International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

# Defending Against Resource Depletion Attacks in Wireless Sensor Networks

**Cauvery Raju**

M. Tech, CSE IInd Year, JNNCE, Shimoga

**Abstract:** ***One of the major challenges wireless sensor networks face today is security. Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Energy is the most essential resource for sensor nodes. Resource depletion attacks means draining the energy of the nodes by introducing routing loops and stretching the path during packet transmission. Routing protocols are vulnerable to resource depletion attacks. This attack is grouped under "vampire attacks". Vampire attacks include carousel and stretch attack. Vampire attacks not only affect a single node but they bring down the entire system by depleting the energy. Secure packet traversal algorithm is developed to avoid vampire attacks. The proposed algorithm increases the network lifetime.***

**Keywords:** Denial of Service, Routing, Security, Vampire Attacks, Wireless Sensor Networks

## 1. Introduction

WSN is characterized with low power, low computational capabilities and limited memory nodes. Developing energy-efficient routing protocol on wireless sensor networks is one of the important challenges. Therefore, a key area of WSN research is to develop a routing protocol that consumes low energy. Unfortunately, current routing protocols suffer from many security vulnerabilities. Already many solutions have been proposed to defend attack that lives for short duration on the network. Wireless sensor networks suffer from four different kinds of attacks. Denial of Service (DoS) attacks, Reduction of Quality (RoQ) attacks, Routing infrastructure attacks and Resource Depletion attacks. Of these, the resource depletion attack affects long-term availability of the network by entirely depleting node's battery power. But these solutions do not defend permanent resource depletion attack. Resource depletion attacks [1] on networks have become very common in the present scenario. All the real time networks need to be consistent even under such attacks. The permanent resource depletion attack is the depletion of the node's battery thereby rendering it useless for any communication.

During attacks by malicious nodes, the node's energy expenditure increases drastically thereby leading to its energy depletion making the node incapable of transmission in future. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. The battery power consumption attacks at routing layer protocol to completely disable networks, by depleting node's battery power and it is defined as vampire attacks. These attacks never flood the network with large amount of data instead it drains node's life by delaying the packets. Vampire attack [2] means creating and sending messages by malicious node which causes more energy utilization by the network leading to slow reduction of node's battery life. This attack is not particular to any protocol.

The remainder of this paper is organized as six sections. The first section gives an idea about resource depletion attack and how it will drain the battery power of nodes. The second section will discuss the literature survey which familiarizes the earlier security measures on wireless sensor network. The third section gives an idea about problem statement, solution strategy and fourth section will discuss system architecture. The Fifth section will discuss the module description. The result and simulation result is discussed in next section and lastly we conclude our paper.

## 2. Literature Survey

There are several challenges pose by the resource limitations in the wireless sensor networks due to the vulnerabilities that may occur due to dynamic behavior of networks. . Due to some of hardware constraints the algorithm must be framed with the parameters like bandwidth, computational complexity and memory. Since the cost occurred is very high when we equate communication in terms of power, it may not be a trivial task. So energy efficient wireless sensor networks must be given at most priority. The problem of security has received considerable attention by researchers in ad hoc networks. Vulnerabilities in WSN could occur based on certain dimensions in accordance with the characteristics of dynamic topology and lack of central base station. There are many different kinds of attacks that occur in wireless sensor networks. There are preventive measures for these attacks in the MAC layer. The table 2.1 below depicts the attacks and its features and defense developed for the attack has some disadvantages.

**Table 2.1:** Literature Survey

| *Attacks* | *Features* | *Disadvantages Of Defences* | *References* |
|---|---|---|---|
| Sleep deprivation torture | Prevents nodes from entering sleep cycle and depletes batteries fast | It considers attacks only at the medium access control(MAC) | 3 |
| Resource Exhaustion | Mentions resource exhaustion at MAC and transport layers | Only offers rate limiting and elimination of insider adversaries | 4 |
| Flood Attack | Multiple request connections to server, run out of resources | Punishes nodes that produce bursty traffic but may not send much data | 5 |
| Reduction of quality attacks | Produce long term degradation in networks | Focus is only on transport layer and not on routing protocols | 6 |
| DoS attacks | Malefactor overwhelms honest nodes with large amount of data | Applicable only to traditional DoS, does not work with intelligent adversaries i.e protocol compliant | 7 |
| Wormhole attack and Directional antenna attack | Allows connection between two non neighboring malicious nodes disrupt route discovery | Packet Leashes: Solution comes at high cost and is not always applicable | 8 |

## 3. Problem Statement

In carousel attack, the attacker composes packets with purposely introduced routing loops. It allows single packets to repeatedly traverse the same set of nodes. This process continues for the particular period of time, transmitting the process in the loop and wasting every nodes power which is presently in the routing path. In stretch attack, an adversary constructs long routes, potentially traversing every node in the network. Routing loop happens because nodes are not aware of whether they are processing the same packet that it processed previously. Stretching of routes happens because nodes are not aware of whether they are forwarding the packet towards destination or making a path that takes packet away from destination.

