Energy Effectual Trust Based Technique for Prevention of Vampire Attack

Jitendra R. Patil[1], Prof. Preetesh Purohit[2], Prof. Manish Sharma[3]

[1]M.Tech. Student, [2]Head & Associate Professor, [3]Guide & Assistant Professor
Department of Computer Science & Engineering
SVCE, Indore, Madhya Pradesh, India

***Abstract*—Wireless ad-hoc sensor network is noticeable platform for communication and research. Wireless Adhoc sensor network is defenseless to Denial of Service (DOS) attack. Denial of service attack (DOS) makes resources are blocked and not presented to users. This Denial of service attack is formright condition for Vampire attack and make main effect for it. In Vampire attack it makes the node to exhaust more battery power and reduces the network performance. Vampire attackdoes not rely on any particular type of routing protocol.In proposed system energy consumption and trust value iscalculated for each node to mitigate the vampire attack.**

Keywords-Denial of Service, Wireless Sensor Network, ad-hocnetwork, routing.

I. INTRODUCTION

Wireless sensor network (WSN) is promise of providing thecommunication in complex environments. Nodes in Wirelesssensor networks are connected to each other and forms thenetworks. These nodes are use in various application such asto monitor environmental condition, provided thatcommunication services in military. All this applicationrequires node is more trustworthy and well-suited. Node isgetting the power from its battery for performing its job .Ifthe node uses more battery power for its work then itslifetime is less and that node can disconnected from thenetworks. This makes the performance of the network isreduces. The wireless sensor network (WSN) is ad-hoc innature so it is helpless to Denial of service attack [1].Generally Denial of service (DOS) attack is anattempt to make a machine or network resource unavailableto its intended users. There are various types of DOS attacksuch as jamming the signal, power exhaustion and floodingwith useless traffic. In power exhaustion adversary is attackson the node and consumes more battery power of the node [8].Vampire attack is one of the type of power exhaustion attack.In carousel attack adversary sends the packet in routing loopand in stretch attack adversary sends the packet in longestpossible path so that it consumes more battery power of thenode[8].In vampire attack node is consumes more batterypower for its packet transmission. If the node consumes morebattery power then it can be discharge and disconnectedfrom rest of the networks. Vampire attack forms by thecombination of carousal and stretch attack. These two attacksmainly focus on decreasing the energy of the nodes.

A) Carousal Attack

In Carousel attacks, an adversary sends the packets inrouting loop as shown in figure1. In figure 1 packet issending from source to sink. If we send packet from source tosink then shortest path is from source - node f- node E - Sink.But here packet is not follows shortest path. Adversaryattacks on the network and forms the loop as shown figure1 [8]. Packet is send from source to node A. Node A forwardpacket to node B. then node B sends packet to node C. Node C forward packet to node D. then node D send packet to nodeE. Then node E instead of forwarding packet to Sink, it isSends packet to node F. Then node F forward packet to nodeA and forms loops [8]. Then same path is repeated for manytimes and it causes more energy consumed by the nodes. So,because of these energy depletion performance of thenetworksdegrades [8].

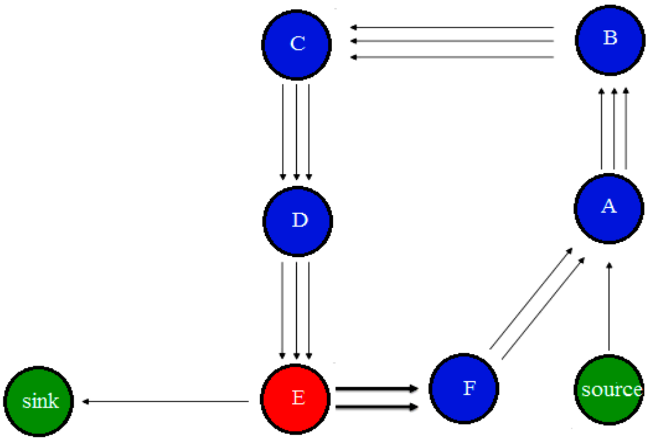

Figure1:An honest route exit the loop immediately from E to the sink, but malicious packet makes it way around the loop twice more before exiting.

