ISSN:0975-9646

# Avoidance of Power Draining in Mobile Ad-HOC Network over Vampire Attack

Anamika Garg[#1], Mayank K Sharma[#2]

*PG scholar, Department of CSE, RGPV University*
*Asst. Professor, Department of CSE, RGPV University*

***Abstract*— MANET stands for Mobile ad hoc network which is independent of any fixed infrastructure or centralized administration. In exacting, a MANET has no base stations: a node communicates directly with nodes within wireless range and indirectly with all other nodes using a dynamically-computed, multi-hop route via the other nodes of the MANET For the communication purpose every node contain certain energy and used this energy for the communication. This work presents a model for evaluating the energy consumption behavior of a mobile ad hoc network in the presence of vampire attack which is energy draining attack. For the simulation NS2.35 used having energy model. For the detection and prevention Intrusion Detection technique used which is based on the highest energy level of the node. Detection technique consider node to be malicious if node contains highest energy level of the other nodes.**

***Keywords*— MANET, Denial of Service, Security, Routing, Ad-Hoc Networks, Sensor Networks, Wireless Networks.**

## I. INTRODUCTION

Mobile ad-hoc Networks is one of growing technology in wireless networks field. It may be defined as temporarily or infrastructure less topology based collection of autonomous nodes. Mobile nodes have self-manageable characteristic which help to establish and communicate automatically. Furthermore, Dynamic topology nature gives facility to join or leave network any time.

Mobile nodes are collection of battery, processor, memory storage and suit of transducer. Here, battery may be chargeable or fixed nature depends requirement and node type. Subsequently, life of node is directly proportional with capacity of battery. Degradation in battery leads to degradation in node life. The complete phenomena impact on overall network performance and degrade the packet delivery accordingly.

Communication among nodes depends on transmission range of mobile node. A wide range communication expects intermediate node or router to discover and transfer the packet. Here, each mobile node is capable to work as node or router or switch. Therefore, it does not require any external device to connect mobile nodes or mobile networks.

Due to wide range applications require distant communication and route discovery on intermediate nodes. The nodes discover multi-hop routes to each other by exchanging topology information in the form of control messages. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure such as military, transport, aviation and commercial. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves.

Routing protocols are used to discover routes from source to destination. It may be classified into two category; Proactive Routing Protocol or Reactive Routing Protocols. Proactive routing protocols discover routes before their demand. Where, Reactive routing protocols are on-demand routing protocols. Here, reactive routing protocols are more suitable for mobile ad-hoc networks due to their on-demand route discovery nature.

The complete phenomena require lots of energy for route discovery and packet transmission. A heavy route discovery process or information processing will quickly degrade the battery capacity. The complete work observes that, energy consumption is the key challenge in mobile ad-hoc networks and it should be as possible as least amount.

## II. RELETED WORK

Energy conservation is an important issue in ad hoc networks as nodes are usually battery powered. Even though a node may not have any message of its own to transmit, its battery is drained when it acts as a router and forwards packets for other nodes. In transmit mode a mobile unit uses its maximum power level to transfer packet to another node. Communication involves the cost of sending data along with control packet from source, routed through intermediate node and cost at receiving at destination end.

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

Zubair A. Baiget. 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.

S. N. Premnathet. al. [3] proposed a advanced DDOS attack They also propose a special attack named as SDP Attack (Service Discovery Protocol based attack) to make Heavy Power Drain on node.SDP sends new service request similar to SYN Flooding to create conjunction and overwhelming the nodes. SDP attack effectively make it inoperable and reducing the battery life by as much as 97%.

Ambili M. A, BijuBalakrishnan [4] 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 nodes 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 melicious node will have more power than other node because it will consumes other nodes energy so it will ave 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.Vaghela [5] 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.

## III. SECURITY THREATS

Security threats come when basic security breaks down and this can be any form like energy based security threats.

Attacks are classified into two categories:

- Active Attack
- Passive Attack

DOS attack is considered to be active attacks which prevent the normal use of communication services.

DOS attacks in wireless network not only cause damage to the victim node but decrease the performance of the entire network because nodes have a limited battery power and the network can be congested due to limited bandwidth.

