# Detection and Prevention of Vampire Attack in MANET

Anamika Garg
Department of CSE,
RGPV University
*anaccna@gmail.com*

Mayank K Sharma
Asst. Professor, Department of CSE,
RGPV University
*mayank.sharma@sims-indore.com*

***Abstract***— 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. 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. The objective of this study is to detect and prevent mobile ad- hoc networks from unwanted power draining due to 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 forcefully shutdown malicious nodes and transfer communication.

***Keywords***— *Mobile ad-hoc Networks, Vampire Attack, AODV*

*****

## 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 such kind of attack which aims to disrupt the network by draining resource capability. Here, Attacker communicates worthless messages formally known as false packet to increase network traffic and make target node busy in useless activity.

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**

In the Carousel attack, [4] attackers introduce some packet within a route as a sequence of loops, such that the same node appears in the route of communication many times.

 ISSN: 2321-8169
6793 - 6798

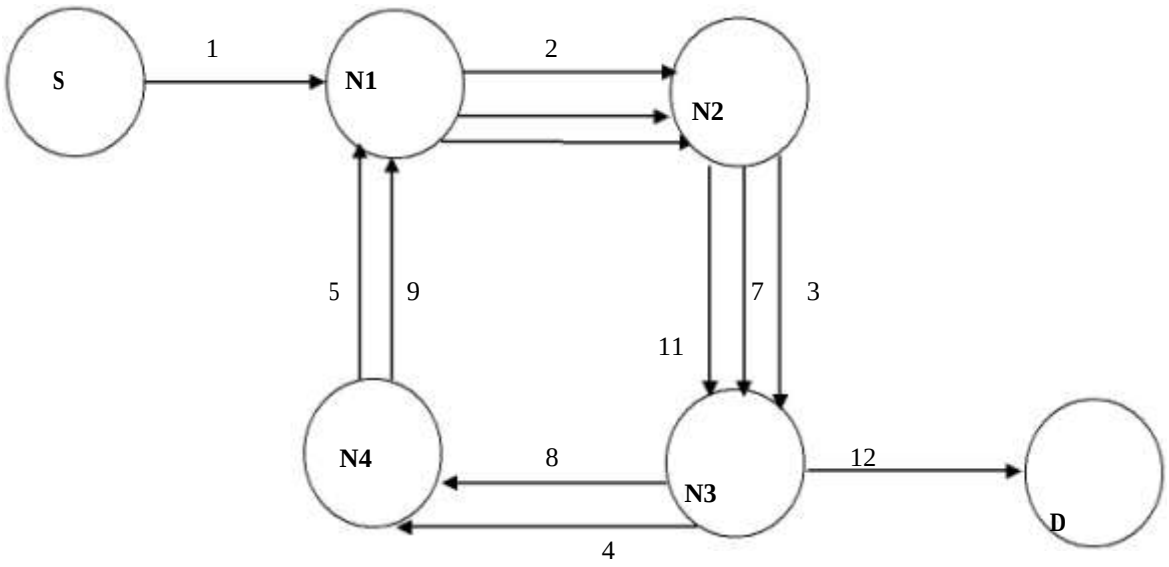


Fig. 1 (a) Carousel Attack

Honest path must be the 1-2-3-12 but in the presence of vampire attack communication path generating loop which is due to the vampire attack and the path is 1-2-3-4-5-6-7-8-9-10-11-12. Node N1, N2, N3,N4 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