B) Stretch Attack

In Stretch attack, an adversary constructs artificiallylong routes and potentially traversing every node in thenetwork[8].In these attack it increases packet path length.Infigure 2 packet sending from source to sink. The shortest pathfor forwarding packet is source-node F-node E-Sink but herein Stretch attack, an adversary forward packet in longest pathas shown by dark line in figure2[8]. So it increases energyusage by the network. As carousel attack is depending onposition of attackers, Stretch attack is more effective and thisattack is independent on attacker's position relative to the destination. The impact of these attacks can be furtherincreased by combining both Carousel and Stretch attack and increasing the number of adversarial nodes in the network. Although network does not employ authentication or network use only end-to-end authentication. So here adversary can replace routes in any overhead packets [8].

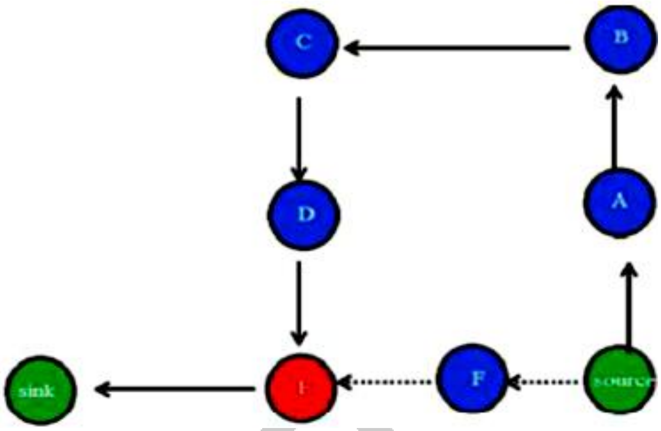

Figure 2: Honest route is dotted while malicious route is dashed. The last line is to the sink is shared.

II. Literature survey

Power draining attack is not perfectly mitigate at routinglayer. Power draining found in Denial of sleep attack. Denial of sleep attack to keep away the node to enter in to low power sleep mode and consumes more battery power.In This adversary host based lightweight intrusion detection technique, Clustered Adaptive Rate Limiting based on the rate limiting approach at MAC layer is proposed to prevent denial of sleep attacks. The primary shortcoming of above technique is that the period during which nodes are awake is not synchronized, so if a node has packet to send, there is no guarantee that other nodes will poll at proper time to overhear a portion of preamble and remain awake for the data packet. The technique used in B-MAC increases latency in multi hop networks and if bursts of network traffic are generated at a higher rate than is supported by rate-limiting policy, network traffic is lost. So in adaptive rate limiting, network traffic is prohibited only when malicious packets have been sensed at a rate sufficient to suspect the attack. That technique can be used to maintain network lifetimes and better throughput at a time even in face of sleep deprivation attack.

In path based Denial of Service (DOS) attack adversaries'attacks on network by flooding the data packet along multihop end to end communication path [3]. Path based DOS attack is easy to launch and disabling large portion ofwireless sensor network. To defend against path based DOSattack an intermediate node must able to detect spuriouspacket or replayed packet and then reject them. For thedetection of spurious packet use lightweight securemechanism to defend against path based DOS attack. In thismechanism configures one way hash chain along a pathenabling each intermediate node to detect a Path based DOSattack and prevent propagation of spurious or replayedpacket.Another attack can be possible through path based DOSattack is wormhole attack [4].

In wormhole attack adversaryrecord the packet or individual bit of packet at one location.After recording the packet tunnel it to the other location andthen replays them in to the networks from that point. Thistunnel distance is longer than normal wireless transmissionrange of single hop. Packet leash is used for detection ofwormhole attack. In packet leash sender node uses temporalpacket leash and geographical packet leash. In temporalpacket leash sender node uses its timestamp i.e. sending timeof the packet. In geographical packet leash sender Uses itslocation and sending time of the packet to receiver.

In DOS adversary can be disturb communication.itestablish routes through themselves for drop, monitor andmanipulates the packet. Some protocols are providingsecurity on path discovery and ensure only valid path arefound. But this cannot protect against vampire attack.Vampire cannot use illegal path for communication.

