Vampire Attacks: Detection and Prevention

[1]Riddhi Jagdish More, [2]Priyanka Bharat Beldar, [3]Mayur Ashok Chaudhari, [4]Pritesh Anilkumar Raka

BE Students
Computer Engineering Department
SSBT's COET Bambhori, Jalgaon

***Abstract*: Wireless Sensor Network (WSNs) is used nowadays, and therefore it has very large number of interesting applications. WSN can be of hypersensitive nature and therefore might require enhanced secured environment because 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 resource consumption attacks called a vampire attack. 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 lead to traversing almost every node in the network. Stretch attack, increases packet routes length, and packets get processed by a number of nodes. Carousel attackers introduce some packet of 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 weights monitoring algorithm and Route tracking algorithm, so energy consumption is reduced to a great extent. EWMA and Route tracking algorithm is used to detect and prevent the above problems.**

Introduction:-

Background:-

In day to day life the computer networks become more popular especially ad-hoc wireless sensor networks (WSN). Its applicability and popularity attracts some miss users for malfunctioning and disturbing the network traffic. The ad-hoc networks are the temporarily established wireless networks of doing specific task, which do not to require fixed infrastructure. Each node functions as base station and as router forwarding packets for other nodes in network. There are various types of attacks of sensor network but among all attacks denial of service attack is most dangerous attack. Denial of service attacks make the network resources are unavailable to users. Vampire attacks are one of the type of denial of service attack. In vampire attack transmission of a message causes more energy consumed by the network node. After consuming more energy, nodes can be discharging and it can be disconnected from the network. Vampire attacks are not protocol-specific i.e. they do not rely on any specific protocol. Vampire attack constitutes of two different types of attacks called stretch attack and carousel attack. These two mainly focuses on reducing the energy of the nodes. For the prevention of vampire attack use the energy weight monitoring algorithm (EWMA) and trust value of the node.

Motivation:-

In military applications Ad-Hoc network is deployed for communication purpose. That communication is done by either data transmission or voice communication. In both cases security is measuring concern through which no can intercept transmission information. Security is breakable by different types of attacks out of which much more dangerous attack is vampire attack. Hence to implement secured network of vampire attack it need to implement a system, which will detect and prevent these types of attacks. It will helpful for application purpose areas and avoid the misuse of their operations.

II. RELATED WORK

A very early mention of power exhaustion attacks can be found as “sleep deprivation tortures.” As name suggest, the attack obstructs 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 defense 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 assign 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 lead 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). It can be modified to prevent vampire attacks because its original version is vulnerable to vampire attack.

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.

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 between destinations. PLGP is the protocol that reduces vampire attack. Path attestation includes the extra verification like it checks a corresponding entry to the signature chain, and should be logically 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 neighbor. 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 a 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 to WSN while at the same time a method of authenticating the new nodes which try to change the sleep schedule of the nodes is proposed. Only transmissions of 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 furthers the interlock protocol is used during key exchange. [3]

Vampire attacks to disable the networks by drastically draining the node's battery power. Finding of vampire attacks in the network are not an 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 is 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 to 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 neighbor node behavior 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, two methods are used to detect and prevent the 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 EWMA & Routing algorithm.

