Detection and Prevention for Avoidance of Energy Draining Vampire Attack in MANET

Sandeep Singh
Department of CSE, Patel College of Science & Technology, Indore, Madhya Pradesh, India

Pritesh Jain
Asst Professor, Department of CSE, Patel College of Science & Technology, Indore, Madhya Pradesh, India

DOI: 10.23956/ijarcsse/SV7I5/0200

Abstract—A mobile ad-hoc (MANET) network is a temporary, infrastructure less network where nodes communicate without any centralized mechanism. This dynamic behaviour of MANET makes this network applicable in conference, battlefield environment and disaster relief, and has received significant attention in recent years. Attacker may use this weakness to break the network. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network. The objective of work is to detect and prevent mobile ad-hoc network from power draining causes by Vampire attack. Here, Targeted Flooding through high battery capacity node has been used to deploy Vampire attack in mobile ad-hoc network. Subsequently, energy consumption and capacity observation technique has been used to detect malicious node(s). Furthermore, prevention method detect malicious nodes and prevent communication.

Keywords—Mobile ad-hoc Networks, Vampire Attack, AODV, E2E, PDR

I. INTRODUCTION

A mobile ad-hoc network is a temporary, infrastructure less network where nodes communicate without any centralized mechanism. This dynamic behaviour of MANET makes this network more potentially applicable in conference, battlefield environment and disaster relief, and has received significant attention in recent years. Due to open nature communication medium, it becomes more vulnerable to outside attacks. Security threats are classified in two category passive and active attacks. In passive attack attacker can listen the packets in the network while in the active attack attacker can also modify the packet contents. Subsequently, little attack may lie into both categories. Poor resources availability is the major weakness of wireless Ad-Hoc network. Attacker may use this weakness to disrupt the network. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network.

Vampire attack is energy draining attack where messages send by the malicious node which causes more energy consumption. This energy consumption is very high and leading to slow depletion of network node’s battery life. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, so it takes large energy to transmit the data and consumes the node energy. Since Vampires use protocol-compliant messages, and because of this, detection and prevention are very difficult in this attack. Two types of Vampire attack are as follows:

Carousel Attack

Carousel attack, makes route as a sequence of loops, such that the same node appears in the route of communication many times. It is a looping attack.

Fig. 1 (a) Carousel Attack
Normal communication path must be 1-2-3-12 but the vampire attack change the communication path and generate loop and the path is 1-2-3-4-5-6-7-8-9-10-11-12. Node NA, NB, NC, ND are communication in loop and making carousel attack.

**Stretch Attack**

For this type of attack malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. The honest path is very less distant but the malicious path is very long to make more energy consumption.

![Fig. 1 (b) Stretch Attack](image)

Normal communication path must be S-NA-ND-D the dotted arrow showing the normal path but the stretch attack generates the long for more energy consumption.

## II. RELATED WORK

To understand the concept and impact of power draining on MANET, work consider certain research work which is explain below:

Zubair A. Baig et. Al [1] proposed a solution where it concludes that Distributed Denial of Service (DDoS) attack is most popular attack for power draining. They also discussed about various attack models and impact. They designed pattern recognition problem to detect DDOS attack. Proposed method improves performance on basis of timely and energy-efficient manner.

Ambili M. A, Biju Balakrishnan [3] proposed energy draining in WSN and introduced energy Based Intrusion Detection System. Intrusion Detection method detect vampire node on the basis of energy level of the node. All node that present in the network will have same energy level and during the communication little changes will take place. Intrusion Detection based on the fact that the malicious node will have more power than other node because it will consumes other nodes energy so it will aver high energy level. Thus all nodes energy level measured and the node which have abnormally high energy, considered as vampire node.