In SYN Flood attack adversary attacks on the networkand depletes the resources such as CPU time, bandwidth andthat cause the problem in the network. In this adversarymakes the multiple connections with the server and allocatesthe more resources. Such attack can be prevented by usingSYN cookies [5]. It form minimal load on the client whoinitiated with small number of connections and preventadversary or malicious node to consume more number ofconnections.

III. EXISTING SYSTEM

In Existing system uses AODV for routing. In AODV sourcenode broadcast the route request (RREQ) message across thenetwork [1]. The neighbouring node receives this requestmessage and updates their information for source node to setup backward pointers for source node in routing table. Routerequest (RREQ) message contain source node IP address,current sequence number and broadcast ID. The nodereceiving route request (RREQ) message send routereply (RREP) message to the source node. If source node notgetting any response then it rebroadcast the routerequest (RREQ) message. The node keeps the track of routerequest's (RREQ) source IP address and broadcast ID. If theyreceive a route request (RREQ) which they have alreadyprocessed, they discard the route request (RREQ) messageand do not forward it. As the route response (RREP)propagates back to the source nodes set up forward pointersto the destination [1]. Once the source node receives the routeresponse (RREP), it may begin to forward data packets to thedestination. The major drawback of AODV has it do notprovide any security mechanism. AODV performs its basicoperation only.

IV. PROPOSED SYSTEM

In proposed work vampire attack prevented by using energyweight monitoring algorithm (EWMA) and findingcorresponding trust value of each node. For preventingvampire attack first detect carousal and stretch attack. Afterdetection of carousal and stretch attack reduce their impact inwireless sensor networks by using energy weight monitoringalgorithm (EWMA) [8].Then finding trust value of each nodein the network for performing routing operation.In this paper we use three steps to prevent vampire attack. Inthe first step reduce the impact of carousal attack. Reduce theimpact of stretch attack in second step. In third step performsecure routing based on trust value.

Step 1: Reduce impact of carousal attack

As we see in the carousal attack in figure1 it formthe loop for forwarding the packet. These repeatedlytransmission of same packet through same node depletesmore battery power of the node and degrade the networkperformance. The process of repeating the packet iseliminated by aggregating the data transmitting withinforwarding node. In data aggregation copy the content of thepacket which is transmitting through the node. This copiedcontent compare with the data packet transmitting through thenode. If the transmitted packet is same as the copied packetthen stop the packet transmitted through them. In this way itavoids the redundant packet transmitting through the samenode and protect from the carousal attack

Steps:

1. Initialize source and destination node in networks
2. Source node sends packet to its neighbouring node.Then neighbouring node forward packet to its nextnode till packet reaches its destination.
3. If loop is detected then it is identified as carousalattack.
4. Perform data aggregations for each node.
5. If (transmitted packet= = copied packet)
Then discard the packet
6. Stop packet transmission

Step 2: Reduce impact of stretch attack

In stretch attack adversary is finding artificially longroute. For find out malicious node in the network every nodeis add the test field while receiving the packet and forwardpacket to next node. Then test field is check for each node. Ifthe test field is correct then normal operation is continue andif the test field is wrong then create an alarm packet. Thenalarm packet is broadcast and announces that node ismalicious so that it avoid for further communication.In stretch attack use energy weight monitoringalgorithm (EWMA)[8].In this algorithm use energy of thenode for identified adversary and perform routing operation.Attacked node consumes more energy and reaches thresholdenergy level. In this phase the node with threshold levelenergy (attacked node) sends ENG_WEG message to all itssurrounding nodes. After receiving the ENG_WEG packetsthe surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographicalposition and current energy level. The node upon receivingthis stored in its routing table to facilitate furthercomputations.

Steps:

1. Initialize source and destination node in networks
2. For finding adversary added test field whilereceiving packets.
3. If (Test field of current node= = Test field of nextnode)
Then
Continue
Else
Create alarm packet
4. If Node energy> =Threshold energy
Broadcast alarm packet and announce that node ismalicious
5. Then malicious node broadcast ENG_WEG packetto its all neighbour nodes.
6. After receiving ENG_WEG packet neighbour nodesends ENG_REP packet that contain geographicalposition and current energy level of the node.
7. Stored in routing table for routing purpose.