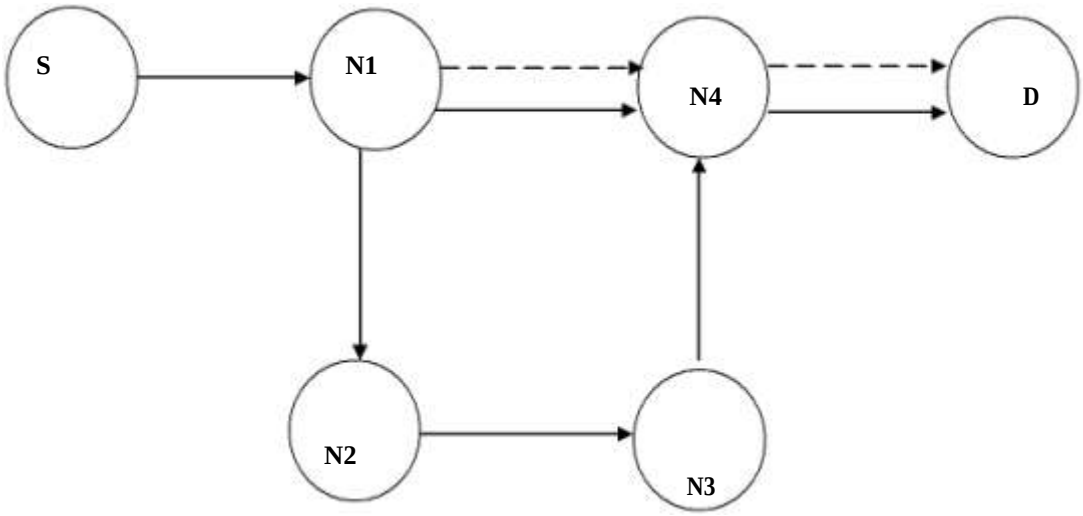


Fig. 1 (b) Stretch Attack

Honest path must be S-N1-N4-D the dotted arrow showing the honest path but the stretch attack generates the long path and it causes 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 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 l 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.

```
iNode =( MobileNode*)
(Node::get_node_by_address(index
));
xpos = iNode->X();
ypos= iNode->Y();
iEnergy = iNode->energy_model()->energy();
```

Flow Chart

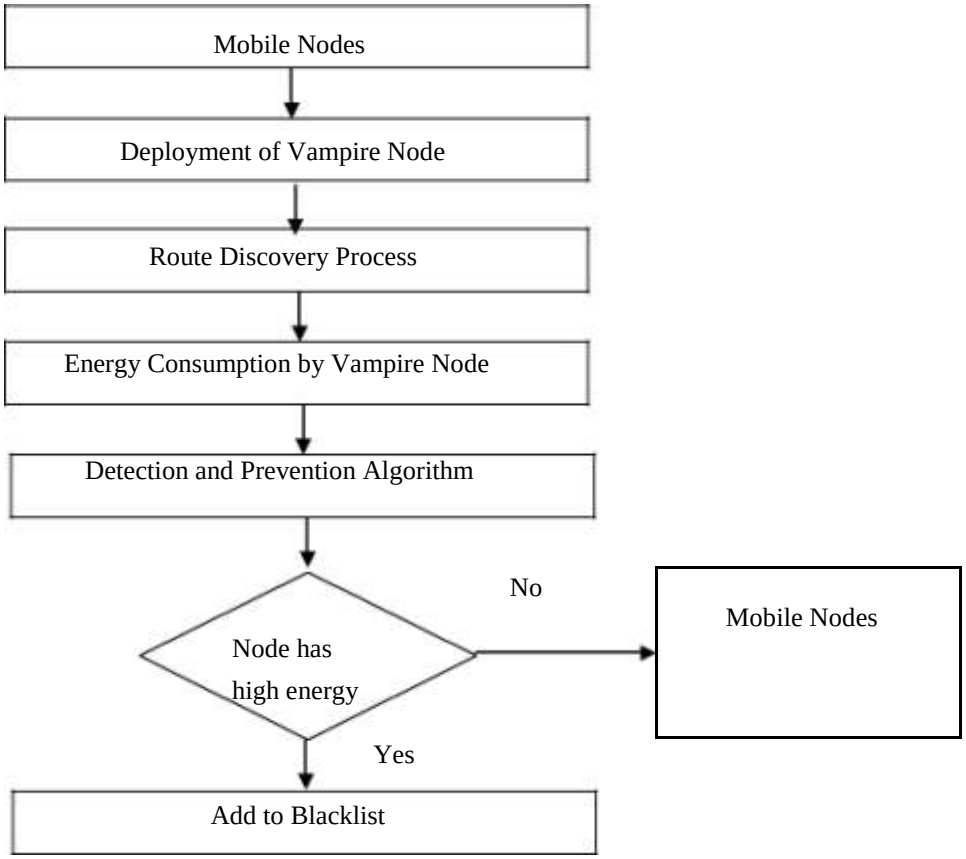


Fig. 2 Flow Chart for Proposed Solution

**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.

 ISSN: 2321-8169
6793 - 6798

| | |
|---|---|
| Channel | Channel/WirelessChannel |
| Propagation | Propagation/TwoRayGround |
| Network Interface | Phy/WirelessPhy |
| 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 | 20,50,100 |
| 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.

