ISSN 2395-1621

Implementation of Carousel attack and Stretch attack on WSN

[#1]Atul Sontakke, [#2]Rahul Jaybhaye, [#3]Sanket Chavan, [#4]Vivek Bagade

[1]atsontakke@gmail.com,
[2]rahuljaybhayerj7@gmail.com.
[3]csanket48@gmail.com,
[4]vivekbagade7@gmail.com

[#1234]Deparment of Computer Engineering
JSPM's, ICOER, Wagholi, Pune.

ABSTRACT

Wireless ad-hoc sensor network is prominent platform for communication and research. A sensor node collects information about the physical environment. Now-a-days one main issue in wireless sensor network is wastage of energy at each sensor nodes. Carousel attack and stretch attack, which occurring at network layer. A vampire attack is caused by the malicious node on the decentralized ad hoc wireless network. They leads to resource depletion (energy) at each sensor nodes, by reducing the battery power of any node. We propose method to mitigate this type of attack. . In Carousel attack and stretch attack it 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 energy consumption and trust value is calculated for each node to mitigate the vampire attack. It works on the threshold energy of node. Thus, the problem of vampire attack can be reduced to some extent.

ARTICLE INFO

Article History

Received: 6th June 2017

Received in revised form :

6th June 2017

Accepted: 9th June 2017

Published online :

9th June 2017

I. INTRODUCTION

Wireless sensor network (WSN) is promise of providing the communication in complex environments. Nodes in Wireless sensor networks are connected to each other and forms the networks. These nodes are use in various application such as to monitor environmental condition, providing communication services in military.
Wireless sensor network is the one of the type of wireless ad hoc network. A wireless sensor network (WSN) is made of sensors which are used to monitor environmental conditions, such as temperature, sound, vibration, pressure, motion at different locations. Wireless sensor networks are made of many small sensor nodes. Each node can send messages to sink through the network or controlling device. The nodes can forward messages to other nodes to perform network organization tasks and other functions. A wireless sensor network contains number of sensors that are distributed across a wide geographical area. Several applications uses a constitute network which is formed by autonomous sensor

Attacks in WSN are as follows:

1) Tampering: it is the result of physical access to the node by an attacker; the purpose will be to recover cryptographic material like the keys used for ciphering [3].

2) Black hole: a node falsifies routing information to force the passage of the data by itself, later on; its only mission is then, nothing to transfer, creating a sink or black hole in the network

3) Jamming Attack: - It is a type of DOS attack. There are many different attack strategies that a jammer. can perform in order to interfere with other wireless communications. Some possible strategies are exposed below:

[a] Constant Jammer: A constant jammer continuously emits a radio signal that represents random bits; the signal generator does not follow any MAC protocol.

[b] Deceptive Jammer: Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless.

[c] Random Jammer: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second

mode (the sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

[d] Reactive Jammer: A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only minimum amount of power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded.

The wireless sensor network (WSN) 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, power exhaustion and flooding with useless traffic. In power exhaustion adversary is attacks on 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 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 is 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. Vampire attack forms by the combination of carousal and stretch 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 routing loop as shown in figure1. In figure 1 packet is sending from source to sink. If we send packet from source to sink then shortest path is from source - node f- node E - Sink. But here packet is not follows shortest path. dversary attacks on the network and forms the loop as shown figure 1[8]. Packet is send from source to node A. node A forward packet to node B. then node B sends packet to node c. node c forward packet to node D. then node D send packet to node E. Then node E instead of orwarding packet to Sink, it is Sends packet to node F. Then node F forward packet to node

A and forms loops [8]. Then same path is repeated for many times and it causes more energy consumed by the nodes. so, because of these energy depletion performance of the networks degrades[8].

