RESEARCH ARTICLE OPEN ACCESS

Vampire Attacks: Detection And Prevention

Devikarani Roy[1], Shilpa Verma[2]
[1](ME Student, Department of Computer Engineering,
Thadomal Shahani Engineering College, Mumbai University, Mumbai-50)
[2](Associate Professor, Department of Computer Engineering,
Thadomal Shahani Engineering College, Mumbai University, Mumbai-50)

----------**********----------

Abstract:

Wireless Sensor Networks (WSNs) are used nowadays, and therefore have broad range of interesting applications. WSN can be of hypersensitive nature and therefore might require enhanced secured environment. In today's world WSNs are the basic means of communication. The resources like battery power, processing capabilities, communication and transmitting range are limitations of the system. One of the major challenges in Wireless Networks is the security concerns. Attacks affecting these types of systems are increasing. One of the major resource consumption attacks called vampire attacks. It includes Stretch attack and Carousal attack which affects node and even bring down the entire system by draining the Battery power. In Stretch Attack, attackers construct wrong long routes which leads to traversing almost every node in the network. Stretch attack, increases packet route length, and packets get processed by a number of nodes. Carousel attackers introduce some packet within a route tranquil as a sequence of loops, and so the same node appears in the route many times. The proposed system overcomes this challenge by using the techniques which include the Energy weight detection algorithm and Route Tracking algorithm, so energy consumption is reduced to a great extent. EWDA and Route Tracking algorithm is used to detect and prevent the above problems.

Keywords —**Networking, WSNs, Stretch attack, Carousal attack, EWDA , Routing algorithm, NS2**

----------**********----------

I. INTRODUCTION

Vampire attacks which are the most common Energy depletion attacks where the energy consumed by the network to compose and transmit a message is more when its compared to that of an ordinary network. Vampire attacks distort the working of a network immediately rather than work overtime to entirely disable a network.

The proposed system overcomes this challenge by using the techniques which include the Energy weight detection algorithm and Route Tracking algorithm so energy consumption is reduced to a great extent.

Wireless ad-hoc networks are particularly prone to denial of service (DOS) attacks due to their ad-hoc organization. Vampire attack can be defined as the formation and transmission of a message that causes more energy to be consumed by the network in comparison to an honest node transmitted a message of same size to the same destination, by using different packet headers. We can calculate the potency of the attack by the ratio of network energy used in the honest case to the energy used in the malicious case. There are two main types of vampire attacks. In the carousal attack, an adversary composes packets with routing loops, it targets source routing protocols, allowing a single packet to repeatedly traverse the same set of nodes . The second type of attack i.e. stretch attack also targeting source routing, where attacker constructs artificially long routes, which leads to almost traversing every node in the network. We call this the stretch attack, since it increases packet route lengths, causing packets to be transmitted by a number of nodes that is liberal of hop count along the shortest path between the packet destination and attacker .

The impact of these attacks can be further increased by linking them, increasing the number of adverse nodes in the network, or by simply sending

lots of packets. In networks that do not employ authentication and use end-to-end authentication, attackers are free to replace routes in any overheard packets, and we assume that only messages generated by attackers may have maliciously-composed routes. There is no secure and reliable mechanism available to detect and prevent vampire attacks in wireless adhoc networks. So a new mechanism is introduced, which detects the vampire attacks i.e Stretch and Carousal attack and prevents the system from energy draining.

The ad hoc wireless network contains a number of small wireless devices which has the wireless communication capability, signal processing intelligence and transferring of the data. Communications are vulnerable to various kinds of attacks due to insecure wireless channels. The objective is to examine energy depletion attack which attempts to permanently disable nodes by draining their battery power which is known as vampire attack. These attacks rely on the properties of many popular classes of routing protocol. The proposed prevention technique is used to reduce vampire attack using new protocol and route recovery technique to decrease the energy loss due to packet transmission over the unwanted route in the network.