Step 3: Secure Routing based on Trust value

For performing routing operation calculate trustvalue for each node. Node sometimes fails to transmit and start dropping packets during the transmission. Such nodesare responsible for untrustworthy routing. Trust based scheme can be used to track untrust nodes and isolate them fromrouting. Find out trust value of each node by calculating total packets they transmit, total packets they receive and totalpacket they drop [7].Attacker node which is having low trustvalue is eliminated from data transmission. Node with hightrust value is selected and that leads to reliable datadelivery [7].Trust value calculation is based on parametersshown in table 1.Count type describe whether transmission is successful or failure.

Count type	RREQ	RREP	Data
Success	Qrs	Qps	Qds
Failure	Qrf	Qpf	Qdf

Table 1: Node trust calculation parameters

RREQ and RREP are route request and route replymessages respectively which are exchanged between thenodes. Qrs is query request success rate which is calculatedfrom number of neighbour node who have successfullyreceived RREQ message from source node [7]. Qrf is queryrequest failure rate which is calculated from number ofneighbour node who have not received RREQ message fromsource node[7]. Qps is defined as the query reply success ratewhich is calculated as successful replies (RREP) received bythe source node who broadcast RREQ. Qpf is defined as thequery reply failure rate which is calculated based on thenumber of neighbouring nodes which have not sent the repliesfor the query request. Qds is defined as the data success ratecalculated based on successfully transmitted data and Qdf isdefined as data failure rate calculated based on data whichhave failed to reach destination.

$$Qr = (Qrs-Qrf)/(Qrs+Qrf)$$
$$Qp = (Qps-Qpf)/(Qps+Qpf)$$
$$Qd = (Qds-Qdf)/(Qds+Qdf)$$

Where Qr, Qp and Qd are intermediate values thatare used to calculate the nodes Request rate, Reply rate andData transmission rate. The values of Qr, Qp, and Qd arenormalized to fall in range of -1 to +1. If the values fallbeyond the normalized range then it clearly shows that thefailure rate of the node is high and denotes that thecorresponding node may not be suitable for routing[7].Trust value of each node is calculated from Qdwhich gives data transmission rate. Energy consumption forevery node calculated above in step 2.Adversary is having thelower trust value and consumes more energy. So the nodewith low trust value and more energy consumption isdiscarded from the network.

Steps:

1. Calculate the Qr, Qp, and Qd for each node in thenetwork
2. Calculate the trust value of node by considering datatransmission rate i.e. Qd
3. Sorted in the routing table according to trust value
4. The node with low trust value and more energyconsumption is eliminated from data transmission
5. Node with high trust value and low energyconsumption refer for routing.
6. Perform routing operation in the network

V. RESULT AND DISCUSSION

The above proposed system implemented in networksimulator-2(NS2).For the result we discuss throughput,energy consumption by the node and delay. Throughput isdefined as the number of successful packet receives at thedestination. The average time taken by a data packet to arrivein the destination is referred as delay. It also includes thedelay caused by route discovery process and the queue in thedata packet transmission. Only the data packets thatsuccessfully delivered to destination that countered. Energyconsumption is defined as the amount of energy consumed bya network process.