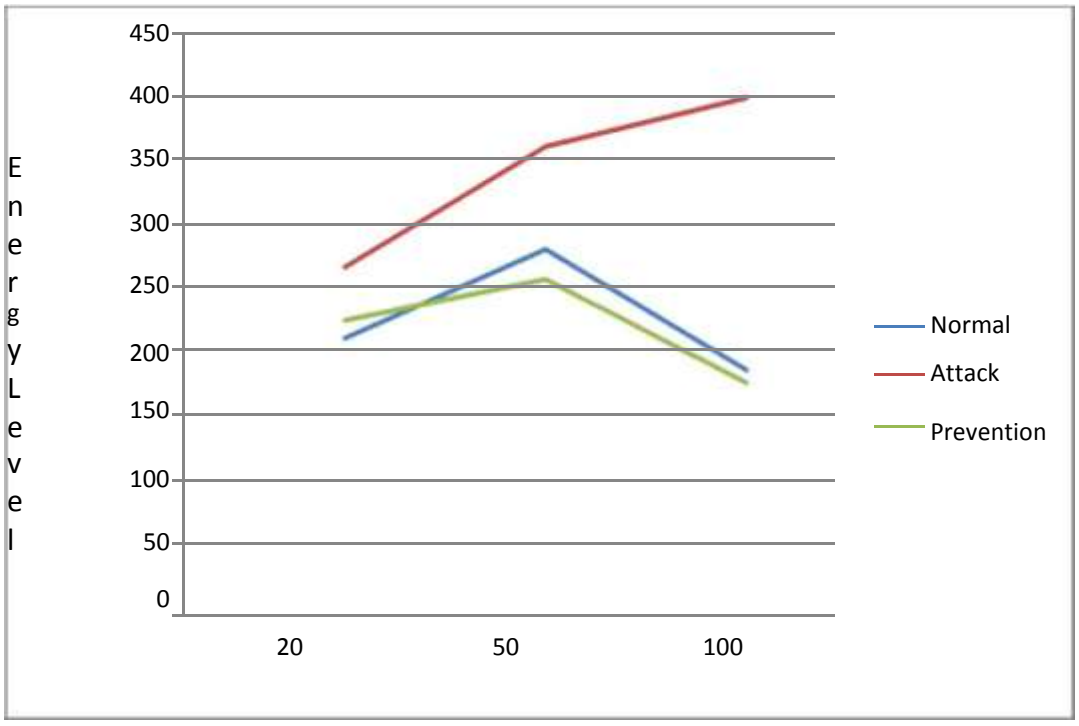


Fig. 3 Energy Consumption of stationary nodes based networks

## 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 IDS based detection technique to identify malicious node(s) into ad-hoc networks. NS-2 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.