II. RELATED WORK

A very early mention of power exhaustion attack can be found as “sleep deprivation torture.” As name suggest, the attack obstruct nodes from entering a low-power sleep cycle, and thus consumes their batteries faster. New research concluded that “denial of- sleep” only considers attacks at the medium access control (MAC) layer. Additional work mentions resource consumption at the transport and MAC layers, but it only offers rate restricting and elimination of insider adversaries as potential solutions.

Malicious routing loops have been briefly mentioned, but no effective defences are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing. Even in non-power constrained systems, exhaustion of resources such as CPU time, bandwidth and memory may effortlessly cause problems. A famous example is the SYN flood attack, wherein attackers make multiple connection and attackers then requests to a server, which will allocate resources for each connection request, leading to running out of resources, while the attackers, who assigns minimal resources, remains operational, such attacks can be defeated or attenuated by putting greater burden on the connecting entity. Moreover, since Vampires do not drop packets, the quality of the malicious route itself may remain high (although with increased latency). In Stretch Attack, attackers construct falsely long paths, which leads to traversing every node in the network. It increases packet lane length, causing packets to be processed by many nodes.

In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the path of communication many times in the form of loops. This attack increases the routing length and delay in the networks and also inadequate by the number of allowable entries in the resource route.

The vampire attack is a serious problem in WN. Such attacks need to be detected as early as possible. In existing system clean-slate sensor network routing (PLGP) is used which is developed by the scientist Parno, Luk, Gaustad and Perrig (PLGP). Its original version is vulnerable to vampire attacks and can be modified to prevent vampire attacks.

It consists of two phases: Topology discovery phase and Packet forwarding phase.

A. Topology Discovery Phase

Topology discovery regulates nodes to trees. Initially every node knows only itself and at the end of discovery every node should estimate the same address tree as other nodes. All nodes are physical nodes in network and virtual address corresponds to their position in the network. In this phase every node broadcast certificate of identity including public key (Node id). Each node starts as its own group size one, having a virtual address zero. Groups are merged with the smallest group and each group chooses 1 or 0 when merge with another group. Each member pretends to have a group address to their own address gateway nodes. At the end each node knows the virtual address of every

node, public key and certificate and then network forms a single group.[1]

B. Packet Forwarding Phase

In Packet forwarding phase, all decisions are made independently by each node. When a node receives a packet it determines what is the next hop by finding the most significant bit of its address that varies from the message originators address. Every forwarding leads to shorten the logical distance to destination. PLGP is the protocol that reduces vampire attack.. Path attestation includes the extra verification like it checks a corresponding entry in the signature chain, and should be logically more closer to the destination than the previous hop in the chain. This is how the forwarding nodes can enforce the forward progress of a message, preserving no-backtracking. If no authentication is present, the node checks to see if the generator of the message is a physical neighbour. Since messages are signed with the originators key, malicious nodes cannot falsely claim to be the origin of a message, and therefore do not benefit by removing attestations.[1],[2]

The denial-of-sleep attack is a typical type of denial-of-service (DOS) attack that targets a battery-powered device's and attacks power supply resulting in quick exhaust of this constrained resource. It is hard to replace sensors which fail due to battery drainage. The Denial of sleep attack is addressed in WSN while at the same time a method for authenticating the new nodes which try to change the sleep schedule of the nodes is proposed. Only transmissions from valid nodes are accepted. Zero knowledge protocol (ZKP) is used for verifying the authenticity of the sensor nodes which forwards the sleep synchronization messages. Also to enhance security further the interlock protocol is used during key exchange.[3]

Vampire attacks disable the networks by drastically draining the node's battery power. Finding of vampire attacks in the network is not a easy one . A vampire present in the network can increase energy usage in the network. In this paper alternative routing protocols such as Distance Vector routing protocol which consists of Link-State Algorithm and Distance Vector routing Algorithm are used which will be avoiding some sort of problems which are caused by vampire attacks.[4]

