ENHANCED SECURE FRAMEWORK FOR HETEROGENEOUS WIRELESS SENSOR NETWORK

Ms. Varsha Buktare[1] and Dr. Savita R. Bhosale[2]

[1]PG Scholar, Department of Computer Engineering,
MGMCET,Kamothe, Navi Mumbai (India)
[2] Professor, Department of Electronics & Telecommunication,
MGMCET, Kamothe, Navi Mumbai (India)

ABSTRACT

WSN is a communication network of sensor nodes and node gathers information about physical information. Asthe ad-hoc nature of WSN prone to different types of attacks such as Dos. Denial of service (Dos)is an attempt to make a machine /network resource unavailable to its intended users. Dos attack generally consist of efforts to temporarily suspend services of host connected to internet. Many protocols developed to protect against Dos, but it is not completely possible. One of such Dos attack is a vampire attack. Vampire attack is a resource exhaustion attack at the routing protocol layer which disables network by consuming more battery power. Vampire attack can be carried out in two different forms such as stateless protocol and stateful protocol. This attack does not belongs to any specific protocol but depend on properties of many classes of routing protocol such as link state, distance vector and so on. This attack is very hard to identify because it uses protocol compliant messages. In this project we concentrate on detection, prevention and bound the damage from vampire attack in the form of stateless protocol. EWMA is a mitigation method to bound the damage from vampire attacks.

Keywords: Denial of Service, Energy Consumption, Routing, Security, Wireless Sensor Network.

I. INTRODUCTION

WSN is a group of large number wireless sensor nodes / is a communication network spread in a space where all nodes are connected by links which communicate over the wireless channeland also node performs many tasks as information gathering, data processing, signal processing. Sensor produces a measurable response to change in a physical condition as temperature or magnetic field. WSN acts as self-configured/self-organised, energy constrained and is a very efficient in many applications for security purposes such as military applications, to monitor the environmental changes and so on.

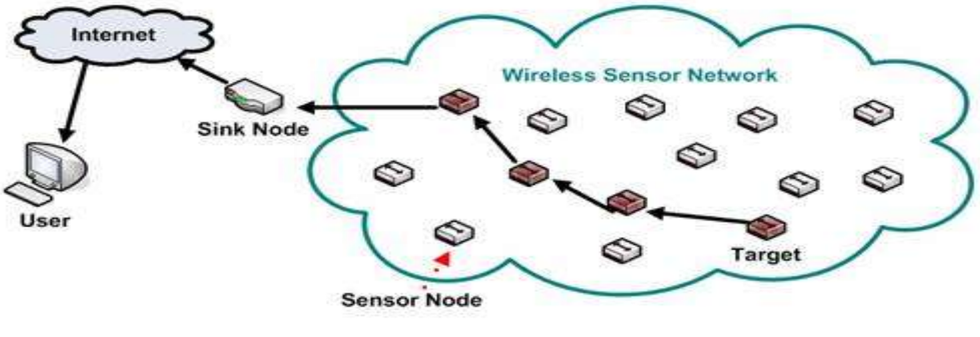


Figure: 1 Wireless Sensor Networks.

Today it is very important to have a secured communication and real time delivery of operation going on network. Ad-hoc wireless sensor network provides continuous connectivity, efficiently-deployable communication for military applications. WSNbroadcasts communication messages to the nodes but it gets affected by different attacks. One of the most popular attack is a Dos (Denial of service) which leads to resource exhaustion. We focus on a vampire attack which is one kind of Dos attack. In this paper we focus on how lacking protection security protocols causes vampire attack in WSN.

II. VAMPIRE ATTACK

Vampire attack is a composition and transmission of a message leads to consumption of a more energy by the network than identical size message transmission without attack. Vampire attack carried out in stateless and stateful protocols.*Stateless protocol*treat request as independent transfer which are not related to any previous request. Source node which initiates message transfer carries full path route/ address to be followed to reach to the destination.It simplify the server design as if dynamically allocates the storage while transaction in progress.it is responsible for cleaning the server if the client dies in the middle. Stateful protocols are able to remember and store details of interaction between nodes and make decision for flow of data when in stored state. It uses two different protocols such as link state protocol called OLSR and distance vector protocol called DSDV.