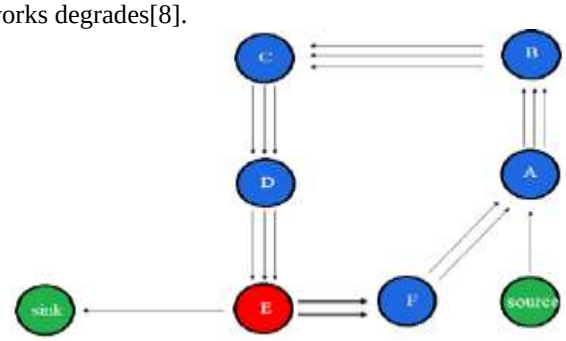

Figure 1: Carousal Attack

B) Stretch Attack:

In Stretch attack, an adversary constructs artificially long routes and potentially traversing every node in the network[8].In these attack it increases packet path length.In figure 2 packet 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 attackers 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]. Section two describes the literature survey. Existing system describes in section three. Section four describes proposed system .Discuss the result in section five.

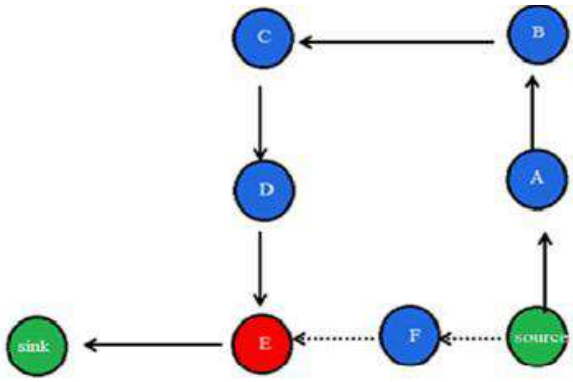

Figure 2: Stretch Attack

II. 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 the destination. The major drawback of AODV has it do not provide any security mechanism. AODV performs its basic operation only.

III. SYSTEM OVERVIEW

In this project we, considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture.

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

In this paper we use three steps to prevent vampire attack. In the first step reduce the impact of carousal attack. Reduce the impact of stretch attack in second step. In third step perform secure routing based on trust value.

Step 1: Reduce impact of carousal attack

As we see in the carousal attack in figure1 it form 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. Source node sends packet to its neighboring node.Then neighboring node forward packet to its next node till packet reaches its destination.
3. If loop is detected then it is identified as 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 is finding artificially long route. For find out malicious node in the network every node is add 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 added 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 Nodeenergy > =Thresholdenergy
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 neighbour 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 dro[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].

System Flow:

Step 1. Start
Step 2. User can login with userID and Password, if new user then firset need to register.
Step 3. Select packet to be sent.
Step 4. Select Source node and Destination node.
Step 5. Packet Sent.
Step 6. Detect the attack in network
Step 7. Securely transfer the packet.
Step 8. Verify the packet delivered to destination.
Step 9. Check status of very node.
Step 10. Stop.

IV. SOFTWARE REQUIREMENT SPECIFICATION

We have created system in java programing. Data is stored in mysql database. We have created a application which transfer packet securely over network. Application detect the attack such as carsouel attack and stretch attack. We have multiple user to login system. User login using his userID and password.

V. MATHEMATICAL MODEL

System Description:

S= {I, O, N, P, Path, Loop, S, D}.

where,

S = input, output
Input = Packet Sending ()
N : Node.
P : Packets.
Path : Sending Path.
Loop : Loop for sending packet.
S : Source
D : Destination
P = {f1, f2, f3, f4, f5}. where,

f1= Select Packet.
f2= Send packet in network.
f3= Detect Attack in network.
f4= Prevent attack.
f5= Successful Delivery of Packet

S1= Initial state is the state in which system
Detect the attack in network.
S2= Final state is the successful prevention of attack and delivery of packet secirly.