### 3.1 Solution Strategy

The packet forwarding algorithm goes secure forwarding of packet to destination posture of the node. It captures the transfer message packet from nodes which want to send the data and it retrieves the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list. If this next hop is present in the neighbor list it simply transfers the packet to next hop otherwise it deletes the packet from its network.

### 3.2 Objectives

Secure packet traversal algorithm reduces the energy usage of the network by avoiding vampire attacks and increases the network lifetime.

## 4. System Design

The major components of the system architecture are network formation, attacks on protocol, security against vampire attacks. The system architecture is shown below in Fig 1.

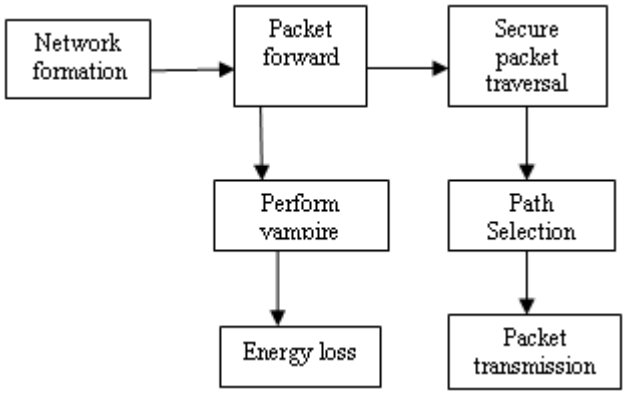


**Figure 1:** System Architecture

### 4.1 Network Formation

A network describes a collection of nodes and the links between them. Source node would wish to send the packet to destination through intermediate nodes. Packet contains the control information and user data. Network creation is the process to create the N number of nodes within the network. Each and every node has its own address and initial energy value by its creation time. The nodes are wished to transfer the data from one node to another. Select the source and destination node and also maintain the neighbor list.

### 4.2 Vampire attack

In carousel attack, the adversary composes packets with purposely introduced routing loops. This is one of the major problems of the network where the consuming energy of each node in the network will increase. Since it sends packets in circle. It allows single packets to repeatedly traverse the same set of nodes. This process continues for the particular period of time, transmitting the process in the loop and wasting every nodes power which is presently in the routing path. In stretch attack, an adversary constructs artificially long routes, potentially traversing every node in the network. Every networks node is involved in the transmission.

### 4.3 Secure Packet Traversal

The secure packet forwarding algorithm goes secure forwarding of packet to destination posture of the node. It

captures the transfer message packet from nodes which want to send the data and it retrieves the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list. If this next hop is present in the neighbor list it simply transfers the packet to next hop otherwise it deletes the packet from its network.

### 4.4 Data Flow Diagram for Carousel Attack

As shown in Fig 2, an adversary diverts the packet away from honest route and forms malicious loop path construction. This allows a single packet to traverse the same set of hops repeatedly over a period and finally reaches the destination

### 4.5 Data Flow Diagram for Stretch Attack

As shown if Fig 3, DFD for Stretch Attack, here adversary diverts the packet away from honest path to malicious path by traversing every network node in the network.