Chahana B. Thakur , V.B.Vaghe la [4] describe vampire attack and its types and introduced flag based technique to detect and prevent vampire attack. Flag set to header to it cannot take much space and can prevent from the repeated path as for the carousel attack. Flag initializes with 0 and when RREQ generates it set to ne one and when RREP generates it incremented by one so the flag field is key point to discover the basic loop and since vampire attack is to be detected.

Eugene Y. Vasserman et al [5] discovered that every studied protocol is vulnerable to vampire attacks that are complex to discover and simple to introduce with the help of one malicious node transferring. At its worst case, only single attacker is able to enlarge extensive battery power consumption by a factor of O (N), where N is number of nodes in network. Author discusses solution to moderate all vampire attacks that include a fresh proof – of - concept which provably limits the harm caused by attacker in duration of the packet forwarding phase.

## III. PROPOSED SOLUTION

The main requirement for the proposed work is to first observe the actual performance of network in terms of energy consumption on every node. Subsequently, it also requires observing the energy consumption after attack and deployment of detection and prevention technique to analyse the variation into energy consumption. A NS2 .35 simulator is used to develop and observe the performance of proposed sensor network scenario and prevention technique. "Generic" Energy model is configured to specify energy consumption at transmission, receiving, idle and sleeping stage by modifying adv.h and aodv.cc files.

AODV routing protocol and keep track on battery consumption, introduce overload during attack and calculate natural and intentional power consumption.
Flow Chart

Fig. 2 Flow Chart for Proposed Solution

Step 1: Broadcast the message
RREQ Packet end to all the nodes and check which have the shortest path for the communication. RREQ message is broadcasted in the network.

Step 2: Receive Reply message.
Destination sends the RREP message to the source. RREP message is unicast to source.

Step 3: Compare energy level of each node.
All the nodes will have the same energy level rather to the vampire node. Vampire node will have the highest energy level in compare to the other nodes energy level.

Step 4: If node has highest energy level

4.1 Detection
Get the particular node id from the routing table which have the highest energy level.

4.2 Prevention
Add node as a Vampire Node and find another route to send message.

Step 5: Else, Accept Node as legitimate node.
If all nodes have the same energy level means all the nodes are legitimate nodes.

Step 6: Stop

IV. SIMULATION STRATEGY
Simulation is the replication of essential features of some system or process in order to study the characteristics or performance of the system. This thesis work requires a network simulator as the proposed work is based on MANET. In this work, Network Simulator (NS-2) software version 2.35 (NS2.35) is used due to its open source simplicity and free availability.

The simulation configuration for mobile nodes consists of many network components and simulation parameters that are shown in the table 4.1 in detail.

<table>
<thead>
<tr>
<th>Channel</th>
<th>Channel/WirelessChannel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagation</td>
<td>Propagation/TwoRayGround</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Phy/WirelessPhy</td>
</tr>
</tbody>
</table>
Platform | Ubuntu 13.10 / 15.04  
---|---  
NS Version | Ns-allinone-2.35  
MAC | Mac/802_11  
Interface Queue | Queue/ DropTail / PriQueue  
Link Layer | LL  
Antenna | Antenna/OmniAntenna  
Interface Queue Length | 50  
No. of Nodes | 20,40,50  
Simulation area size | 750*750  
Traffic Pattern | CBR Sessions  
CBR Packet Size | 512 bytes  
Simulation Duration | 130 seconds

V. RESULTS

Energy consumption is the residual amount of the nodes energy.

VI. CONCLUSIONS

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. This research work carried out the study of routing protocols and various security threats. This research work proposed Intrusion Detection System based detection technique to identify malicious node(s) into ad-hoc networks. NS-2.35 simulator has been used to simulate and evaluate the performance of proposed system. Simulation of security strategies provides the facility to select a good security solution for routing protocols and gives the knowledge how to use these schemes in hostile and compromised environments. Energy consumption in the static node scenario and the mobile node scenario is less in compare to vampire attack but high with the compare of original AODV protocol.
Fig. 4 Simulation of Mobile Ad hoc network

REFERENCES


