Prevention of Carousal Attack and Stretch Attack in Wireless Sensor Network by using Trust value

Manojkumar L Mahajan[1], DushyantVerma[2], Prashant Lakkadwala[3]

[1]P.G. Student,[2]Assistant Professor,[3]Associate Professor and Head
[1]Department of Computer Science,
[1]Acropolis Technical Campus, Indore,India

***Abstract*—Wireless sensor network is an importantplatform for communication. Wireless ad-hoc sensor network is vulnerable to Denial of Service (DOS) attack. Denial of service attack (DOS) blocks resources and not available to users. This Denial of service attack creates suitable condition for Vampire attack and makes main cause for it. Vampire attack makes the node to consume more battery power and degrades the network performance. Vampire attack does not rely on any particular type of routing protocol. In propose system trust value and energy consumption is calculated for each node to minimize the vampire attack.**

***IndexTerms*—Denial of Service, Wireless Sensor Network, ad-hoc network, routing.**

I. INTRODUCTION

Wireless sensor network (WSN) provides the communication in complex environments. Nodes in Wireless sensor networks are connected to each other and forms the networks. These nodes are useful in various applications such as providing communication services in monitoring environmental condition, military. For this application node must be more reliable and compatible. Node gets the power from its battery to perform its task .If the node uses more battery power for its work then its lifetime is less and that node can disconnected from the networks. This degrades the performance of the network. The wireless sensor network is ad-hoc in nature so it is vulnerable to Denial of service attack [1].

Generally Denial of service (DOS) attack is an attempt to make a machine or network resource unavailable to its intended users. There are various types of DOS attack such as jamming the signal, flooding with useless traffic and power exhaustion. In power exhaustion adversary attacks on the node and consumes more battery power [8]. Vampire attack is one of the types of power exhaustion attack.

In carousel attack adversary sends the packet in loop and in stretch attack adversary sends the packet in longest possible path so that it consumes more battery power of the node [8].

In vampire attack node consumes more battery power for its packet transmission. If the node consumes more battery power then it can be discharge and disconnected from rest of the networks. combination of carousal and stretch attack forms the Vampire attack. These two attacks mainly focus on reducing the energy of the nodes.

A) Carousal Attack

In Carousel attacks, an adversary sends the packets in loop of routing as shown in figure1. In figure 1 packet is sending from source to sink. If we send packet from source to sink then here packet is not follows shortest path. Adversary attacks on the network and forms the loop as shown in figure 1[8]. Packet is send from source to node A which forwards packet to node B→ node C→ node D → node E. Then node E instead of forwarding packet to Sink, it sends packet to node F. Then node F forward packet to node A and forms loops [8]. Then path is repeated for many times and it causes more energy consumed by the nodes. Hence energy consumption performance of the networks degrades [8].

.

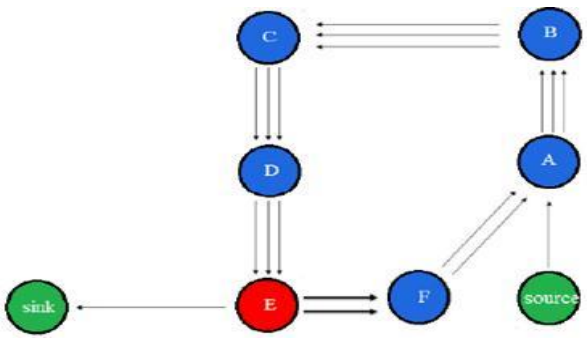

Figure 1: Carousal Attack

B) Stretch Attack

In Stretch attack, an adversary constructs long routes and potentially traversing every node in the network [8]. Packet path length increases by Stretch attack. In figure 2 packets sending from source to sink. The shortest path for forwarding packet is source-node F-node E-Sink but here in Stretch attack, an adversary forward packet in longest path as shown by dark line in figure2[8]. So it increases energy usage by the network. As carousel attack is depending on position of attackers, Stretch attack is more effective and this attack is independent on attacker's position relative to the destination. The impact of these attacks can be further increased 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].