DOS attack means that a node couldn't provide required services to other valid nodes, and can be carried out on the every layer in network. In order to preserve limited resources of the nodes, an end-to-end authentication, performance rate of cache memory, two-threshold value, and distributed voting are used in this paper to detect DOS attackers. Through performance analysis and simulations experiment, the scheme would improve the flexibility and preciseness of DOS attack detection, and would improve its security in WN[5],[6],[7]

III. THEORETICAL ISSUES

The work on secure routing attempts to ensure that attackers cannot cause path discovery to return an invalid network path, but Vampires do not affect or alter discovered paths, instead using existing valid network paths and protocol they drain the battery power of network. Protocols that maximize power efficiency are also not effective, since they rely on neighbour node behaviour and cannot optimize out malicious action. Mainly the issues include:-

Power outages.
Lost productivity.
Various DOS attacks.
Security level is low.

IV. PROPOSED METHOD

In the proposed system, mainly two methods are used to detect and eliminate the important class of resource consumption attack called vampire attack which drains the battery power of nodes in the network abnormally. The vampire attacks are stretch attack and carousal attack. The two methods used are EWDA & Routing algorithm.

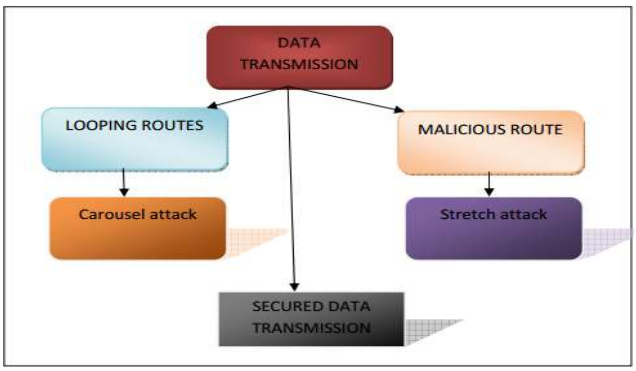

Fig.1 System Architecture: Vampire Attacks.

A. Energy Weight Detection Algorithm

This section focuses on the design details of our proposed protocol EWDA. Where energy of a node gets to threshold level. It plays a vital role by bringing out the energy efficiency of the sensors and rendering the network endurable.

EWDA functions two phases namely:-

Network configuring phase &

Communication phase

1. Network configuring phase

The objective of this phase is to establish a optimal routing path from source to destination in the network. Balancing the load of the nodes and minimization of energy consumption for data communication are the key factors which are considered here. In this phase the node which has the threshold level energy (attacked node) sends ENG_WEG message to all its neighbour nodes. After receiving the ENG_WEG packets the neighbour nodes sends the ENG_REP message that encapsulates information. this information is regarding their geographical position of the node and current energy level of the node. The node after receiving this stores the information in its routing table to for processing further computations. After this the node establishes the routing path. It first traces the very next node by computing the energy required to forward the required data packet, that is suitable energy node and less distant node selected as the next forwarding node. thus the route from source to destination with suitable energy and less distant is fixed. in this way this algorithm avoids data packet dropping. the allotted forwarding node transmits the packets safely to the destination. This algorithm priority is to achieve balancing of load in the network. The node with suitable energy will be assigned as a forwarding node and as long as this suitable node has the capacity to handle. minimal less distant path with multi hop is established to bound the network damage from vampire attack. EWDA avoids the collapsing of entire network by dropping the packets in the network. The load is balanced depending upon the capacity of the nodes. In this way multi hop load balanced network is achieved.

2. Communication Phase

The main objective of communication phase is to avoid the same data packets transmitting through the same node repeatedly so that battery power does not get depleted fast and does not lead to network failure because of vampire attacks. The process of repeating the packets is removed by collecting the data transmitting within the forwarding node and route the remaining packets safely to the destination.

