RESEARCH PAPER | Engineering | Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X



Detection and Elimination of Vampire Attack in Mobile Ad hoc Network

KEYWORDS: Ad-hoc networks, vampire attack, stretch attack, carousel attack, Energy consumption, AODV

Chahana B. Thakur	V.B.Vaghela
PG Student, EC Engineering, SPCE, Visnagar,	Assot. Professor and Head, EC Engineering, SPCE, Visnagar

ABSTRACT Ad hoc Networks are vulnerable due to their structure less property. The limitations of the Ad hoc networks are resources like battery power, communication range and power capabilities. Prior security work has focused on Denial of Communication at the routing or medium access control levels. These types of resource depletion attack called as Vampire attacks which drain's nodes battery power and permanently disable the entire network. These "Vampire" attack are not specific to any specific protocol. They not only affect single node but they bring down entire system battery power. In this paper, we discuss two types of vampire attack and the proposed system detects and eliminate vampire node in mobile ad hoc network which causing vampire attack.

I. INTRODUCTION

1.1 Background of MANET

Ad hoc in Latin means "For this purpose only", and its implies spontaneous and temporary settings. MANET is new emerging technology which enables users to communicate without any fixed infrastructure regardless of their geographical location. [1] MANET is a collection of wireless mobile nodes forming a temporary network, without the aid of any centralized administration or standard support services that are regularly available on the wide-area network, to which the nodes may normally be connected. The aim of such network is to provide communication capabilities to areas with limited or no exiting communication infrastructure. [2]

Routing Protocol play a vital role in MANET to find routes for packet delivery and make sure that the packets are delivered to the correct destination. These protocols are classified as: (1) proactive (2) reactive (3) hybrid. Among these protocols, the reactive category is widely used because they find routes whenever needed (on demand). [3]

Here we consider a reactive routing protocol, AODV (Ad-hoc On Demand Distance Vector). AODV is a reactive protocol that maintains routes only between nodes which need to communicate. The routing messages do not contain information about the entire path, but only about the source and destination.[6] Therefore routing messages don't have an increasing size. It uses destination sequence numbers to specify how a fresh route is, which is used to grant loop freedom.

The major characteristics of mobile Ad-hoc networks are:
Power consumption constrains for nodes using batteries, Ability to cope with node failures, Mobility of nodes, Dynamic network topology, Communication failures, Ability to withstand complex environmental conditions, Ease of use, deeply distributed architecture.

1.2 Resource Depletion Attack

Due to the Ad-hoc organization, mobile ad-hoc networks are particularly vulnerable to Denial of Service (DoS) attacks and a great deal of research has been done to enhance survivability. Attacks can be of two types, a resource depletion attack and a routing disruption attack. A routing disruption attack tries to alter the routing path e.g.: Worm hole, Sybil attack, etc. whereas the resource depletion attack only focuses on the battery power and memory. The most permanent DoS attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with the battery power as the resource of interest. These attacks are commonly called as "Vampire attacks". They are called so because they drain the battery power from the nodes. These are a type of Denial of Service since they affect the entire system from performing. They are difficult to be detected since they are protocol compliant and are orthogonal to them. They are not protocol specific. They do not affect a single node they take their time attack one by one and disrupt the entire system.[7] Vampire attacks can be defined as the composition and transmission of a message that cause more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers .

1.3 Types of Vampire Attack

Vampire attack constitutes of two different types of attack called Stretch attack and Carousel attack. These two mainly focuses on reducing the energy of the nodes.



Fig.2. Types of vampire attack [8]

A. Carousel attack

In this type of attack, a malicious node sends a packet with a route composed as a series of loops, it targets source routing protocols by manipulating the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly travelling in the same set of nodes. Hence same node appears in the route many times.[11] We call it the carousel attack, since it sends packets in circles .Times strategy can be used to increase the route length and in this way the energy is lost from the nodes.

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

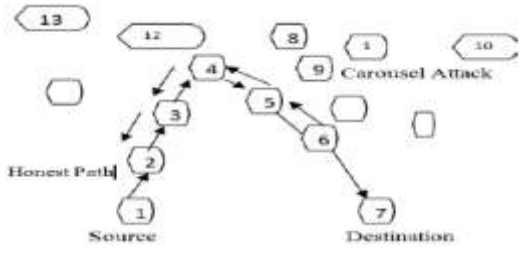

Fig.3. Carousel Attack same node in the route many times

B. Stretch attack

In this type of attack, a malicious node artificially select long 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. In this stretch attack it mainly shows more uniform energy consumption for all the exiting nodes in the network. This attack mainly lengthens the route by causing more numbers of nodes to process the packet in the network.[11] These attacks mainly make use of network-wide energy usage significantly at each and every node so that they are also affected until it reach destination.