The Literature survey describes in section two. Section three describes Existing system. Proposed system described in Section four. Section five describes the result.

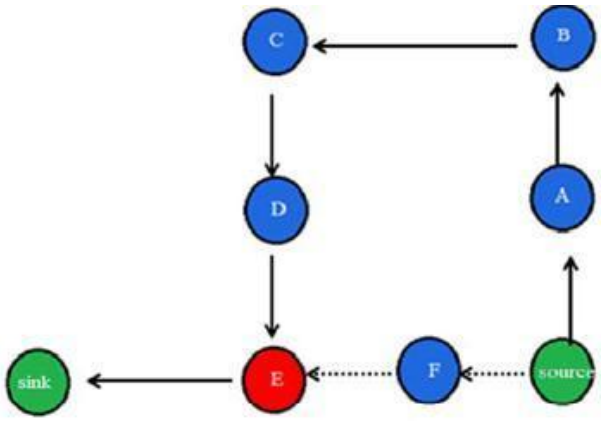

Figure 2: Stretch Attack

II. RELATED WORKS

Power draining attack is not perfectly reduce at routing layer. It founds in Denial of sleep attack. Denial of sleep attack keeps away the node to enter in to low power sleep mode and consumes more battery power. In this adversary is having the knowledge of MAC layer [2]. MAC layer protocol is designed for wireless sensor network and battery power saved by placing radio in low power mode. Raymond and Marchany suggested use of G-MAC protocol to improve its performance [2].In G-MAC protocol requests to broadcast traffic must be authenticated by the gateway node before the traffic can be sent to other nodes. Therefore, unauthenticated broadcast causes power loss of gateway.

In path based DOS attack adversaries attacks on network by flooding the data packet along multi hop end to end communication path [3]. Path based DOS attack is easy to launch and disabling large portion of wireless sensor network. To defend against path based DOS attack an intermediate node must able to detect spurious packet and then reject them. For the detection of spurious packet use lightweight secure mechanism. In this mechanism one way hash chain along a path enabling configures each intermediate node to detect a Path based DOS attack and prevents propagation of spurious packet.

Another attack is wormhole attack which can be possible through path based DOS attack [4]. In wormhole attack adversary record the packet or bit of packet at one location. After recording the packet tunnel it to the other location and then replays them in to the networks from that point. This tunnel distance is longer than normal wireless transmission range of single hop.

Wormhole attack is detected by Packet leash. In packet leash sender node uses two types of packet leash temporal and geographical. In temporal packet leash sender node uses its timestamp means sending time of the packet. In geographical packet leash sender uses its location as well as sending time of the packet to receiver

In DOS adversary can disturb communication. it establishes routes through themselves for drop, monitor and modifies the packet. Some protocols provide security on path discovery and check only valid path found or not. But this cannot protect against vampire attack. Vampire cannot use illegal path for communication.

In SYN Flood attack adversary attacks on the network and uses the resources such as CPU time, bandwidth and that cause the problem in the network. In this adversary makes the multiple connections with the server and allocates the more resources. Such attack can be prevented by using SYN cookies [5]. It form minimal load on the client who initiated with small number of connections and prevent adversary or malicious node to consume more number of connections.

III. EXISTING SYSTEM

In Existing system uses AODV for routing. In AODV source node broadcast the route request (RREQ) message across the network[1]. The neighboring node receives this request message and updates their information for source node to set up backward

pointers for source node in routing table. Route request(RREQ) message contain source node IP address, current sequence number and broadcast ID. The node receiving route request(RREQ) message send route reply(RREP) message to the source node. If source node not getting any response then it rebroadcast the route request(RREQ) message. The node keeps the track of route request's (RREQ) source IP address and broadcast ID. If they receive a route request (RREQ) which they have already processed, they discard the route request (RREQ) message and do not forward it. As the route response (RREP) propagates back to the source nodes set up forward pointers to the destination [1]. Once the source node receives the route response (RREP), it may begin to forward data packets to thedestination. The major drawback of AODV has it do not provide any security mechanism. AODV performs its basic operation only.