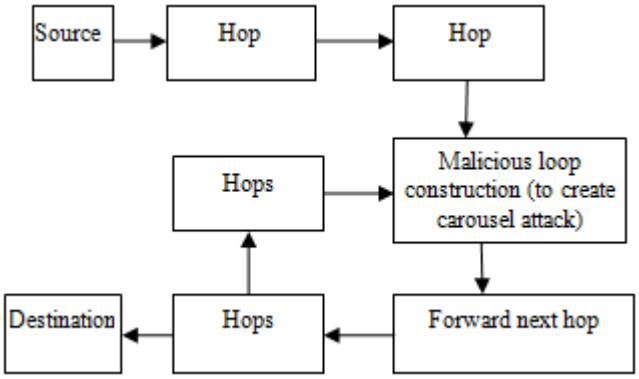


**Figure 2:** DFD for Carousel Attack

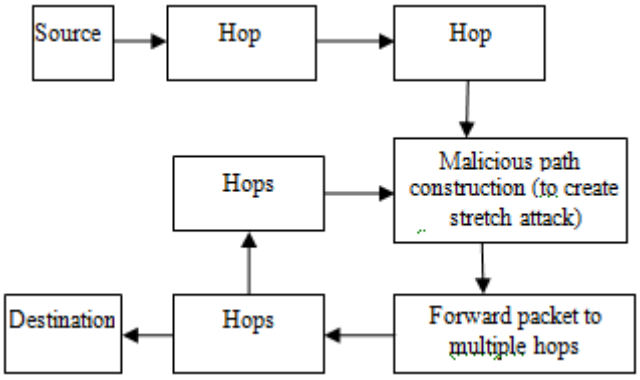


**Figure 3:** DFD for Stretch Attack

## 5. Module Description

The modules involved for the implementation of vampire attacks are as follows.
5.1 Topology Creation
5.2 Carousel Attack
5.3 Stretch Attack
5.4 Secure packet traversal

### 5.1 Topology Creation

Before implementing the actual algorithm simulator must be configured according to the wireless sensor network topology and node must be configured as sensor nodes. Since the implementation is done in NS2 simulator, simulator must be configured by setting various parameters such as type of channel, queue, antenna, initial energy, protocol used for the simulation etc.

Node configuration essentially consists of defining the different node characteristics before creating them. They may consist of the type of addressing structure used in the simulation, defining the network components for mobile nodes, turning on or off the trace options at Agent/Router/MAC levels, selecting the type of adhoc routing protocol for wireless nodes or defining their energy model.

### 5.2 Carousel Attack

An attacker sends a packet with a path which consists of a sequence of loops, such that the same node appears in the route more than one time. This strategy can be used to increase the length of the route beyond the number of nodes in the network which is only restricted by the number of allowed entries in the source route.In this malicious node introduces loop in the path of packet travel purposely to drain the energy of honest nodes.

### 5.3 Stretch Attack

In stretch attack, an attacker constructs falsely long routes potentially traversing every node in the network, thereby draining the energy of nodes. It causes packets to traverse longer route than optimal number of nodes. It causes a node that does not lie on optimal path to process packet, but the malicious node selects a longer route, affecting all nodes in the network. In contrast to carousel attack, this attack shows more uniform energy consumption for all the nodes in the existing network, as it increases the length of the route, by causing more number of nodes to process the packet in the network.

### 5.4 Secure packet Traversal

1) n←Number of nodes
2) sa←Source Address
3) da←Destination Address
4) For each node in n do
5) Find neighbousrList
6) Store NL
7) End For
8) For i=1 to NL
9) Send test packet(sa,da)
10) If verified da= NL(i) then
11) Maintain in separate route
12) Set desired spath (route)
13) Forward test packet
14) End If
15) End For

The packet-forwarding algorithm goes secure forwarding of packet to destination posture of the node. It captures the transfer message packet from nodes that want to send the data and it retrieves the packet source and destination address. After gathering the both address it take this next hop address from that packet then it check this next hop address to its network neighbor list. If this next hop is present in the neighbor list it simply transfers the packet to next hop, otherwise it deletes the packet from its network.

We have evaluated both carousel and stretch attack and the performance of secure packet traversal algorithm. We launch the simulation on NS2. We consider constant bit rate (CBR) data traffic; packet size is 1024bytes and chooses different source-destination connections. Simulation can be conducted up to 500 nodes. Fig 4 shows the simulation for a randomly generated topology of 100 nodes. Node number 84 and node number 65 are Source and Destination respectively where those nodes are indicated by red and black color. Using packet traversal algorithm, the traversed path is 84→81→65.