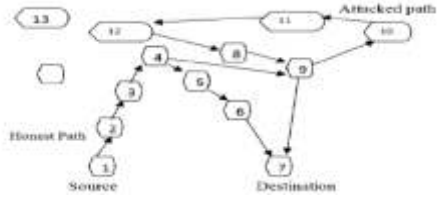

Fig.4. Stretch Attack with two different paths from source to destination (4-9-10-11-12-8-9-7 long route)

II. PROBLEM MOTIVATION

The life of the wireless ad-hoc network, especially that of mobile network depends on its node's battery power. In any real time application of mobile Ad -hoc networks, millions of nodes may be present. And in most of the applications, battery recharging or replacing is impossible. Power drainage will leads to the failure of the node and it will affect the network also. Data loss will also occur. But some malicious packets called vampire packets may consume more energy for packet forwarding than that of honest packet forwarding .This will lead to very large amount of power drainage of node, unnecessary packet loss and network failure. If we can find and avoid these type of vampire packets, then we can increase the life of the node and thereby the network. It will be very crucial in many of the situations and will increase the wide acceptability of ad-hoc wireless networks in many important applications.

III. PROBLEM OBJECTIVE

The objective of this paper is to create a secure mechanism for vampire attack which consumes more energy for packet forwarding than that of honest packet forwarding. This paper also detect the particular node that act as a vampire node which causes large routes or loops in the network and also elimination of this vampire node to prevent the forwarding of packets from source-destination route. In this paper, we discuss the effect of vampire attacks on Ad-hoc On Demand Vector Routing (AODV).

IV. RELATED WORK

In this section, we will see some of the related works to the detection of vampire attack in ad-hoc network using different approaches:

Eugene Y. Vasserman and Nicholas Hopper introduced a definition of a vampire attacks in February 2013. Vampire attacks are clearly defined in their study. A clean state secure sensor network routing protocol PLGP has been designed to reduce the energy drain due to stretch and carousel attack. The PLGP protocol makes sure that the packet always travels towards the destination without any back tracking. PLGP does not satisfying No-back tracking property. To overcome this problem author introduced PLGPa, which uses attestations that are added to the packet header and which satisfies No-backtracking property.

S.Kaul, H.Samuel, J.Anand, introduced Energy Weight Monitoring Algorithm (EWMA), used to overcome two types of vampire attack called carousel attack and stretch attack. EWMA technique is based on the concept of energy level.
There are mainly two phases in EWMA. 1. Network configuring phase and 2. Communication Phase.
Research on vampire attacks and different approaches are used to detect vampire attack based on Energy.

4.1Drawbacks of Existing System

1. PLGPa added attestations to the packet, which are similar to signatures, every time the packet is forwarded. This way the nodes cannot modify the previous node's details and will have to add their own signature to forward it. Attestations added to the packet header made the header size larger thereby leading to difficulty in encryption, decryption and coding. In scenarios where the malicious node can duplicate the signature of another node, the PLGPa protocol is rendered useless.

2. After that, various algorithms like EWMA, TRUST ALGORITHAM, CBEWRA, and ECDH are used to Detect Vampire attack in international journal papers 2014. All algorithms are based on concept of energy level. It works on the fact that the malicious nodes will have abnormally high energy than honest nodes. Thus in this energy of all nodes are measured and the node with abnormally high energy is detected as malicious node. But this method is not convenient because a node which participating in many source-destination route than energy used by that node is very high so that there is abnormal change in its energy level. There is chance to detect this honest node as a vampire node. So in that type of situations this type of methods is not work well.

V. PROPOSED WORK

In this paper, our proposed algorithm is used to delete Vampire node data transfer which causes large routes on loop in the network in order to overcome vampire attack in mobile ad hoc network.

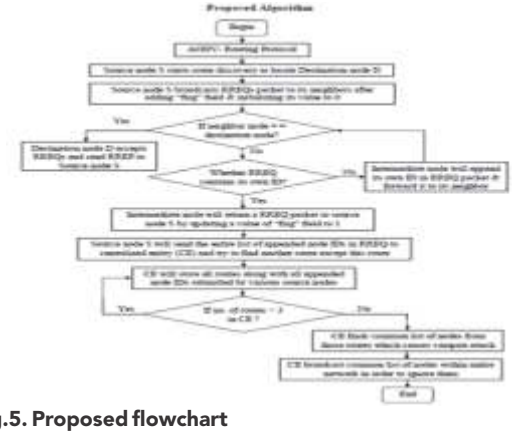

Fig.5. Proposed flowchart

Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

A Flag field added as a security to the packet header in order to avoid packets loops or stretch attack. This is8 bit in size therefore does not occupy much space in the header. The flag field is 0 in the begging. Only when a node receives repeated packet or a packet which contain its own ID then its forwards repeated packet to the destination node.

In order to find common nodes among all routes, we have decided to choose minimum three routes, so that is why we selected value 3. It is actually not a threshold but value which specifies 3 different paths/routes.