IV. PROPOSED SYSTEM

In proposed work vampire attack prevented by finding trust value of each node and using energy weight monitoring algorithm(EWMA). For preventing vampire attack first detect carousal and stretch attack. After detection of carousal and stretch attack reduce their impact by using energy weight monitoring algorithm (EWMA) in wireless sensor networks [8].Then find trust value for performing routing operation of each node in the network.

In this paper we use following steps to prevent vampire attack. In the first step reduce the impact of carousal attack. In second step reduce the impact of stretch attack. Secure routing based on trust value is performed in third step.

Step 1: Reduce impact of carousal attack

The carousal attack forms the loop for forwarding the packet. These repeatedly transmission of same packet through same node depletes more battery power of the node and degrade the network performance. The process of repeating the packet is eliminated by aggregating the data transmitting within forwarding node. In data aggregation copy the content of the packet which is transmitting through the node. This copied content compare with the data packet transmitting through the node. If the transmitted packet is same as the copied packet then stop the packet transmitted through them. In this way it avoids the redundant packet transmitting through the same node and protect from the carousal attack

Steps:

1. Initialize source and destination node in networks
2. Send packets from Source to its neighboring node. Then neighboring node forward packet to its next node up to packet reaches its destination.
3. If loop is detected then it forms carousal attack.
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 finds long route. To find out malicious node in the network every node adds the test field while receiving the packet and forward packet to next node. Then test field is check for each node. if the test field is correct then normal operation is continue and if the test field is wrong then create an alarm packet. Then alarm packet is broadcast and announces that node is malicious so that it avoid for further communication.

In stretch attack use energy weight monitoring algorithm (EWMA)[8].In this algorithm use energy of the node for identified adversary and perform routing operation. Attacked node consumes more energy and reaches threshold energy level. In this phase the node with threshold level energy (attacked node) sends ENG_WEG message to all its surrounding nodes. After receiving the ENG_WEG packets the surrounding nodes sends the ENG_REP message that encapsulates information regarding their geographical position and current energy level. The node upon receiving this stored in its routing table to facilitate further computations.

Steps:

1. Initialize source and destination node in networks
2. For finding adversary add test field while receiving packets.
3. If (Test field of current node= = Test field of next node)

Then Continue Else

Create alarm packet

4. If $Node_{energy}$> =$Threshold_{energy}$

Broadcast alarm packet and announce that node is malicious

5. Then malicious node broadcast ENG_WEG packet to its all neighbour nodes.

6. After receiving ENG_WEG packet neighboring node sends ENG_REP packet that contain geographical position 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 trust value for each node. Node sometimes fails to transmit and start dropping packets during the transmission. Such nodes are responsible for untrustworthy routing. Trust based scheme can be used to track untrust nodes and isolate them from routing. Find out trust value of each node by calculating total packets they transmit, total packets they receive and total packet they drop [7].Attacker node which is having low trust value is eliminated from data transmission. Node with high trust value is selected and that leads to reliable data delivery [7].

Trust value calculation is based on parameters shown in table 1.Count type describe whether transmission is successful or failure.

Table 1:Node trust calculation parameters

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

RREQ and RREP are route request and route reply messages respectively which are exchanged between the nodes. Qrs is query request success rate which is calculated from number of neighbor node who have successfully received RREQ message from source node[7]. Qrf is query request failure rate which is calculated from number of neighbor node who have not received RREQ message from source node[7]. Qps is defined as the query reply success rate which is calculated as successful replies (RREP) received by the source node who broadcast RREQ. Qpf is defined as the query reply failure rate which is calculated based on the number of neighboring nodes which have not sent the replies for the query request. Qds is defined as the data success rate calculated based on successfully transmitted data and Qdf is defined as data failure rate calculated based on data which have 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 that are used to calculate the nodes Request rate, Reply rate and Data transmission rate. The values of Qr, Qp, and Qd are normalized to fall in range of -1 to +1. If the values fall beyond the normalized range then it clearly shows that the failure rate of the node is high and denotes that the corresponding node may not be suitable for routing[7].