By first copying the content of the packet that is transmitting through the node the data aggregation is achieved. This copied content compares with the data packet that is transmitting through the node and if the transmitted packet is same then node stops the data packet transmitting through them.

Thus it avoids the excessive packets transmitting through the same node again and protect the depletion of batteries fast. Then send the only required data packets through the established node safely to the destination.

Average Energy Consumption for differing message lengths shows the average energy consumption of the network with varying packet size. In the data communication phase transmitting data at varying message lengths of big size and small size respectively. Suppose when message length is small the energy is less than 1J and the energy consumption is greater than 1J when packet size is big. That is when the message length is increased the average energy consumption of the sensor network is greater. This is because of greater overhead involved in aggregating and transmitting a larger sized packet or message. A message length of small size packet as lesser length message may not be in a position to carry out the desired task and a

larger length may unnecessary contribute to addition overhead which can degrade the performance of the network.

Average path length comparison of EWDA path length with attacked or malicious path length. it is clear that Attacked path length takes more Hop count but with EWDA it takes less hop count that is a malicious path takes more hops for a message to reach its destination but with EWDA we can transfer with less hops to reach the destination.

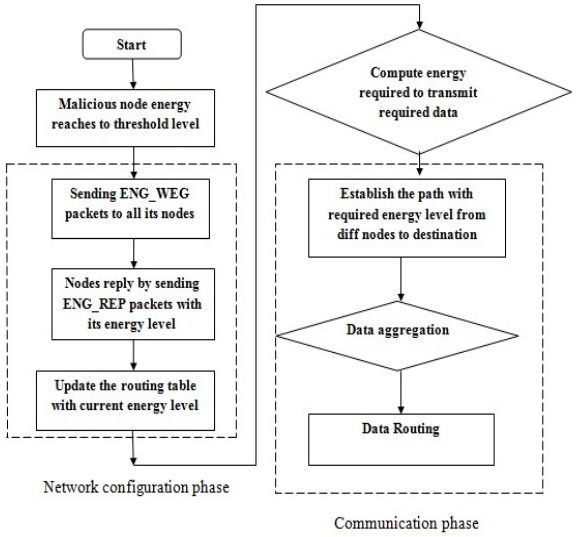

Fig.2 EWDA Flowchart

B. Route Tracking Algorithm

In proposed system Node trust level is assigned and while taking the routing path, the node which is having high trust value is considered for routing. In this, routing is dynamic. To enhance more security in the routing phase, we can include trust factor in the routing path, i.e. routing can be taken considering nodes trust factor. For example, the trust level is denoted as T. Trust value is assigned to each and every node during re-routing, after attack is detected. So trust value is nothing but the numeric value such as 0 or 1, whereas the trust value 0 is considered to be malicious node and trust value 1 is considered as normal node. Based upon that routing path is constructed. The node, which has trusted value 1, will be included in the route rather than the node having trust level 0.

An algorithm for secure routing decision process based on knowledge based trust values of the node is proposed. the source node broadcasts routing request message to its neighbour nodes in order to find a route to the destination node. The neighbours of the source node forward the request to their neighbours if the trust evaluation on the source node passes its predefined threshold, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached. And then that node would like to accept the data transfer based on its trust evaluation. some nodes respond that they have fresh enough route to the destination node , if so happens then the source node checks the trust evaluation using TM System on the responded nodes. the source node selects one preferred route, which it believes the best on the basis of trust evaluation results and hops of the routes.

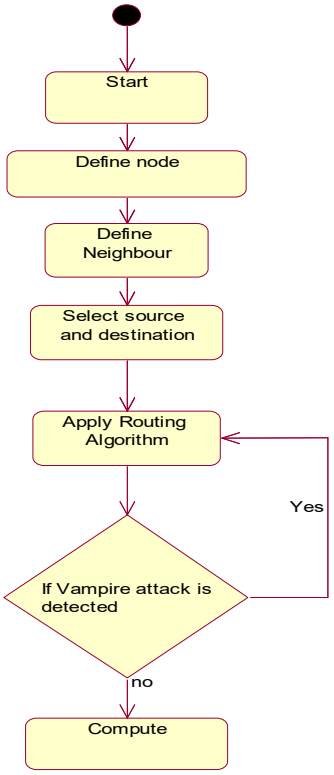

Fig.3Vampire Attack flowchart.

