- **Nodes:** A total of 30 nodes were simulated. Of these, 16 were communicating. Number of bad nodes was varied through the simulation.
- **Mobility:** Random waypoint model was chosen with maximum seed set to 20 meters per second. Pause time was set to 15 seconds.
- **Routing Protocol:** AODV
- **MAC Layer:** 802.11, peer-to-peer MAC Layer model was used.
- **Radio:** We used the 'no fading' radio model with the radio range set to 250 meters.
- **Simulation Time:** 900 Seconds
- **Dropped Packet Timeout:** Timeout period was set to 10 seconds
- **Dropped Packet Threshold:** Set to 10 packets
- **Clear Delay:** Set to 100 seconds, this is an event expiration timer. This is the amount of time for which a node would consider an event before arriving at a conclusion.
- **Modification Threshold:** Set to 5 events
- **Neighbor Hello Period:** Set to 30 Seconds.

For the performance measure of IDAODV, we consider the following metrics: False Positives, Detection Rate and Packet Delivery Ratio in both static and mobile conditions. All results are averaged over a number of simulation runs.

III. RESULTS AND DISCUSSION

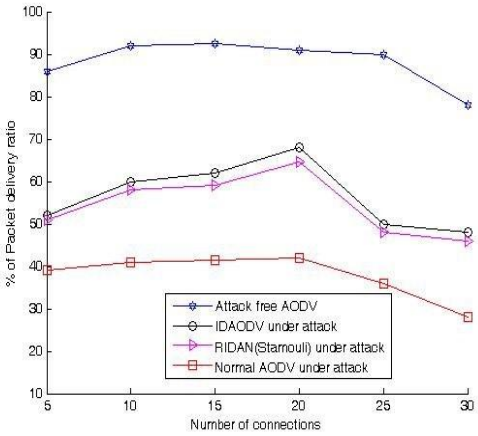


Figure 5: Delivery Ratio vs. Number of Connections

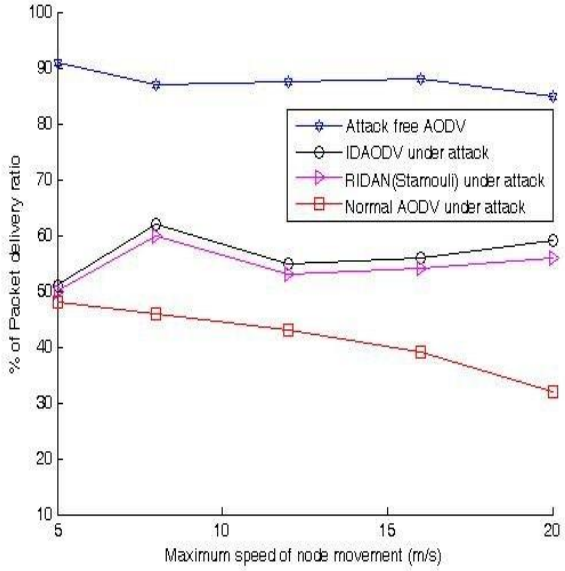


Figure 6: Delivery Ratio vs. Speed of Nodes

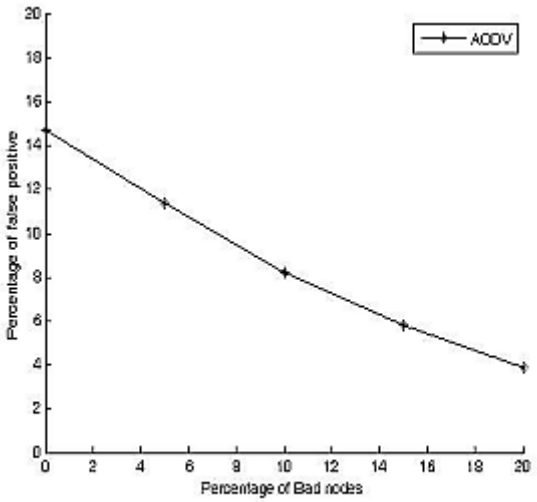


Figure 7. percentage of False Positives Vs. percentage of bad nodes

Response to Intrusions:our intrusion detection protocol allows for either an active or passive response to intrusions. With either response mode, the outcome is the isolation of the offending node from the network. In the passive mode, a node makes a unilateral decision based on its own observations of anomalous behavior. The more frequent and abnormal the behavior on the part of the malicious node, the sooner the intrusive node will be isolated and denied access on the underlying network infrastructure. The active response mode offers a higher level of assurance than does the passive mode. The increased assurance level is due to a majority voting scheme and consequently, the flooding of the intrusive node's identity throughout the network. The active mode, however, is more complex to implement.