Trust value of each node is calculated from Qd which gives data transmission rate. Energy consumption for every node calculated above in step 2.Advesary is having the lower trust value and consumes more energy. So the node with low trust value and more energy consumption is discarded from the netwok.

Steps:

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

V. RESULT AND DISCUSSION

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

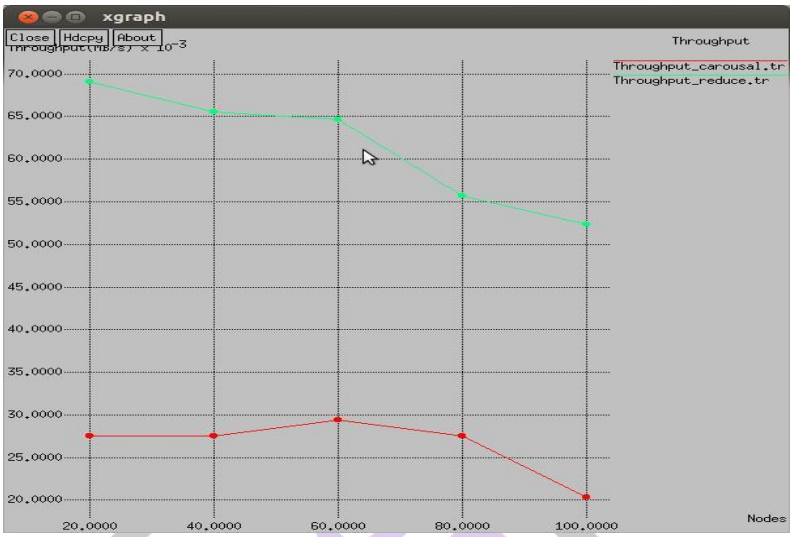

Figure 3: Comparative graph of carousal attack for throughput

.