V. IMPLEMENTATION MODULES

A. Network Creation Module

We setup our Network model with Sink, Source and with twenty nodes in the network creation module. unique Identity number is assigned to each node. topology discovery is done at transmission time and we have static protocols, where during an initial setup phase we discover the topology, with periodic rediscovery to handle rare topology changes. Our attackers are malicious insiders and so they have the same resources and level of network access as the honest nodes have. Furthermore, attackers location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was arranged and used and cannot control their final positions

B. Carousal Attack Module

In our first attack, an attacker composes packets with routing loops. We call it the carousel attack, since it sends packets in circle. in the figure it is been shown. It targets source routing protocols by exploiting the finite verification of message headers at forwarding nodes, leading a single packet to repeatedly traverse the same set of nodes in loop pattern . In this attack, an adversary sends a packet with a route composed as a chain of loops, the loop formation is such that the same node appears in the route many times. This method can be used to increase the path length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

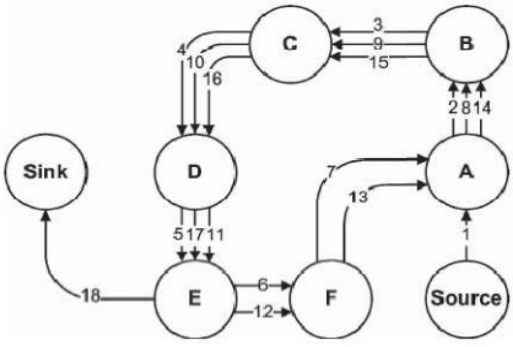

Fig.4 Carousal Attack

C. Stretch Attack Module

In our second attack, source routing is again targeted, an attacker constructs artificially long routes, which leads to traversing every node in the network. We call this as stretch attack, since it increases packet path lengths, which causes packets to be passed by a number of nodes that is free of hop count along the shortest path between the attacked node and packet destination.

An example is illustrated in Fig. 1b. Results show that in a randomly generated topology, a single attacker can use a loop attack i.e. carousal attack to increase energy consumption by as much as a factor of 4, but depending on the position of the malicious node stretch attacks increase energy usage by up to an order of magnitude. The impact of these attacks can be further increased by combining them, increasing the number of attacked nodes in the network, or simply sending more packets. The networks that do not employ authentication or only use end-to-end authentication, attackers are free to replace routes in any overhead packets, we assume that only messages originated by adversaries may have maliciously composed routes.

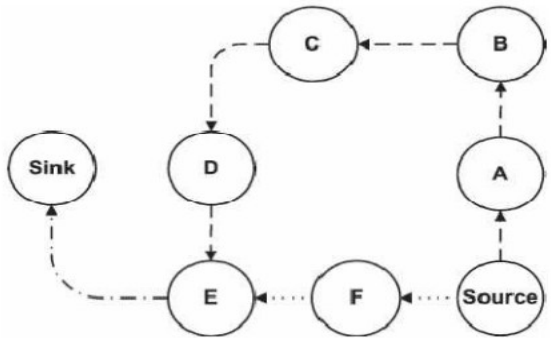

Fig.5 Stretch Attack

D. Vampire Attack Detection Module

This module uses energy weight detection algorithm in which the Network configuration Phase to detect stretch attack if initial value of number of hop count exceeds, then reroute the path. Communication Phase is used to detect carousal attack if same data packets transmitting through the

same node repeatedly. Each node maintains a log file which contains the source, destination and packet id. Whenever a packet arrives each node check the log file and compare the packet id for the source- destination pair of packets. The energy spent for this checking is less compared to the energy drained using infinite looping of a single packet

E. Transmission Analysis Module

This Module Uses Route Tracking Algorithm. This involves facilitating the tracking of all transmission details and its utilization to generate analysis output. This module therefore includes analysing the performance of the network in terms of end-to-end delay generated and throughput observed during the executions.