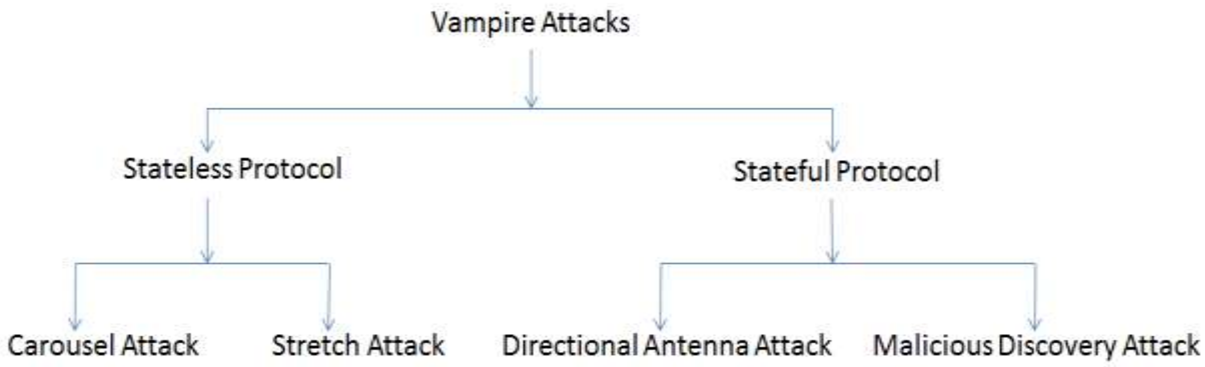


Figure:2 Types of Vampire Attacks

III. OVERVIEW

In this paper we are considering the effect of vampire attack on source routing protocol and also implementation, detection, recovery from *carousel* and *stretch attack*. Energy is consumed from nodes only for packet transmission and not for reception or processing.

*Carousel attack:*Stateless protocols lead to this kind of attacks. An attacker composes a packet within that routing loops are introduced purposely in a way that same nodes can appears many times in a route, because of that route length and delay also increases. As we know energy is exhaustedfrom node for packet transmission and here loop gets introduced in a route means same node transmits same packet multiple times and results in a more energy consumption. As the figure 3.1 shows Carousel attack in which normal path is source → A→B→C→D→E→sink. Attack introduces loops in a route and then route becomes source→

A→B→C→D→E→F→ A→B→C→D→E→F→ A→B→C→D→E→sink. Energy required by the node A, B, C, D, E is two times more than normal energy.

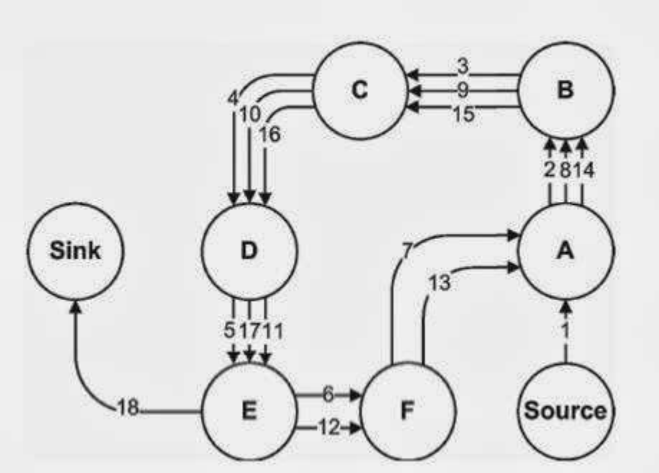


Figure: 3.1Carousel Attack

Stretch attack: Stateless protocol leads to this attack. This attack causes longer distance travel to the packet than needed to reach the destination causes unnecessary energy wastage. Figure 3.2 shows normal route and also route caused by attack. Dotted lines shows normal route path (source→F→E→sink) and other line shows infected route path (source→A→B→C→D→E→sink).

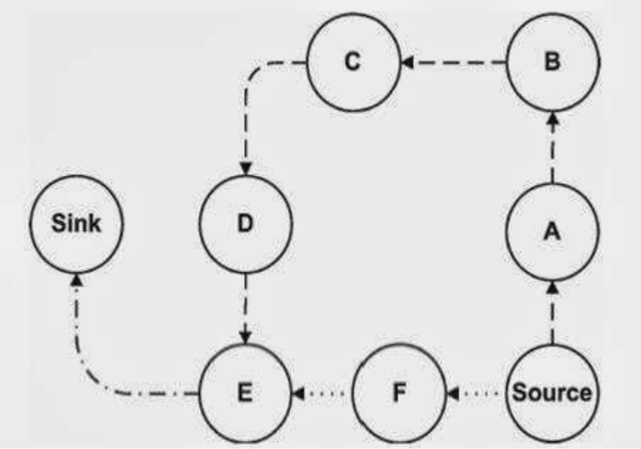


Figure: 3.2 Stretch Attack

Directional antenna attack: Stateful protocols leads to this attack, vampires have some kind of control over packet and each node make forwarding decisions independently. Node waste there energy by restarting packet in a various parts of network.

Malicious discovery attack: Error is generated by the attack that is the link does not exist and new non-existence link has been created. Stateful protocol leads to this attack.5

IV. EXSISTING SYSTEM

No-Backtracking property implies vampire resistance and PLGPa satisfies No-Backtracking. No backtracking property is satisfied if every packet p traverses the same number of hops weather or not an adversary/ attacker is present in the network [1]. This means the adversary cannot perform carousel or stretch attacks, no node may unilaterally specify a suboptimal path through the network [2].