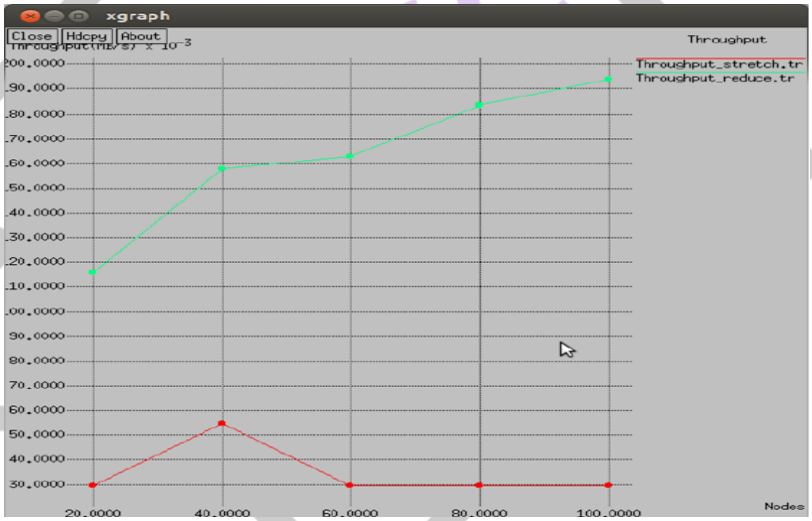

Figure 4: Comparative Graph for the Throughput of Stretch Attack

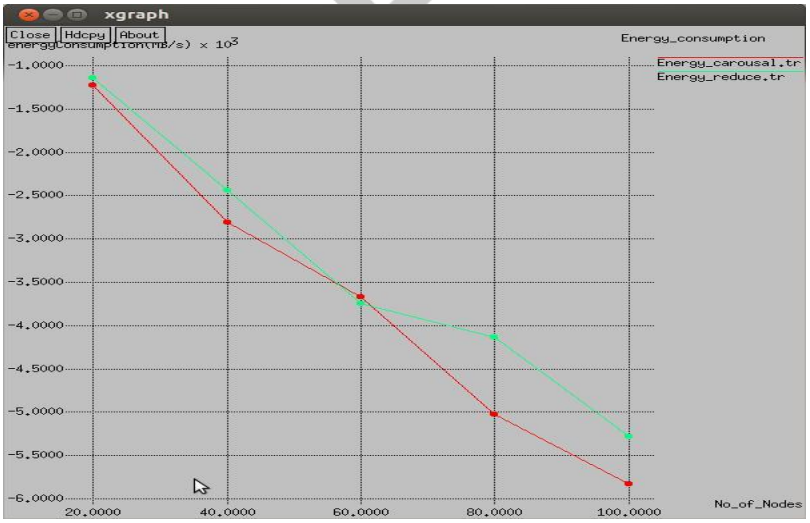

Figure 5: Comparative graph of carousal attack for Energy Consumption

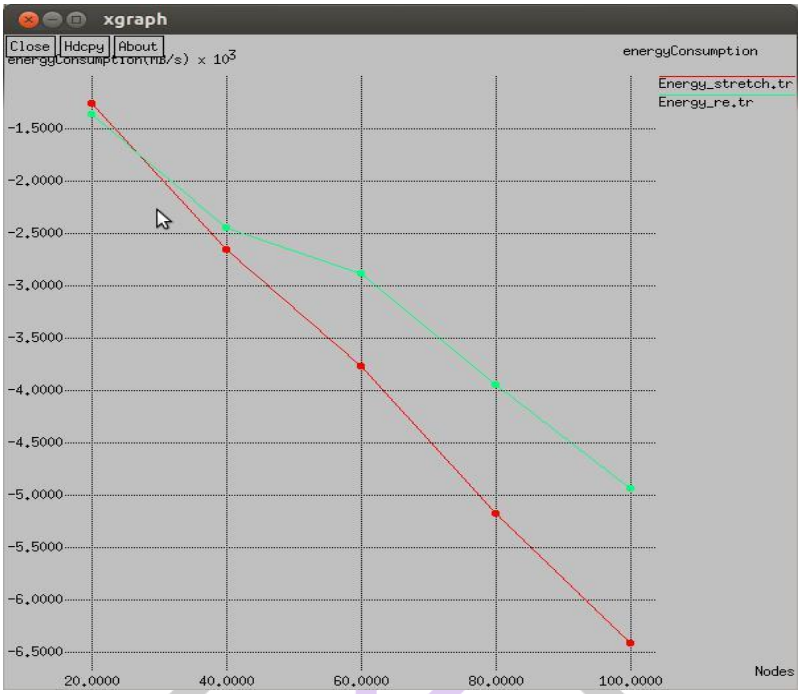

Figure 6: Comparative graph of stretch attack for Energy Consumption

Table 2: Result for carousal attack

No. of nodes	Carousal Attack		
	Throughput	***Delay***	***Energy Consumption***
20	68.8441	46.7895	-1260.612398 J
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 : Result for stretch attack

No. of nodes	Stretch Attack		
	Throughput	***Delay***	***Energy Consumption***
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 a 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 MAC Protocols", IEEE Transactions on Vehicular Technology, Vol. 58, Issue 1, pp. 367-380, January 2009.

[3] Jing Deng, Richard Han, and Shivakant Mishra "Defending against PathbasedDoS Attacks in Wireless Sensor Networks" ACM workshop on security of ad hoc and sensor networks, 2005.

[4] Yih-Chun Hu, Adrian Perrig and David B. Johnson "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks", INFOCOM, 2003.

[5] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.

[6] David R. Raymond and Scott F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses", IEEE PervasiveComputing 7 (2008), no. 1.

[7] Sridhar Subramanian and Baskaran Ramachandran "Qos Assertion in MANET Routing based on trusted AODV (ST-AODV)", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012.

[8] Manojkumar Mahajan, DushyantVerma, "Review of Prevention techniques for Denial of Service Attacks in Wireless Sensor Network", International Journal of Engineering Research and Technology (IJERT), Volume. 4, Issue. 05 , May – 2015.