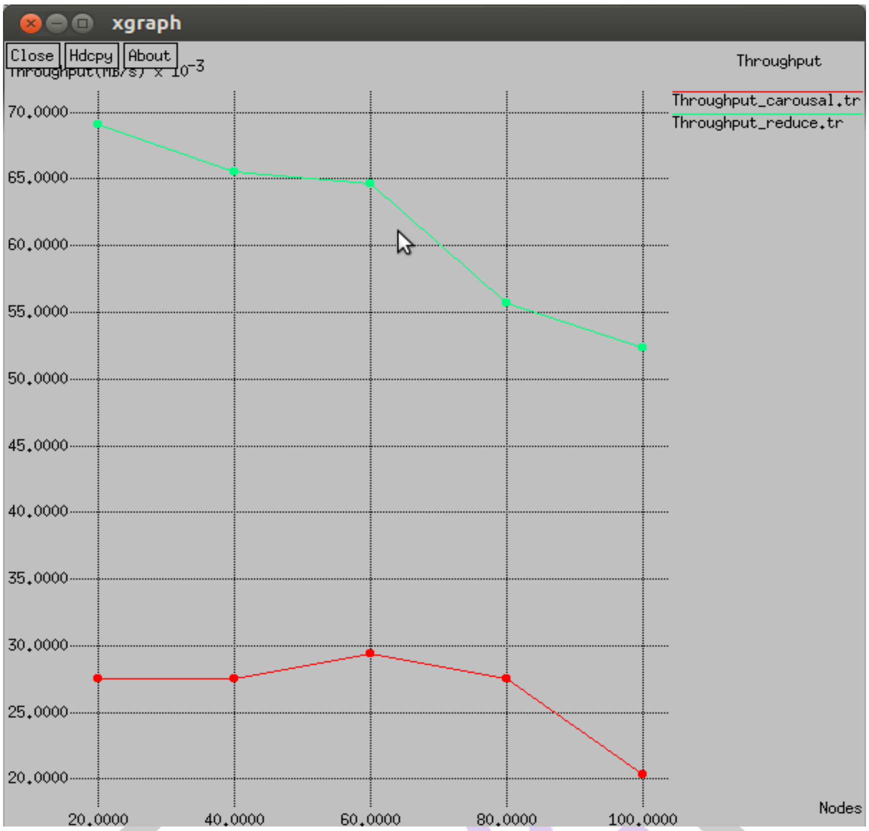

Figure 3: Comparative Graph of Carousal Attack for Throughput

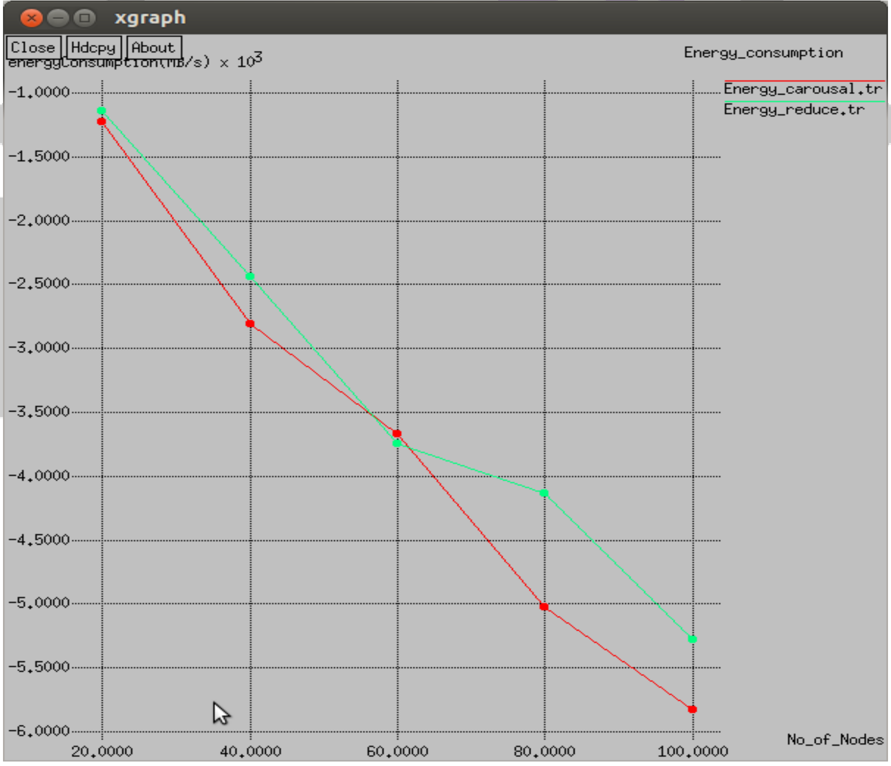

Figure 4: Comparative Graph of Carousal Attack for Energy Consumption

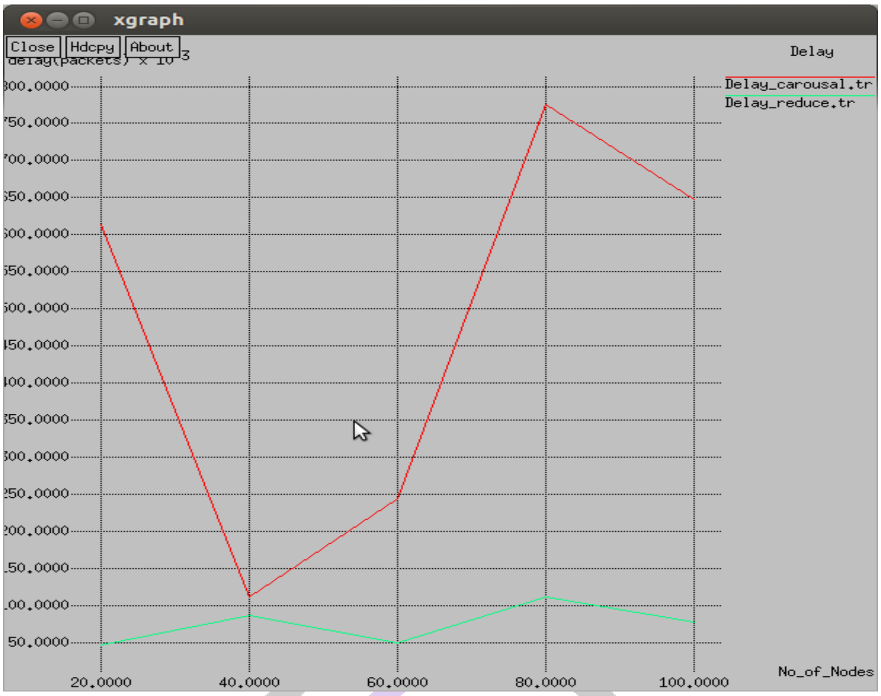

Figure 5: Comparative Graph of Carousal Attack for Energy Consumption