VI . PERFORMANCE EVALUATION

The above proposed system is implemented in network simulator-2 (NS2). The performance evaluation is calculated on the basis of throughput, energy consumption , end to end delay, packet delivery ratio and packet loss.

1. THROUGHPUT

Throughput is defined as the number of successful packet received at the destination.

Bit rate = ((bytes + hold rate1)*8)/2*time*1000000

2. REMAINING RESIDUAL ENERGY

Energy consumption is defined as the amount of energy consumed by a network process.

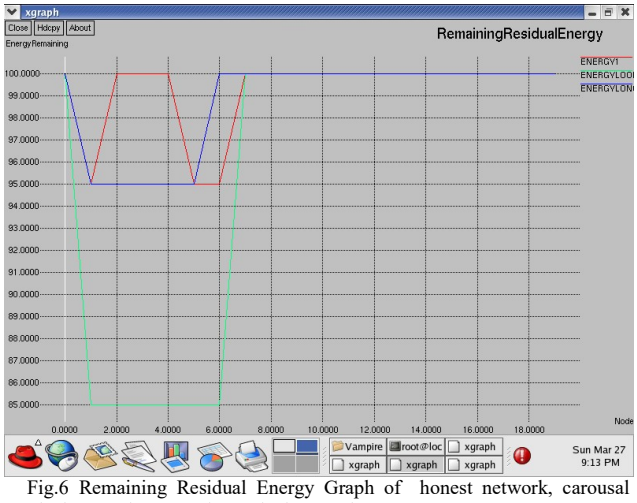

Fig.6 Remaining Residual Energy Graph of honest network, carousal attacked network & stretch attacked network.

3. END TO END DELAY

End-to-end Delay : the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

Packet Delay = (Last received packet time- hold time) / (total no of packets - holding sequence)

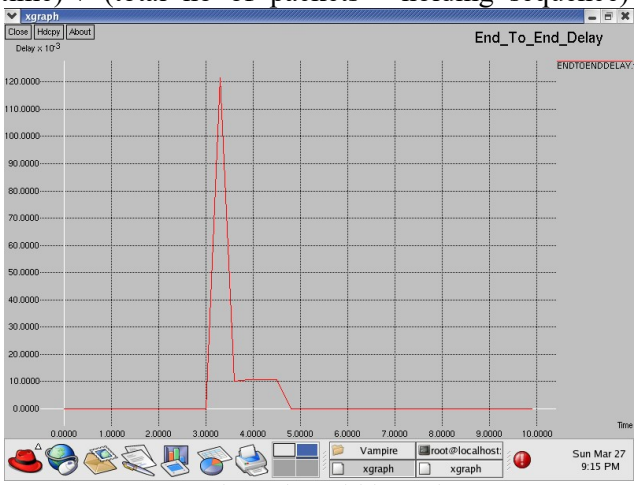

Fig.7 End to End delay graph

4 . PACKET DELIVERY RATIO

Packet delivery ratio : the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol.

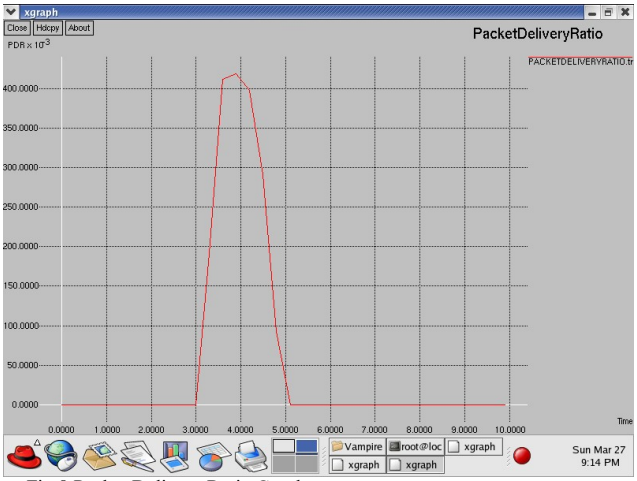

Fig.8 Packet Delivery Ratio Graph

5. PACKET LOST

Packet Lost : the total number of packets dropped during the simulation.