## 6. Simulation Results

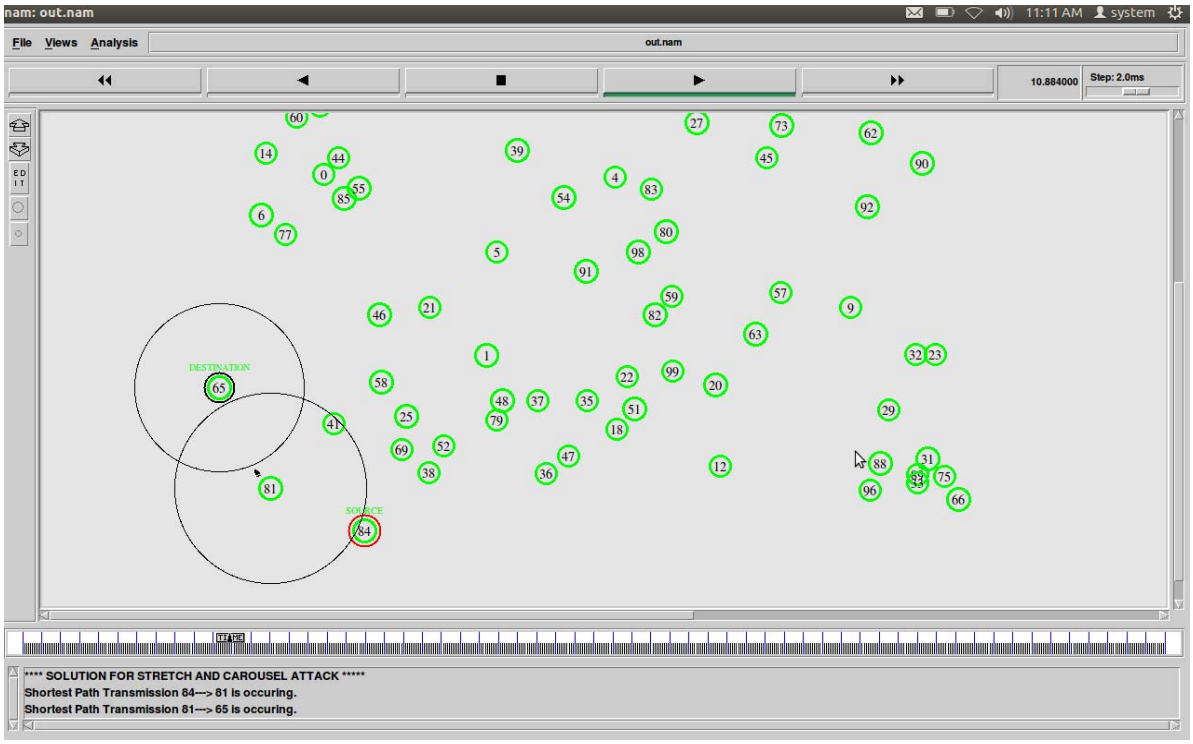


**Figure 4:** Shortest path transmission using secure packet traversal

### 6.1 Analysis

Simulation was conducted for 100 nodes for 50ms.The initial energy of all the nodes is assumed to be 30J. The data transmission begins at 0.1ms and ends at 50ms. Energy is taken along y-axis and time along x-axis. Energy gradually decreases with the transmission of data and in the presence of routing loops. The energy usage in carousel attack is shown below in Fig 5. The energy consumed is 22.41J