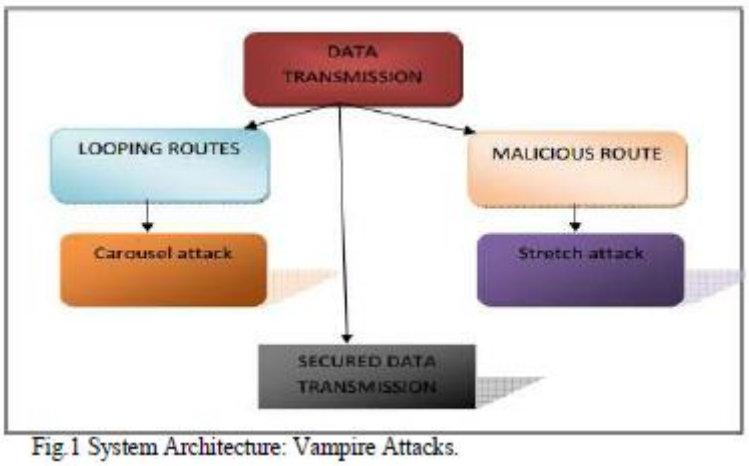


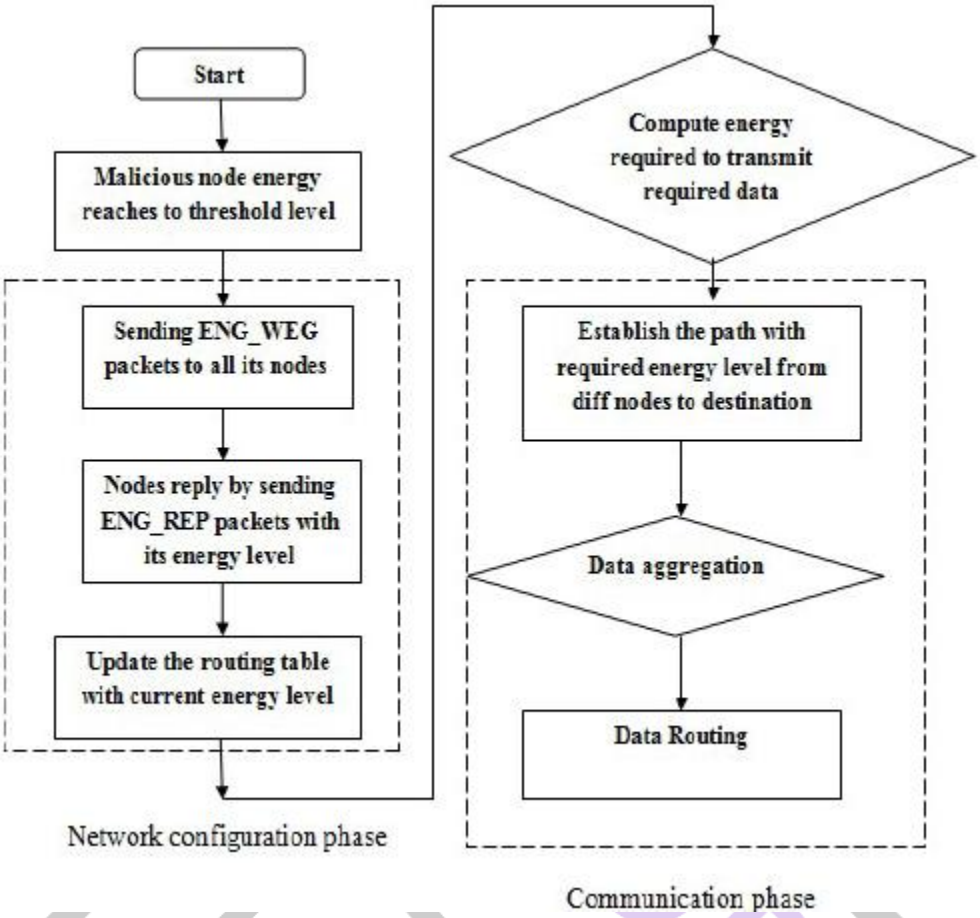
Fig.1 System Architecture: Vampire Attacks.

A Energy Weight Monitoring Algorithm This section focuses on the design details of our proposed protocol EWMA. Where energy of a node gets to threshold level. It plays a very 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 an optimal routing path of source to a destination in the network. Balancing the load of the nodes and minimization of energy consumption of data communication is 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 its entire neighbor. After receiving the ENG_WEG packets the neighbor nodes send the ENG_REP message that encapsulates information. This information about their geographical position of the node and current energy levels 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 neighboring node by computing the energy required to forward the required data packet, that is suitable energy nodes and less distant node selected as the next forwarding node. Thus the route from source to a destination with suitable energy and less distant is fixed. In this way this algorithm avoids data packet dropping. The allotted forwarding node. 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. Minim less distant path with multi hop is established to bind the network damage from vampire attack.
EWMA avoids the collapsing of entire network by dropping the packets in the network. The load is balanced depending upon the capacity of nodes. In this way multi hop loads balanced network is achieved.

