

Detection of Blackhole Attack using AODV Protocol in MANET

Manupriya

M. Tech., Vaish College of Engg, Rohtak (Haryana)
manupriya.dua@gmail.com

Abstract

Security is a major challenge in Mobile Ad hoc Network (MANET) due to their features of dynamically changing topologies, frequent host movement, Multi-hop wireless links and lack of clear line of defense. Protecting the network layer of a MANET from malicious attacks is an important and challenging issue. This paper analyzes the black hole attack which is one of the possible attacks in Mobile Ad hoc Network (MANET). In a black hole attack, malicious nodes advertise itself by sending a false route reply packet to a source node that initiates a route discovery process and drops all packets. Ad hoc On-demand Distance Vector (AODV) routing algorithm is used in simulation of black hole attack. Results are analyzed using Network Engineering Tool NS-2 in CYGWIN environment.

Keywords: Blackhole Attack, AODV Protocol, MANET.

1. Introduction

Mobile Ad hoc Network (MANET) is one of the current active fields and has received impressive consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and supportive environment of wireless network. As a result they focused on problems such as wireless channel access and multi-hop routing. But security has become a primary concern to provide sheltered communication between mobile nodes in an aggressive environment [1]. A Mobile Ad hoc Network (MANET) is a self configuring infrastructure less network of mobile nodes connected by wireless links. Each node in a Mobile Ad hoc Network (MANET) is free to move autonomously in any direction and will therefore adjust its links to other devices frequently [2]. There are five Major security goals that need to be addressed in order to maintain a consistent and safe ad-hoc network environment. They are namely: Confidentiality, Availability,

Authentication, Integrity and non-repudiation [3].

MANETs are vulnerable to various types of attacks. These include active interfering, passive eavesdropping, denial-of-service and impersonation. Intrusion prevention measures such as strong authentication and unnecessary transmission can be used to improve the security of an ad hoc network. However, these techniques can address only a subset of the attacks. Moreover, they are costly to execute. The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which examine security status of the network and identify malicious behavior [5].

Different types of routing protocols have been developed for ad hoc networks and have been classified into two main categories by Royer and Toh (1999) as Proactive (periodic) protocols and Reactive (on-demand) protocols. In a Proactive routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always recognize a recent route to all destinations. In a reactive protocol on the other hand, nodes exchange routing information only when needed, with a node attempting to determine a route to some destination only when it has a packet to send to that destination [1]. In this paper, we use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV) routing for analysis of the black hole attack when the destination sequence number are changed via simulation [4].

2. Existing Work

2.1 IDS Approaches for MANET

Intrusion is defined as “any set of actions that attempts to negotiate the confidentiality, integrity or

availability of resources". Intrusion detection systems (IDS) are mainly used to detect and call attention to apprehensive behavior. The first intrusion detection model was developed in 1987 in which Denning proposed a model based on the hypothesis that security violations can be detected by monitoring a system check records for abnormal patterns of system usage [6]. In 2007, Satoshi Kurosawa analyzed the black hole attack and introduced the feature in order to define the normal state of the network. They have presented a new detection method based on dynamically updated training data. Through the simulation, their method shows significant effectiveness in detecting the black hole attack [4]. In 2009, Payal N.Raj and Prashant B.Swadas proposed a work on "A Dynamic Learning System Against Black hole attack in AODV based MANET" their prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbors. Their solution DPRAODV increases PDR with minimum increase in Average-End-to-end Delay and normalized Routing Overhead [1]. In 2010, Nishant Sitapara, tries to eliminate the black hole effect at the route determination mechanism of the AODV Protocol that is carried out before the nodes start the packets [7]. In 2012, Poonam Yadav works on "A Fuzzy based Approach to detect black hole attack". The fuzzy rule is implemented on response time of node communication. Now instead of transferring data on this node, it will be passing on from the surrounding nodes; it will only handle the transmission that is directed to it only. The algorithm will provide the better solution for reducing the data loss over the network [8]. In 2012, Kamini Maheshwar and Divakar Singh proposed a work, on IDS approach which introduces algorithms for data processing which checks the network normal and abnormal behavior of the network is presented, first they create normal profile table then they apply algorithm for data filtering and filter the resultant part if any mislead happens in the network so node work as loop condition that means no any data receives by the genuine receiver and also work on IPS module in which they implement IPS) and call by the TCL(Tool Command Language) script in this case they internally design the algorithm for prevention of the network through the black hole behavior, IPS node acknowledge the sender node for miss-happen in the routing and also block the black hole node. All the work done under the AODV routing protocol and mobile ad-hoc network and one

node created as IPS node and the network behavior through number of various parameter are analyzed [9]. In Year 2013, Mohan K Mali¹, Pramod A Jadhav performed a work, "Review of DDoS and Flooding Attacks in MANET". In this work, we introduce dynamic counter-based broadcast technique for detecting and controlling flooding attack, average distance estimation technique for detecting and rate limiting technique for controlling DDoS attack. Dynamic counter-based technique proposed to reduce redundant rebroadcasts in order to overcome the "broadcast storm problem" [10].

3. Proposed Work

In this present work, the current node and the neighboring nodes are been analyzed under the different analysis vectors. In this work we have taken two main vectors called Packet Forwarding Ratio and the Packet Delay. Once these all vectors are defined, the node with higher packet forwarding ratio and minimum delay value will be selected as the next communicating nodes. In the same way, the node having the maximum probabilistic loss and the maximum probabilistic delay will be taken as the bad node. The communication over this node will be terminated temporarily for the current session.