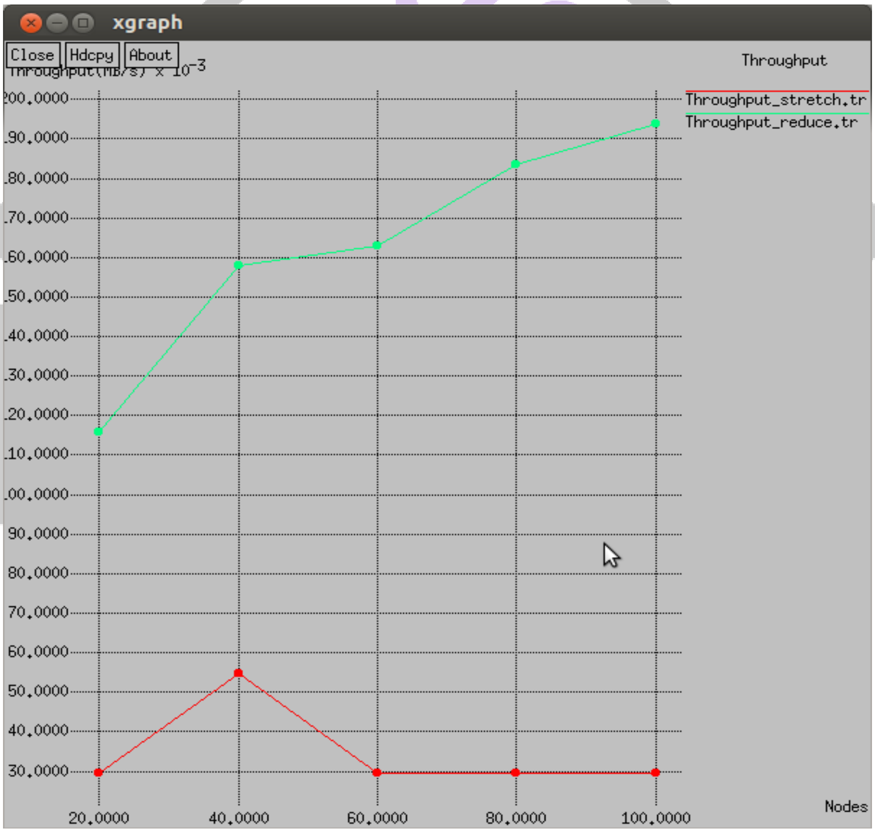

Figure 6: Comparative Graph of Stretch Attack for Throughput

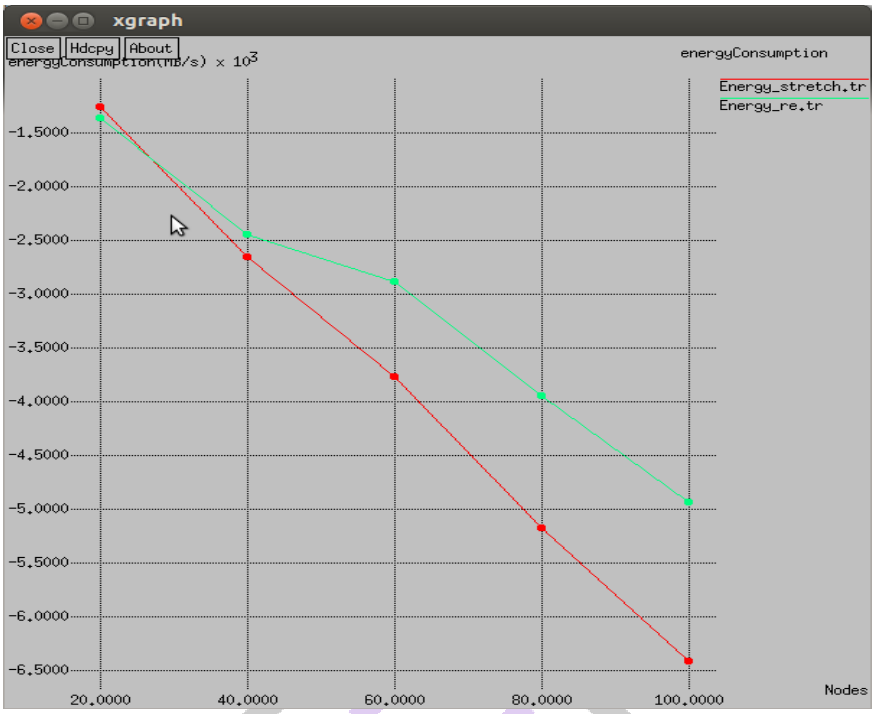

Figure 7: Comparative Graph of Stretch Attack for Energy Consumption

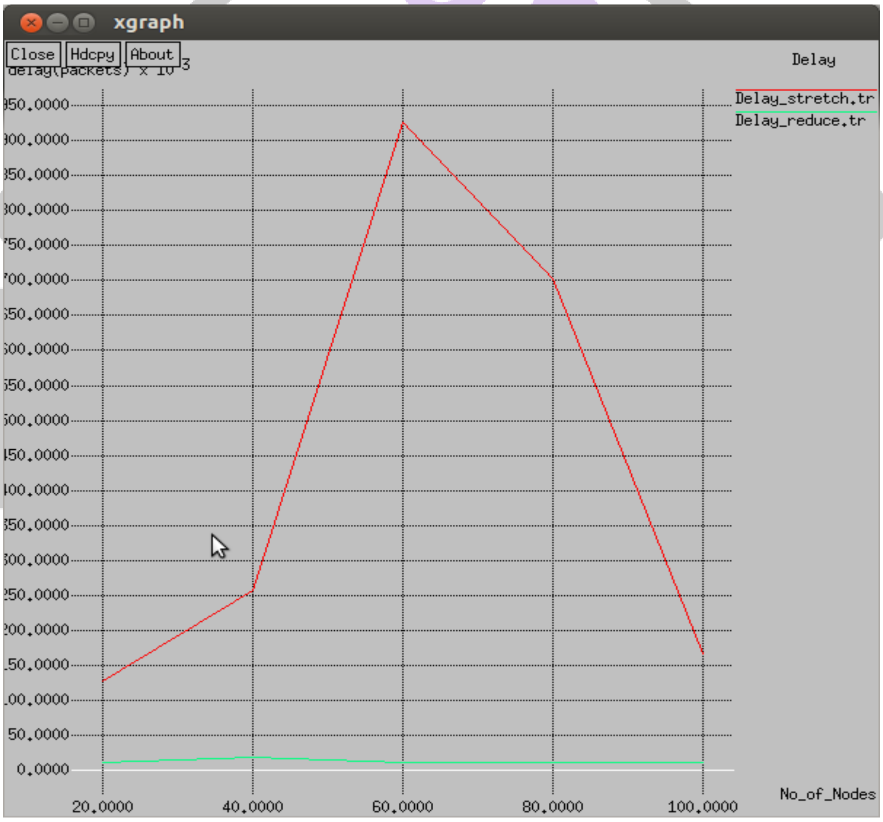

Figure 8: Comparative Graph of Stretch Attack for Delay

Table 2: Results of Carousal Attack

No. of nodes	Carousel Attack		
	Throughput	Delay	Energy
20	68.8441	46.7895	-1260.612398
40	65.5675	87.4385	-2440.22862J
60	64.6271	49.4122	-3744.74090J
80	55.6682	11.1651	-4277.34080J
100	52.386 3	78.6075	-5324.87364J