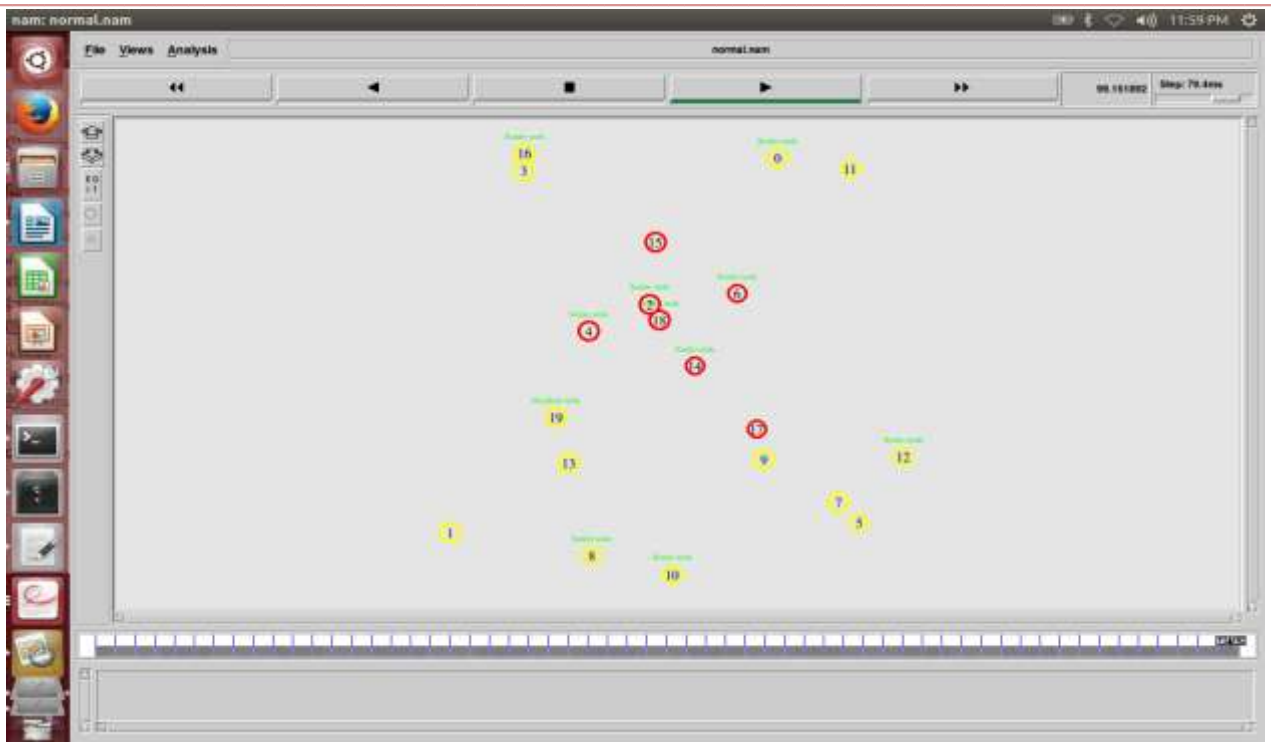


Fig. 4 Simulation of Mobile Ad hoc network

## REFERENCES

[1] Zubair A. Baig et. "Distributed Denial of Service Attack Detection in Wireless Sensor Networks" Doctor of Philosophy Monash University January, 2008.

[2] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns,2012.

[3] Ambili M. A, "Vampire Attack : Detection and Elimination in WSN", in International Journal Of Scientific Research Volume:3 April 2014 ISSN No 2277-8179

[4] Chahana B. Thakur; V.B. Vaghela "Detection and Elimination of Vampire Attack in Mobile Ad hoc Network" Indian Journal of Applied Research Volume: 5 Jan 2015 ISSN No 2249-555X.

[5] T.W. Mehran Abolhasan, "A review of routing protocols for mobile ad hoc network," ELSEVIER, Ad-hoc Network, vol. 2, pp. 1-22, 2004.

[6] M. B. Hardeep Kaur, "Performance of AODV, OLSR AND ZRP Routing Protocol under the blackhole Attack in MANET," IJAREEIE, vol. 2, pp. 2320-3765, June 2013.

[7] V. V. P. Rajipriyadharshini, "Vampire Attacks Deploying Resources in Wireless Sensor Network," International Journal of Computer Science and Information Technology, vol. 5, no. 3, pp. 2951-2953, 2014.

[8] D. J. A. P. Preethi Monoline, "Cache Consistency and IDS for Handling Attacks in Routing Ad-hocNetwork," International journal of Innovative Research in Computer and ommunication Engineering, vol. 2, no. 4, 2007.

[9] S. R. Susan Sharon George, "Attack-Resistant Routing for Wireless A- hoc Network," International Journal of Computer Science and Information Technologies, vol. 5, no. 3, pp. 420-442, 2014.

[10] I.-R. C. Fenye Bao, "Hierarchical Trust Management for Wireless Sensor Networks and its Application to Trust-Based Routing and Intrusion Detection,"IEEE Transaction on network and service managemnet, vol. 9, no. 2, July 2012.

[11] J. D. B. Umakanth, "Detection of Energy draining attack using EWMA in Wireless Ad-hoc Sensor Network," International Journal of Engineering trends and Technology, vol. 4, no. 8, August 2013.

[12] Y.Yuanming Wu,"Insider Threats against Trust Mechanism with Watchdog and Defending Aproaches in Wireless Sensor Networks," IEEE Symposium on Security and Privacy workshop, 2012.

[13] K. S. Jose Anand, "Vampire Attack Detection in Wireless Sensor Network," International Journal of Engineering Science and Innovative Technology, vol. 3, no. 4, July 2014.

[14] Buchegger, S. and J.-Y.L. Boudec. Cooperative Routing in Mobile Ad-hoc Networks: Current Efforts against Malice and Selfishness. 2002. Springer.

[15] Baker, F., Network Working Group, 2002, Cisco Systems. p. 40.