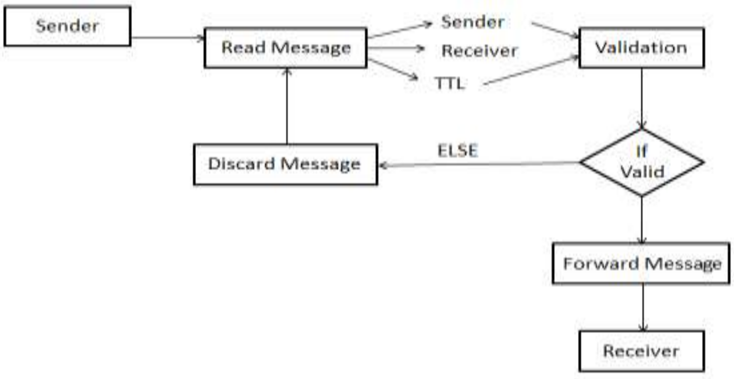


Figure:4 Flow Chart for PLGP-a

V. PROPOSED METHOD

EWMA is an our proposed protocol/ algorithm where node energy get to threshold level and is very important while performing energy intensive task. It is based on sensors energy levels. EWMA works in two phases *Network configuring phase* and *Communication phase*.

Network configuring phase: The main purpose of this phase is to establish a optimal routing path from source to destination. Node balancing of nodes and minimization of energy consumption for data communication are the key factors. Node with threshold level energy sends ENG_WEG massage to all its neighbouring nodes. After receiving the ENG_WEG packets neighbouring node sends ENG_REP massage is consist of current energy of geographical position node finds the next node by calculating energy required to send particular data packet & establishes routing path by selecting nest node of minimum distance. It avoids data packet dropping & next node transmits packet safely to the destination. In this phase we achieve load balancing & assign suitable energy to forwarding nodes. Finally achieve multi hope load balanced network.

Communication phase: It avoids same packet transmitting to same node repeatedly. By using data aggregation technique it eliminates the process of repeating packets, is achieved by coping content of packet while transmitting through nodes.

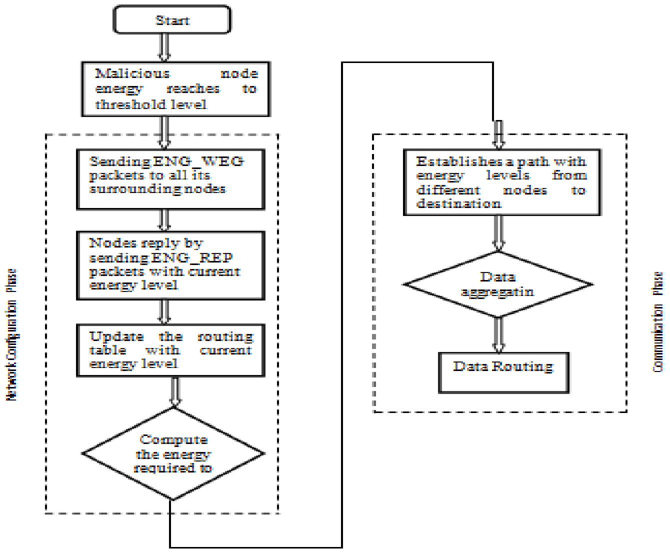
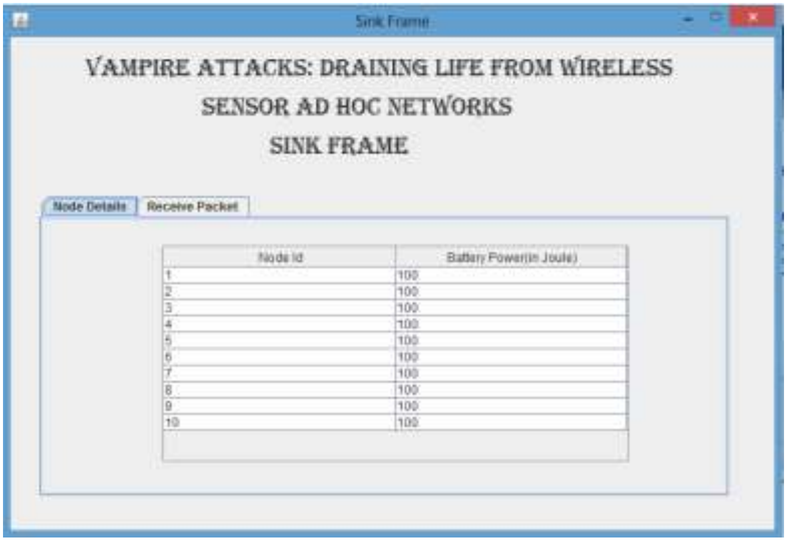

Start
Malicious node energy reaches to threshold level
Sending ENG_WEG packets to all its surrounding nodes
Nodes reply by sending ENG_REP packets with current energy level
Update the routing table with current energy level
Compute the energy required to
Network Configuration Phase
Establishes a path with energy levels from different nodes to destination
Data aggregatin
Data Routing
Communication Phase

Figure: 5 Flow Chart of EWMA in Wireless Sensor

VI. IMPLEMENTATION

a. CASE I: packet transmission without any attack.