Rate of packet loss = (No. of packet loss) / Time

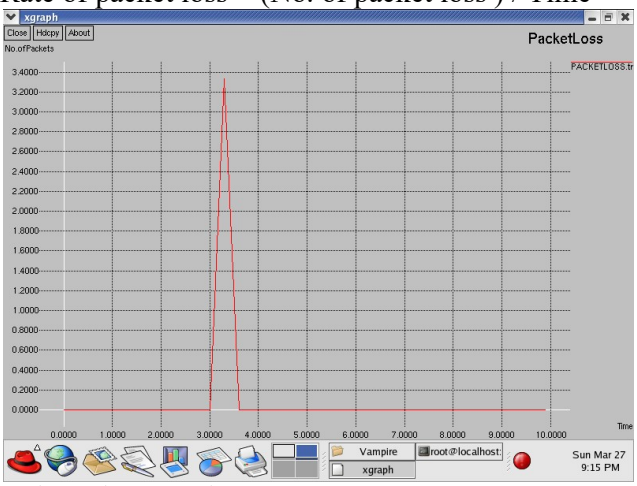

Fig.9 Packet Lost graph

VII . CONCLUSION

In this paper we define vampire attack as an resource depletion attack in which it consumes more battery of the node. Vampire attack are carousal attack and stretch attack .This attack not depends on any particular type of protocol. In proposed system use energy consumption and trust value of the node to mitigate vampire attack. The simulations results show that we are able to detect the attacks on the basis of energy consumption and prevent these attacks by using trust factors for secure routing The proposed prevention technique is used to reduce vampire attack using new protocol and route recovery technique to decrease the energy loss due to packet transmission over the unwanted route in the network.

ACKNOWLEDGMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of this project.

I express my warm thanks to my project guide and mentor Prof. Shilpa Verma for her guidance and motivation and Head of Department (Computer), Mr. Jayant Gadge for his help and guidance. Obviously a publication is not complete without the help from those who choose to stay behind the scenes and yet provide the little things that stand out. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project. Finally I thank my Parents, it is their support and encouraging presence that helped build morale. And above all, God, who keeps blessing us despite our flaws.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper, Vampire Attacks: Draining life from wireless Ad-Hoc Sensor networks. IEEE Transactions on Mobile computing, Vol. 12, No. 2, February 2013

[2] https://en.wikipedia.org/wiki/Routing.

[3] Swapna Naik and Dr Narendra Shekokar, Conservation of energy in wireless sensor network by preventing denial of sleep attack. International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[4] G. Vijayanand, R. Muralidharan, Overcome Vampire Attacks problems in wireless ad-hoc sensor network by using distance vector protocols. International Journal of Computer Science and Mobile Applications,Vol.2 Issue. 1, January- 2014

[5] Liangyu Luan,Yingfang Fu, Peng Xiao, An effective Denial of Service Attack Detection Method in Wireless Mesh Networks. International Conference on Medical Physics and Biomedical Engineering, Physics Procedia 33 (2012) 354 – 360.

[6] Mrs. Roshani Sahare Chandekar , Prof. Vinod Nayyar, Defending Against Energy Draining Attack in Ad-hoc Sensing Network, Universe of Emerging Technologies and Science, Volume I Issue VI , November 2014.

[7] https://en.wikipedia.org/wiki/Ns_(simulator)