Forwarding Ratio (FR)

It is the proportion of the number of packets forwarded correctly to the number of those supposed to be forwarded. Correct forwarding means a forwarding node not only transmits a packet to its next hop node but also forwards devotedly. For instance, when a malicious neighbor node forwards a data packet after tampering with data, it is not considered as correct forwarding. If the sender monitors this illegal modification, the forwarding ratio of this neighbor will decrease.

Algorithm:

Algorithm (Nodes,N){

- (i) Design a network with N number of nodes.
- (ii) Define the source and the destination node
- (iii) Perform the communication between source and Destination
- (iv) While Source <> Destination

- | | | | |
|--------|---|--------|---|
| (v) | { | (xi) | Paramter2=PacketDelay |
| (vi) | Generate the List of NeighborNode called NList | (xii) | } |
| (vii) | For i=1 to Length(NList) | (xiii) | If (High (Parameter1) and Low (Parameter2)) |
| (viii) | Get PacketForwardingRatio and Delay on each neighbor Node | (xiv) | {Set NList(i) as Next Communicating Node} |
| (ix) | { | (xv) | Move to Next Node |
| (x) | Paramter1=PacketForwardingRatio | (xvi) | End |

4. Results

The presented work is implemented in NS2 environment. The simulation is performed under a Mobile Network Scenario. The Scenario taken for the work is shown as under in table 1.

Table 1: Simulation Parameters

Parameters	Values
Simulator	NS-2
Number of Nodes	50
Topography Dimension	500x500
Protocol	AODV
Interval	.01
Traffic Type	CBR
Simulation Time	20 sec

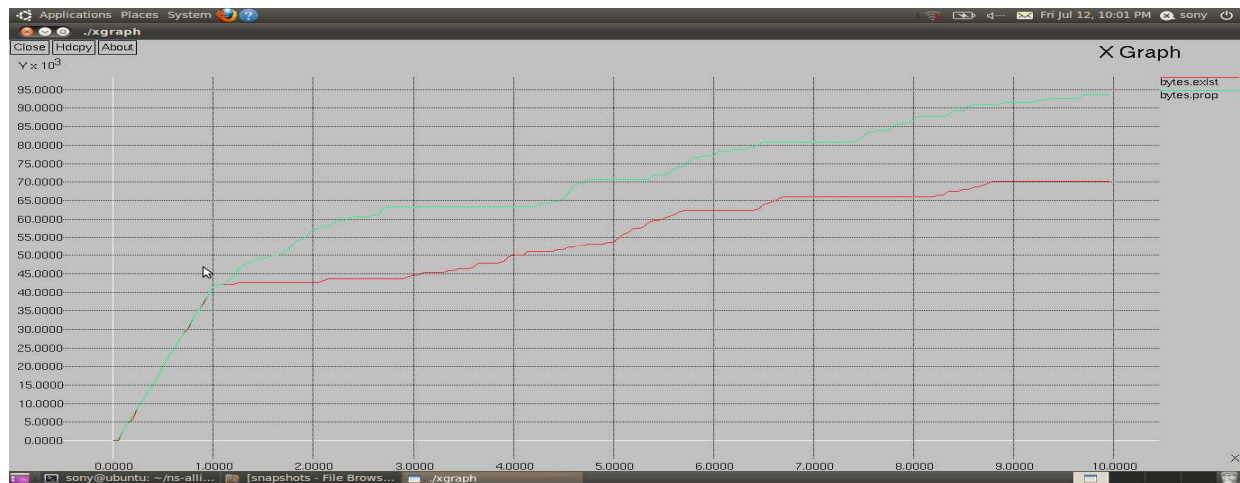


Figure 1: Packet Forwarding Ratio (Existing Vs Proposed)

Here fig 1 is showing the comparison of proposed work with existing protocol transmission under the heavy traffic. As we can see, the green line is showing the packet forwarding ratio in case of proposed work and red line is showing the bytes

transmission in existing approach. X axis is showing the simulation time. As we observe that the proposed work has improved the Packet forwarding ratio up to an extent.



Fig 2: Packet Delay (Existing Vs Proposed)

Here fig 2 is showing the comparison of proposed work with existing protocol under the heavy traffic. As we can see, the green line is showing the packet delay in case of proposed work and red line is showing the delay in existing approach. X axis is showing the simulation time. As we observe that the proposed work has reduced the delay over the network.

4. Future Scope

The proposed system can be enhanced in future by other researchers in the following ways:

1. We have worked only with AODV protocol. The work can be implemented and analyzed along with other protocols.
2. We have performed the work only with Black Hole attack, the work can be enhanced by implementing some other attack such as worm hole, flooding attacks, DOS etc.

References

- [1] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET", IJCSI

- International Journal of Computer Science Issues, Vol. 2, 2009
- [2] M.A. AL-SHABI, "ATTACKS AND DEFENSE IN MOBILE ADHOC NETWORKS (MANETS)", International Journal of Reviews in Computing, 31st December 2012. Vol. 12
- [3] PRADIP M. JAWANDHIYA, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071
- [4] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vol.5, No.3, PP.338-346, Nov. 2007
- [5] Jaydip Sen, "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks".
- [6] Kamini Maheshwar; Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment" European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90
- [7] Nishant Sitapara, Prof. Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks
- [8] Poonam Yadav, Rakesh Kumar Gill, Naveen Kumar, "A Fuzzy Based Approach to Detect Black hole Attack", International Journal of Soft

Computing and Engineering (IJSCE) ISSN:
2231-2307, Volume-2, Issue-3, July 2012

- [9] Kulbhushan, Jagpreet Singh, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET". IJCA Special Issue on "Network Security and Cryptography" NSC, 2011
- [10] Mohan K Mali, Pramod A Jadhav, "Review of DDoS and Flooding Attacks in MANET" International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 5, May 2013