Some recognized attacks are as follows:

### *A. Black Hole Attack*

In this attack malicious node drops the entire packet transmitted by the sender.

### *B. Gray Hole Attack*

Grey Hole attack is similar to black hole attack except that the malicious node drops selective packets not all the packets are dropped.

### *C. Worm Hole Attack*

In this attack two malicious nodes participates for establishing the tunnel. One node takes the data packet from the sender and sends to the other participant (malicious node). In this way two malicious node creates tunnel.

### *D. Sybil Attack*

In this attack one malicious nodes recognize the network and acquires multiple fake identities and pretends to be multiple, distinct nodes in the system.

### *E. Vampire Attack*

It is energy darning attack where malicious node consumes other nodes energy and downs all the nodes energy.

Mobile ad-hoc network particular vulnerable to DoS attack. Attacks can be of two types, a resource depletion attack and a routing disruption attack. [5] 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”.

## IV. VAMIRE ATTACK

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.

[2] 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, these attacks are very difficult to detect and prevent.

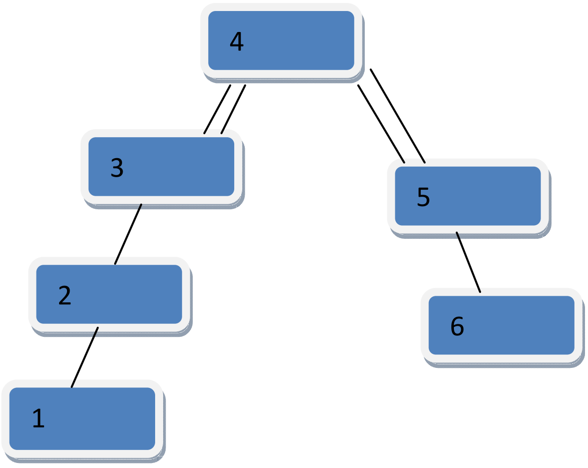
The vampire attacks can be classified has two types. There are: one is Carousel attack and other is Stretch attack.

### *1)* 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. This attack increases the routing length and delay very much in the net- works and also inadequate by the number of allowable entries in the resource route.

Series of loops made in this way, such that the same node appears in the route many times. [3] This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

Route looping causes high energy consumption which drains energy level of the whole network.



Source Destination

**Honest Path 1-2-3-4-5-6**

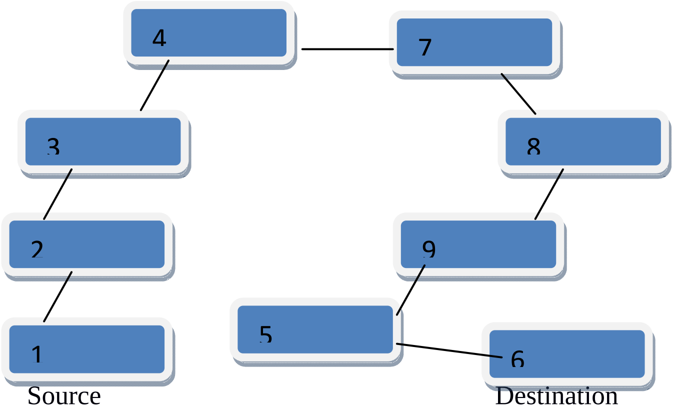
**Carousel Attack Introduce path 1-2-3-4-5-4-3-2-3-4-5-6**

**Introduce Loop between 2-3-4-5**

Fig. Example of Carousel Attack

### *2) Stretch Attack*

Second attack also [4] targeting resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet target. For this type of attack malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. [3] The honest path is very less distant but the malicious path is very long to make more energy consumption.



**Honest Path 1-2-3-4-5-6**

**Stretch Attack Introduce path 1-2-3-4-7-8--9-5-6**

Fig. Example of Stretch Attack

**Impact of Vampire Attack**

Ad-hoc network communication based on the nodes energy level. Vampire attack based on the poser draining of network. Presence of vampire attack leads to the failure of the node and the network also due to the energy consumption of nodes. Data loss will also occur.