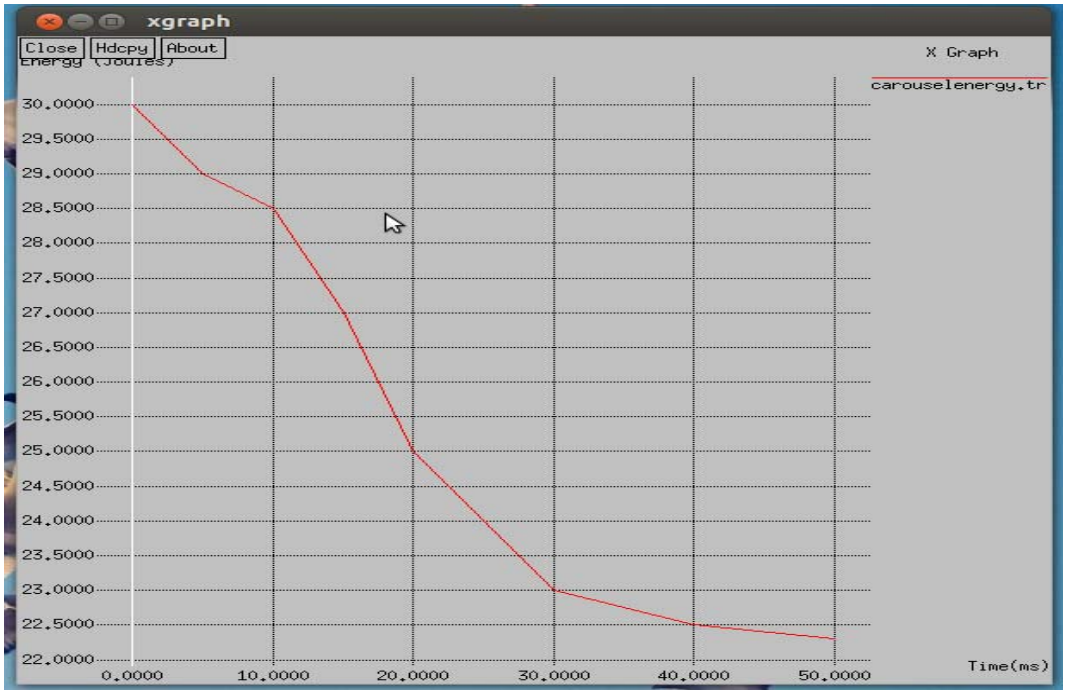


**Figure 5:** Energy Consumption in Carousel attack

Fig. 6 shows the energy consumption during a Stretch attack. Energy gradually decreases with the transmission of data and in the presence of increased number of nodes. All network nodes are involved in the transmission.The energy consumed is 24.81J

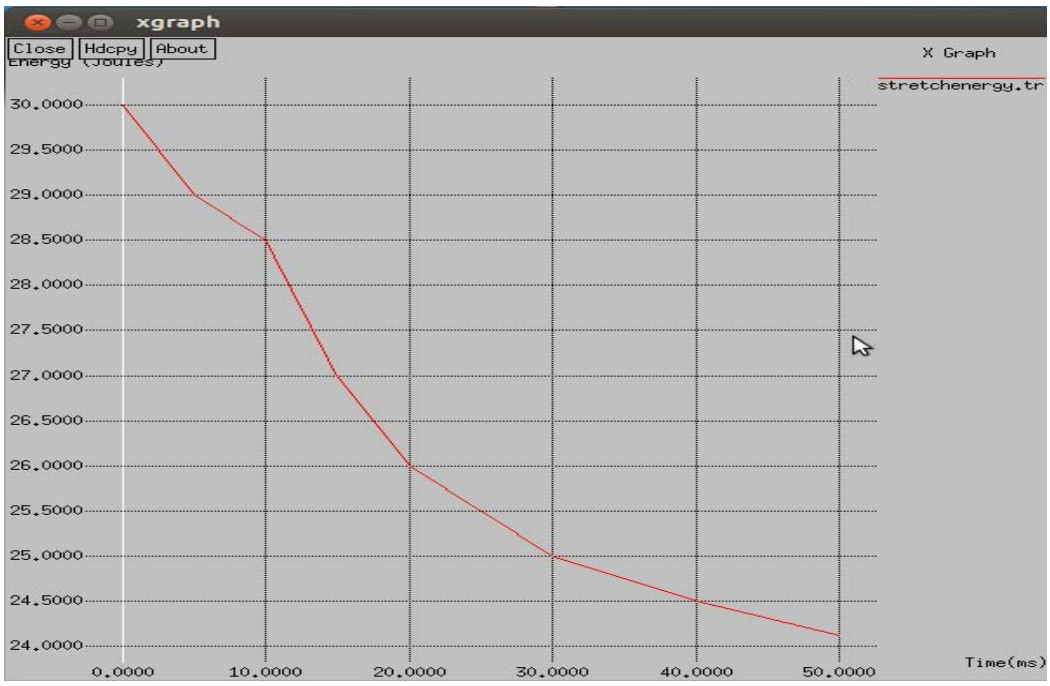


**Figure 6:** Energy Consumption in Stretch attack

Fig 7 shows the mitigation of carousel and stretch attack energy using Secure packet traversal where the x-axis is taken as Time(ms) and the y-axis is taken as the Energy(J). From the analysis of the graph mentioned below the energy consumption is less and stable. The energy consumed is 27J. Using secure packet traversal we can can increase the lifetime of the nodes. This concept increases the overall lifespan of the network by choosing the shortest path.