2. Communication Phase The main role of communication phase is to avoid same data packets transmitting through the same nodes repeatedly so that battery power does not get depleted fasts and does failure because of vampire attacks. Repeated packets are removed by collecting the data transmitting within the forwarding node and route the remaining packets safely to the destination. First copying the content of packet that is transmitting through the node the data aggregation is achieved. This copied content to compare with the data packet that is transmitting through the node and if the transmitted packet is same then the node stops the data packet transmitting through them. Thus it avoids the excessive packets transmitting through the same node again and protects depletion of batteries fast. Then send only required data packets through the established node safely to the destination.
Average Energy Consumption for differing message lengths shows average energy consumption of the network with varying packet size. In the data communication phase transmitting data at varying message length of big size and small size respectively. Suppose that 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 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 position to carry out the desired task and a larger length may unnecessary contributes to addition overhead which can degrade the performance of the network.
Average path length comparison of EWMA path length with attacked or malicious path length. It is clear that Attacked path length takes more Hop count but with EWMA it takes less hop count which is a malicious path takes more hops for a message to reach its destination but with EWMA we can transfer with less hops to reach the destination.



B. Route Tracking Algorithm

In proposed system Node trust level is assigned to node 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 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 nodes 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 as a 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.

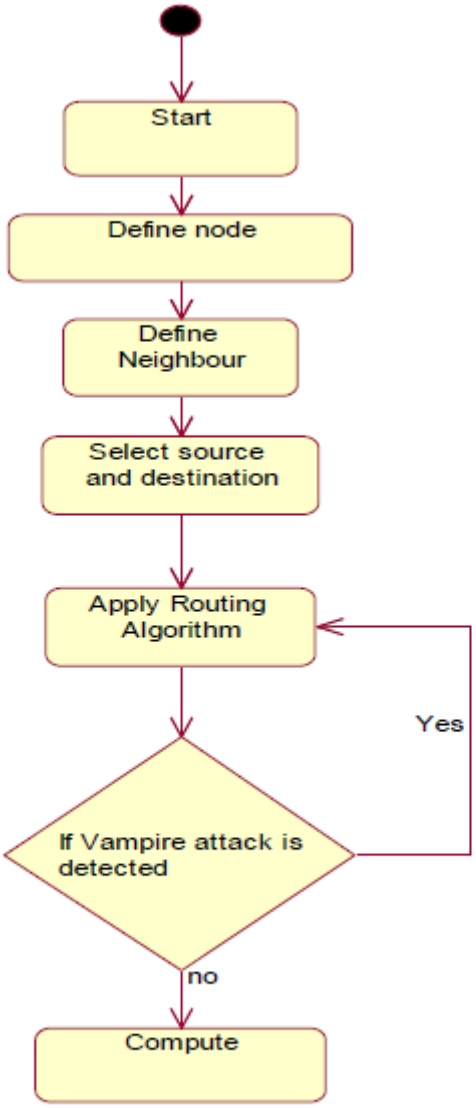


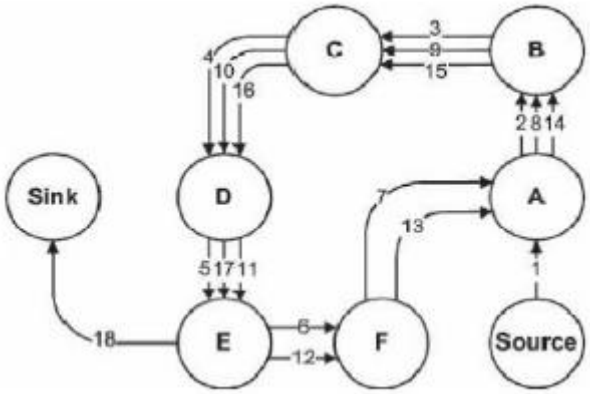
Fig.3Vampire Attack flowchart.