Table 3: Results of Stretch Attack

No. of nodes	Stretch Attack		
	Throughput	Delay	Energy
20	17.8441	16.3459	-1332.398361 J
40	54.7871	25.7638	-2453.98923
60	62.6472	92.652	-2887.88649
80	83.9634	70.3174	-3947.6854050
100	94.6574	16.6992	-4937.684402

Above we see comparative graph of carousal attack and stretch attack for throughput and energy consumption. Throughput is increased after reducing carousal attack as shown in figure3.for stretch attack also throughput is increases as shown in figure4. The result for each parameters are shown in above tables. In proposed work uses energy consumption and trust value for prevention of vampire attack. It improves the security in wireless sensor networks. The throughput of Energy Weight Monitoring algorithm (EWMA) is always better as compared to AODV even by increasing the number of nodes and by varying the speed.

CONCLUSION

In this paper we define vampire attack as resource depletion attack in which it consumes more battery of the node. Vampire attack is one of the type of Denial of Service attack (DOS) .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 the impact of this attack reduced in great extent. A full solution is not given yet but some amount of damage was avoided. In future we improve our techniques to prevent DOS attack which are not able to stop vampire attack fully.

REFERENCES

[1] Eugene Y. Vassermann and Nicholas Hopper "Vampire Attacks:Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Trans.Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.
[2] Raymond D. R., Marchany R. C., Brownfield M. I., Midkiff S. F.,"Effects of Denial-of Sleep Attacks on Wireless Sensor Network MACProtocols", IEEE Transactions on Vehicular Technology, Vol. 58, Issue1, pp. 367-380, January 2009.
[3] Jing Deng, Richard Han, and Shivakant Mishra "Defending againstPath based DoS Attacks in Wireless Sensor Networks" ACM workshopon security of ad hoc and sensor networks, 2005.
[4] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.[6] David R. Raymond and Scott F. Midkiff, "Denial-of-service inwireless sensor networks: Attacks and defences", IEEE PervasiveComputing 7 (2008), no. 1.
[5] Sridhar Subramanian and Baskaran Ramachandran "Qos Assertion inMANET Routing based on trusted AODV (ST-AODV)", InternationalJournal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3,No.3, June 2012
[6] Jitendra Patil and Manish Sharma "Survey of Prevention Techniques for Denial Service Attacks (DoS) in Wireless Sensor Network"International Journal of Science and Research (IJSR), Volume 5 Issue 3, March 2016
[7] Bhuse, Vijay Subhash, "Lightweight Intrusion Detection: A Second Line of Defence for Unguarded Wireless Sensor Networks"(2007). *Dissertations*. Paper 833.
[8] Alejandro Proan˜o and Loukas Lazos, "Packet hiding methods for preventing selective jamming attack", IEEE Transactions on dependable and secure computing, vol. 9, no. 1, January/February 2012.
[9] Eugene Y. Vassermann and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318-332 Feb-2013.
[10] Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes: A Defence against Wormhole Attacks in Wireless Networks", Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications, pp. 267- 279.
[11] Anthony D. Wood and John A. Stankovic, "Denial of service in sensor networks", Computer 35 (2002), no. 10.
[12] David R. Raymond and Scott F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defences", IEEE Pervasive Computing 7 (2008), no. 1.
[13] A. Wood and J. Stankovic. Denial of Service in sensor networks. IEEE Computer, pages 54-62, Oct, 2002.
[14] Sharnee Kaul, Helen Samuel, Jose Anand3 Defending Against Vampire Attacks in Wireless Sensor Networks, International Journal of Communication Engineering Applications, Vol 05, Article C084; March 2014
[15] Jyoti Thalor, Ms. Monika, Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013
[16] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
[17] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.
[18] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.