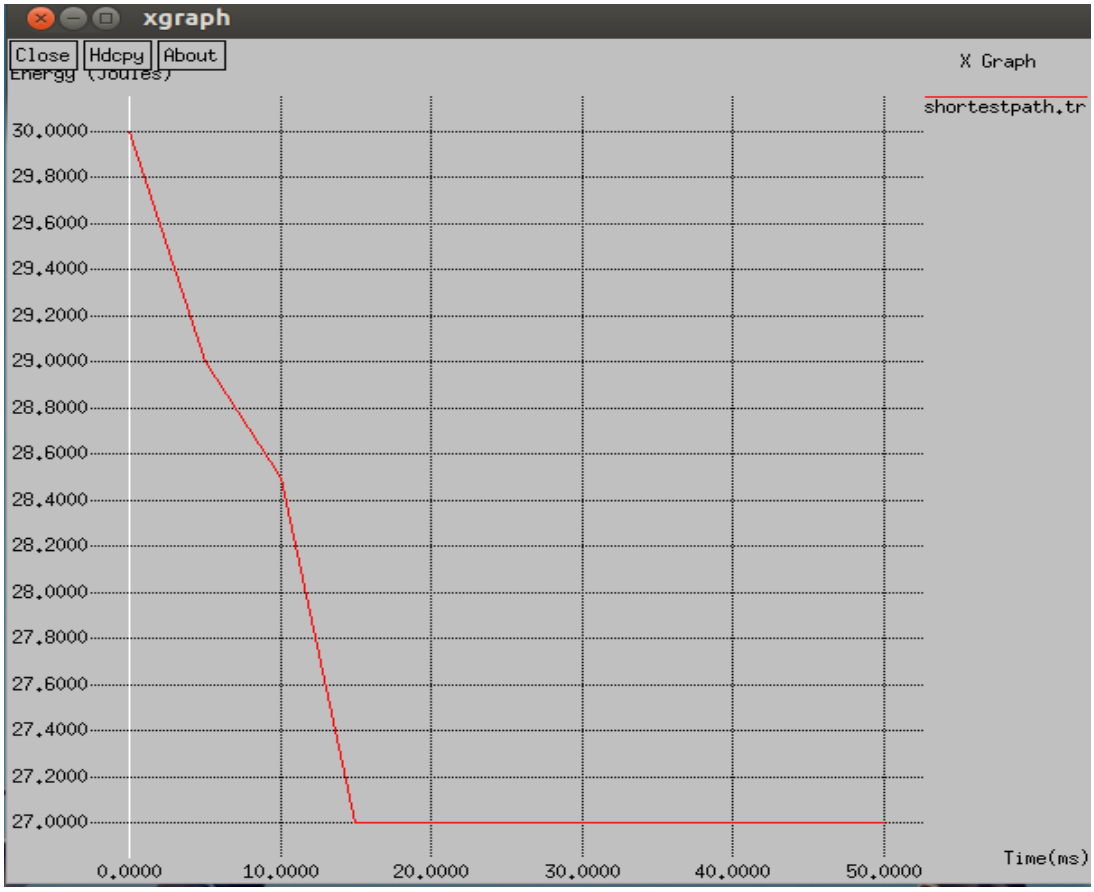


**Figure 7:** Mitigation of Vampire attacks and Energy Consumption in Secure packet traversal

## 7. Conclusion

Vampire attacks, a new class of resource consumption attacks that drain the battery power by using more energy of the nodes during data transmission. These attacks do not depend on any specific type of protocol or condition. According to the simulation results, the energy usage in carousel attack is 22.41J and energy consumption in stretch attack is 24.81J. Using the secure packet Traversal method, secured transmission is established in the packet forwarding process from source to destination which consumes relatively less energy i.e. 27J. The simulations results show that the impact of attacks on the system was reduced to a great extend after implying the algorithm. A full solution is not given yet but some amount of damage was avoided.

## 8. Acknowledgment

I would like to thank my guide Dr. Poornima K M for her continuous support and helpful comments on the project. Finally, I thank almighty, my Parents, Friends and Family members for the constant support and encouragement without them it was impossible for me to complete my work.

## 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] C.Balasubramanian, R. Sangeetha, R.Deepa,, “Provably Secure Routing and Defending Against Vampire Attacks in Wireless Ad Hoc Sensor Networks”,ICIET,2014
[3] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” IEEE Trans. Vehicular Technology, vol. 58, no. 1,pp. 367-380, Jan. 2009
[4] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002
[5] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.
[6] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, “Path-quality monitoring in the presence of adversaries”, SIGMETRICS,2008.
[7] Jing Deng, Richard Han, and Shivakant Mishra, “Defending against path-based DoS attacks in wireless sensor networks”, ACM workshop on security of ad hoc and sensor networks, 2005.
[8] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless ad hoc networks”, INFOCOM, 2003.