## V. SIMULATION TOOL

Work done performed with the help of ns2.35 network simulator. This software is a discrete event driven simulator and is developed at UC Berkelry as a part if the VINT project. It is distributed as open source software.

NS2 is built using object oriented language C++ and OTcl (Object oriented varient of Tool Command Language). NS-2 interprets the simulation scripts written in Otcl. User writes his simulation as an Otcl script. Some parts of NS2 are written in C++ for efficiency reason. It also use various tools like Nam which is Network animator to visualize the running network scenario. Xgraph tool for plotting the graph for result analysis.

## VI. PERFORMANCE METRICS

In order to evaluate the performance, several metrics are used, such as packet delivery fraction, end-to-end delay, throughput, and power consumption. The most important metrics for best-effort traffic are the packet delivery fraction and the end-to-end delay. However, these metrics are not entirely independent as a shorter delay does not necessarily mean a higher packet delivery fraction, as only successfully delivered packets are used to measure the delay. A lower packet delivery fraction and longer delay may, however, cause a larger overhead.

### *F. A. Packet Delivery Fraction*

The ratio of the number of data packets sent by the CBR sources and the number of data packets received by the CBR sinks at their destination. It shows how reliable a protocol is and the higher the PDF, the better the results.

### *G. B. End-to-end Delay*

The average length of time, measured in seconds, necessary to deliver a set of data from the source to the destination node.

It includes all potential delays resulting from queuing at the interface queue, propagation and transfer times, and retransmission delays at the MAC layer.

### *H. C. Throughput*

The number of bytes successfully transferred to the destination during a specific amount of time (s).

### *I. D. Power Consumption*

The average power consumption per node is calculated based on the ratio of the total energy consumed by all nodes in the network divided by the total number of nodes.

TABLE I
SIMULATION PARAMETER

| | |
|---|---|
| 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 |
| Simulation area size | 750*750 |
| Traffic Pattern | CBR Sessions |
| CBR Packet Size | 512 bytes |
| Simulation Duration | 130 seconds |

TABLE IIIII
PERFORMANCE EVALUATION

| | Normal AODV | AODV with Vampire Attack | Modified AODV |
|---|---|---|---|
| Throughput(b/s) | 84.78 | 25.29 | 52.72 |
| Total Energy | 200.813 | 259.39 | 215 |
| Protocol Energy | 50.203 | 64.849 | 53.813 |

## VII. CONCLUSION

This paper introduces energy draining attack and the proposed method to detect and remove it by using intrusion detection method. Intrusion detection method detect malicious node on the basis of energy level of nodes and remove that node from the current path. Thus the securing of network nodes energy is carried out and finding alternate path for route after detection is done. The simulation result proves the improvement in the energy consumed and throughput and decreases hop count and save the nodes energy. By avoiding vampire attack this work will increase life of the node and the network. It will be very crucial in

## REFERENCES

[1] Getsy S Sara1, S.NeelavathyPari, D. Sridharan,"EVALUATION AND COMPARISON OF EMERGING ENERGY EFFICIENT ROUTINGPROTOCOLS IN MANET" in proceedings published in ICTACT JOURNAL OF COMMUNICATION TECHNOLOGY, MARCH 2010.

[2] V.Sharmila1, Mr. K. MuthuRamalingam" Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network" IJCSMC, Vol. 3, Issue. 8, August 2014

[3] P.Suthahar, IIR.Bharathinternational "Defending against Energy Draining attack in Wireless Ad-Hoc Sensor Networks Journal of Advanced Research in Computer Science & Technology (IJARCST 2014) Vol. 2 Issue Special 1 Jan-March 2014.

[4] Ambili M. A, BijuBalakrishnan "Vampire Attack : Detection and Elimination in Wsn".

[5] ChahanaB. Thakur ,V.B.Vaghela "Detection and Elimination of Vampire Attack in Mobile Ad hoc Network" INDIAN JOURNAL OF APPLIED RESEARCH Volume - 5 | Issue - 1 | Jan Special Issue - 2015 | ISSN - 2249-555X

[6] Eugene Y. Vasserman , Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011.

[7] ImadAad, Jean- Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004