VI. SYSTEM ANALYSIS

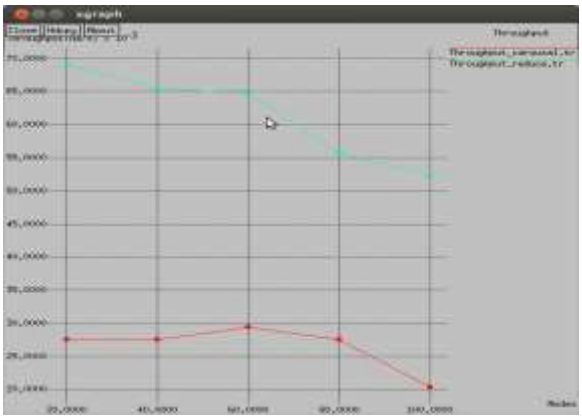

Fig 1. Comparative graph of carousal attack for throughput

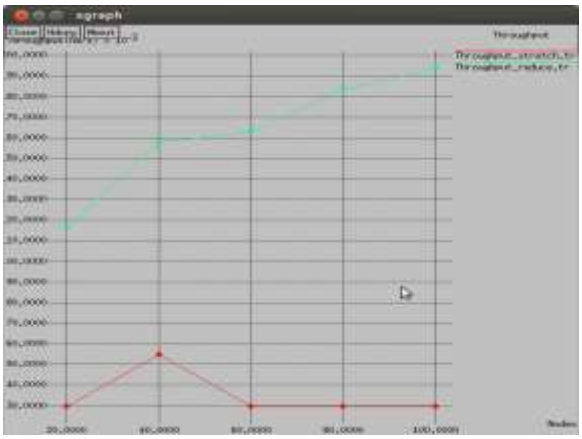

Fig 2. Comparative graph of stretch attack for throughput

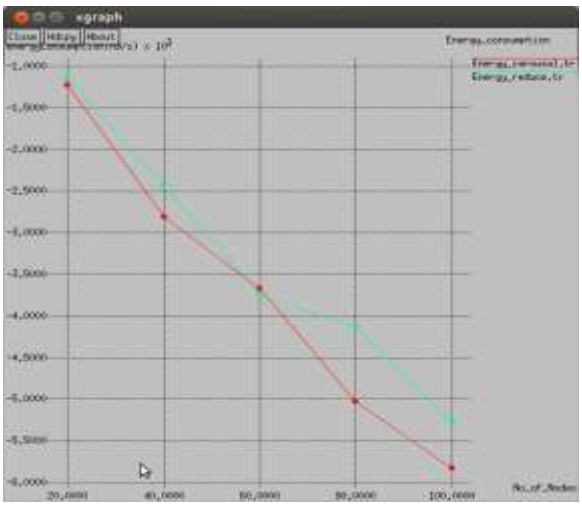

Fig 3.Comparative graph of carousal attack for Energy Consumption

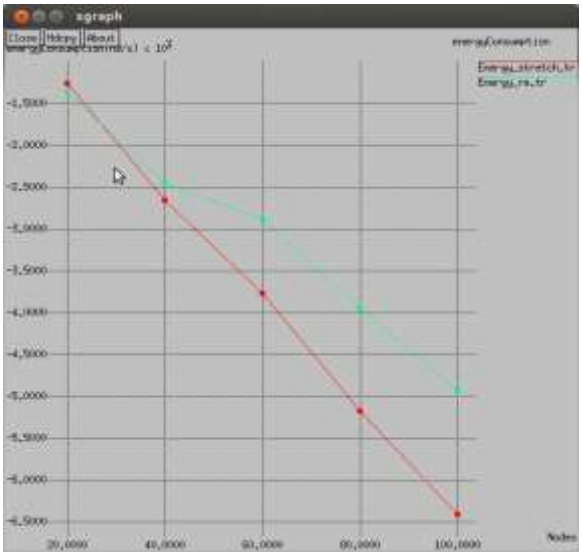

Fig 4. Comparative graph of stretch attack for Energy Consumption

VII. CONCLUSION

In this paper we define vampire attack as an resource deplation attack in which it consumes more battery of the node. 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.

VIII. ACKNOWLEDGMENT

We wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally we wish to thank to all our friends and well-wishers who supported us in completing this paper successfully we especially grateful to our guide for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 60, NO. 10, OCTOBER,2015.

[2] Zhuo Lu,Student Member, IEEE,Wenye Wang,Senior Member, IEEE, and Cliff Wang,Senior Member, IEEE "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 8, AUGUST 2014.

[3] Nani Yalu, RajatSubhra Goswami, Subhasish Banerjee, "An Efficient Packet Hiding Method for Preventing Jamming Attacks in Wireless Networks" IEEE WiSPNET 2016.

[4] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in Proc. 1st Int. Conf. High Confidence Networked Syst., 2012, pp. 47–54.

[5] Saurabh Amin, Alvaro A. C´ardenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks" R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 31–45, 2009. c Springer-Verlag Berlin Heidelberg 2009.