Passive Response Once the *threshold value* which mitigates the effects of link error for message misrouting or message modification has been exceeded, an alarm is raised. In the passive mode, the node that raised the alarm removes the intrusive node from its neighbor table and does participate in further *route discoveries, Hello Messages* or collaborative routing with the intrusive node. Additionally, the intrusive node's address is recorded in the *Bad Node Table*. As we show in a later section on details of experiments, the denser the network, the more the number of nodes simultaneously declaring a node intrusive and preventing the malicious node from utilizing the network resources. If the node in question continues to act intrusively, each node in the network will eventually make a unilateral decision to disassociate itself with the intruder.

Improvements The simulations using NS-2 have shown that AODV versions that use link layer support has the overall best results in almost all simulations. AODV has, as mentioned earlier, the advantage that it learns more information for each request it sends out. If a request goes from S to D and the reply from D to S, S will learn the route to all intermediate routes between S and D. This means that it is not necessary to send out as many requests as, for AODV. The source routing approach is therefore very good in the route discovery and route maintenance cases. However, source routing is not desirable to use for data packets. First of all, it adds a lot of overhead. Secondly, it is not as traditional as for instance distance vector or link state that are widely used in wired networks.

Our proposal is therefore to implement a protocol that is a combination of source routing and distance vector. Source routing should be used in route discovery and route maintenance phases. These phases would also include that the routing tables are set up dynamically during the propagation of the requests and replies. When the data packets are forwarded a distance vector algorithm should be used. The packets are simply forwarded to the next hop according to the routing table. This, in combination with that the protocol stores several routes for each destination,

would probably mean a protocol with a performance that is even better than the protocols that have been simulated.

IV. CONCLUSION

An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification-based technique. It is based on a previous work done by Stamouli et al [10]. The IDS performance in detecting misuse of the AODV protocol has been discussed. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. From the results obtained, it can be concluded that our IDS can effectively detect Sequence Number Attack, Packet Dropping Attack and Resource Depletion Attack with Incremental Deployment. The method has been shown to have low overheads and high detection rate. Our Intrusion Detection and Response Protocol for MANETs have been demonstrated to perform better than the ones proposed by Stamouli et al in terms of false positives and percentage of packets delivered. Since Stamouli et al do not report true positive i.e. the detection rate, we could not compare our results against that parameter with their method. The implementation of the IDAODV protocol has shown its feasibility to work in real life scenarios; IDAODV performs real-time detection of attacks in MANETs running AODV routing protocol. The prototype has also given some insight into the problems that arise when trying to run real applications on an Ad Hoc network.

Simulation results validate the ability of our protocol to successfully detect both local and distributed attacks against the AODV routing protocol, with a low number of false positives. The algorithm also imposes a very small overhead on the nodes, which is an important factor for the resource-constrained nodes.

V. FUTURE WORK

- The work can be extended to study the robustness of Wireless Ad Hoc Networks for all types of protocols.
- A study can be conducted on the relationship between the average detection delay and the mobility of the nodes.
- More types of attacks including group attacks can be studied and their relations to the vulnerability of the protocols can be ascertained.
- A complete system can be designed to implement intruder identification.
- A complete approach can be developed that considers more parameters such as the available queue length and the delay on a path during the route determination. In order to avoid traffic fluctuation, randomness can be introduced into route determination.
- A fast response mechanism (local repair) can be developed for proactive protocols to reduce packet drop due to route changes.

VI. REFERENCES

[1]. Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002,. 3–13.

[2]. X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report,Computer Science, Iowa State University, 2005.

[3]. J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV.di.ionio.gr/medhocnet07/wp content/uploads/papers/90.pdf, 2007.

[4]. S. Kurosawa, H. Nakayama, and N. Kato, "Detecting blackholeattackon AODV based mobile ad-hoc networks by dynamic learning method,"International Journal of Network Security, pp. 338–346, 2007.

[5]. K. Makki, N. Pissinou, and H. Huang, "Solutions to the black holeproblem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.

[6]. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

[7]. Opnet Technologies, Inc. "Opnet Simulator," Internet: www.opnet.com, date lastviewed: 2010-05-05

[8]. M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad-HocNetworks," ACM Southeast Regional Conf. 2004.

[9]. Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[10]. Al-Shurman M, Yoo S-M, Park S , " Black Hole Attack in Mobile Ad Hoc Networks". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[11]. Djenouri D, Badache N, "Struggling Against Selfishness and Black Hole Attacks in MANETs", Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[12]. Chang Wu Yu, Wu T-K, Cheng RH, Shun chaochang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[13]. Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.