Based on knowledge trust values of the node is proposed. The source node broadcasts routing to request message to its neighbor nodes in order to find a route to the destination node. The neighbors of the source node forward the request to their neighbors if trust evaluation on the source node passes its predefined threshold, and so on, until either 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 destination, 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 best on the basis of trust evaluation results and hops of the routes.

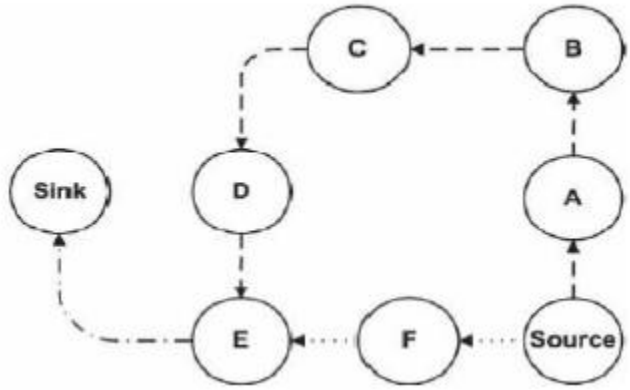
V. IMPLEMENTATION MODULES

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 initial setup phase we discover the topology, with periodic rediscovery to handle rare topology changes. Our attackers are malicious insiders and they have the same resources and level of network access as the honest nodes have. Furthermore attacker's 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 being shown. By developing source routing protocol it limits verification of message headers at forwarding nodes, results in a single packet to repeatedly traverse 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 nodes appear in the route many times. This method can be used to increase the path length across the number of nodes in the network, only limited by the number of allowed entries in the source route.



C. Stretch Attack Module In our second attack, source 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, packets to be passed by a number o 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 at 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 outcome of these attacks can be increased by combining the increasing number of attacked nodes in the network, or simply sending more packets. 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.



Vampire Attack Detection Module

This module uses energy weight detection algorithm in which the Network configuration phase is to detect stretch attack, if initial value of number of hop count exceeds, then re-route the path. Communication Phase is used to detect 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. It involves facilitating the tracking of all transmission details and its utilization to generate analysis output. This module therefore includes analyzing the performance of network in terms of end-to-end delay generated and throughput observed during the executions.

PERFORMANCE EVALUATION

The above proposed system is implemented in Java. The performance evaluation is calculated on the basis of throughput, energy consumption, end to end delay, and 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.

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)

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.

5. PACKET LOST

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

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

Conclusion:

In this paper we discussed vampire attack as a resource depletion attack in which it consumes more battery of the nodes. Vampire attacks are carousal attack and stretch attack .This attack does 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 and prevent the attacks on the basis of energy consumption.

REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper, Vampire Attacks: Draining life from wireless Ad-Hoc Sensor networks. IEEE Transactions on

[2] hMttposb:i/l/ee nc.owmikpiupteindgia, .Vorogl/.w 1i2k,i /NRoo.u 2ti, nFge.b ruary 2013

[3] Swapna Naik and Dr Narendra Shekokar, Conservation of energy in Iwnitreerlneastsi onsaeln sCoor nfneeretwncoer ko nb yA dvparenvceendt iCngo mdpeuntiinagl Toef chsnleoelopg ieastt aacnkd. Applications (ICACTA-2015).

[4] Gi.n V wijiaryealensasn add, -Rh.o cM suernasloidrh naeratwn,o rOkv beryc oumsine gV daimstpanircee Avtetcatcokrs pprrootbolceomlss. 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 oAfg aEinmste Ergnienrgg y TDercahinnoinlogg Aietsta cakn idn ASdc-ihenocce S, enVsionlugm Nee twI orIkss, uUen ivVeIr se, November 2014.