B. Proposed Algorithm Figure

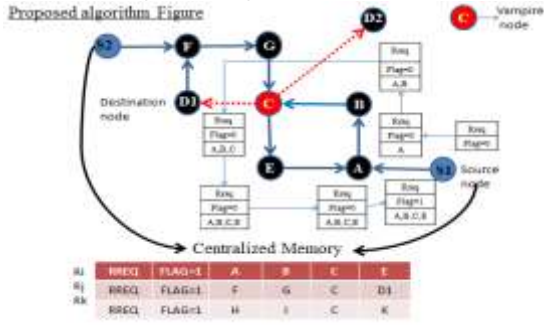

Fig.6. Proposed Algorithm figure for detecting and eliminating vampire node

C. Proposed Algorithm steps:

1. Routing Protocol: AODV
2. Source node S starts route discovery to locate Destination node D.
3. Source node S broadcasts RREQs packet to its neighbors after adding "flag" field & initializing its value to 0.
4. If (neighbor node = = destination node) {
   Destination node D accepts RREQs and
   Send RREP to Source node S.
   Return.
   }
5. If (Whether RREQ contains its own ID == true) {
1. Intermediate node will return a RREQ packet to source node S by updating a value of "flag" field to 1.
2. Source node S will send the entire list of appended node IDs in RREQ to centralized entity (CE) and try to find another route except this route.
3. CE will store all routes along with all appended node IDs submitted by various source nodes.
4. If (If no. of routes < 3 in CE) {
Go to Step 5.3 (within if case).
   }
5. Centralized Entity (CE) finds common list of nodes from those routes which causes vampire attack.

$X_{set} = R_i \cap R_j \cap R_k$ where i, j & k are three different routes in CE.

6. Centralized Entity (CE) broadcast common list of nodes X_{set} within entire network in order to ignore them.
7. Return
   }

Else {
1. Intermediate node will append its own ID in RREQ packet & forward it to its neighbor.
2. Go to step 4.

} }

V. NETWORK SIMULATOR (NS2)

NS2 is open-source discrete event network simulator that provides significant simulation of transport, routing, and multicast over- wired and wireless networks, including most MANET routing protocols and an implementation of the IEEE 802.11 MAC layer [12] NS-2 code is written using c++ and OTCL interpreter, thereby generating a communication trace file and a NAM (network simulator) file as its output. NS-2 may be installed over either LINUX or any UNIX-based operating system [13]

VI. CONCLUSION

In this paper we define vampire attack, a new class of resource draining attack that use routing protocols to permanently disable ad hoc networks by depleting nodes battery life. These energy attacks do not depend on specific protocol and define proposed algorithm which detect and eliminate vampire node in mobile ad-hoc network which disrupt the entire network and permanently disable the network.

In future we implement our proposed mechanism in NS2 and detect vampire node which causes vampire attack and eliminate the vampire node. We also compare reading of energy consumption with and without vampire attack and after that we compare that one with our proposed algorithm reading.

REFERENCE

[1] P.Goyal, V.Parmar, R. Rishi, "MANET:vulenerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 | [2] S.Y.Han, D.Lee, "An Adaptive Hello Messaging Scheme for Neighbor Discovery in ON-Demand MANET Routing Protocols", IEEE COMMUNICATION LATTERS, VOL.17. NO.5.MAY 2013 | [3] S.Pandey, V.Prakash, S.Yadav, "QOS Optimization of Multipath Routing in MANET", International Journal of Emerging technology, Volume 3,.Issue 8, August 2013 | [5] M.Swathi, B.Pravallika, N.V.Muralidhar," Implementing And Comparison of MANET Routing Protocols using NS2", International Journal of Emerging technology, Volume 4, Issue 2, February 2014 | [6] S.Arvind Kumar, D.Divakaran, "Detecting and Avoiding Network attacks using routing protocol in Wireless Sensor networks", COMPUSOFT, volume.3, Issue.4, April 2014 | [7] G.Vijyanand, R.Muralidharan," Overcome vampire Attacks problem in wireless ad hoc sensor network by Using distance vector protocols", International Journal Of Computer Science and Mobile Applications" Vol.2, Issue.1, January2014 | [8] M.G.Aruna, G.Y.Nivedita, "Vampire Attacks: Wearing Out Life of Wireless Adhoc Sensor Networks", ISOR Journal of Computer Engineering, Volume.16, Issue 3, June 2014 | [9] J.Anand, K.Sivachandar,"Vampire Attack Detection in Wireless Sensor Network", International Journal of Engineering Science and Innovative Technology, Vol.3, Issue.4, July 2014 | [10] L. Santhaosh, A.V.Krishna Mohan, "Prevention of Resource Attack in Wireless Sensor Network" Proceedings 5th SARC-IRF International Conference, angalore, India, May, 2014. | [11] S.Kaul, H.Samuel, J.Anand," Defending against Vampire attacks in wireless sensor networks", International Journal of Communication Engineering Applications, Volume 5, Article C084, March 2014 | [12] G. Yan, K.Ibrahim, Basic simulator for Wireless ad hoc Network, computer science department, VA 23529 | [13]Fan Li, Y. Wang, "Routing in Vehicular Adhoc Networks Networks: A Survey", IEEE vehicular Technology Magazine, Volume .2, Issue.2, June 2007