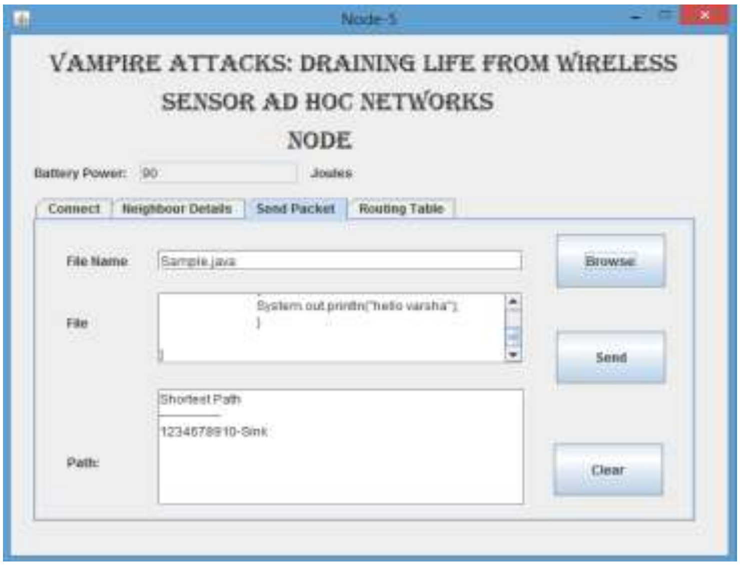


VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR AD HOC NETWORKS

SINK FRAME

Node Id	Battery Power(in Joule)
1	100
2	100
3	100
4	100
5	100
6	100
7	100
8	100
9	100
10	100

Figure: 6.1 Battery Power of all Nodes



VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR AD HOC NETWORKS

NODE

Battery Power: 90 Joules

File Name: Sample.java

File:

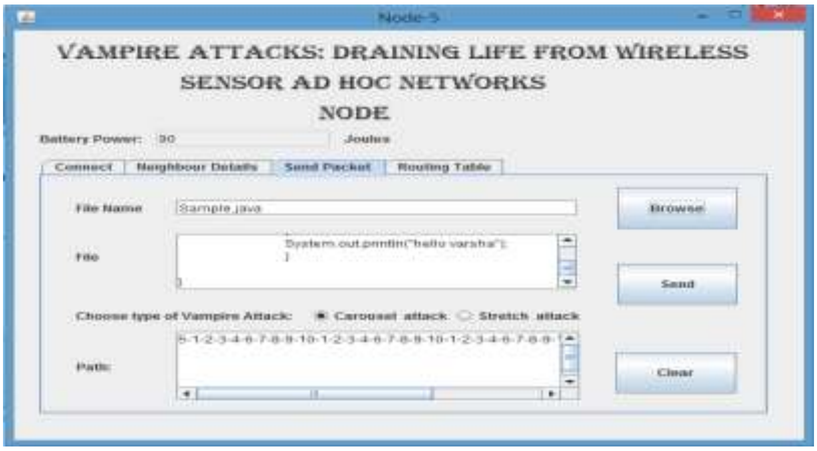
```
System.out.println("hello varsha");
}
}
```

Path:

```
Shortest Path
1234678910-Sink
```

Figure: 6.2 Packet Transmission without Attack

b. CASE II: packet transmission in the presence of vampire attack.



VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR AD HOC NETWORKS

NODE

Battery Power: 90 Joules

File Name: Sample.java

File:

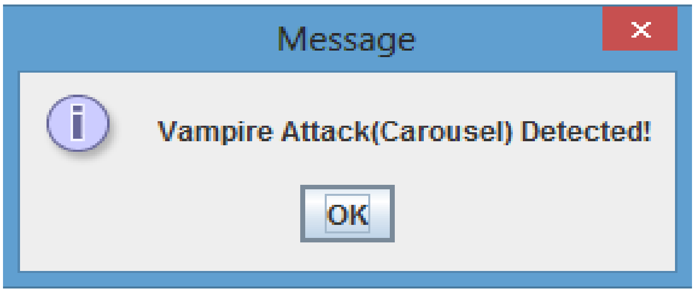
```
System.out.println("hello varsha");
}
}
```

Choose type of Vampire Attack: ● Carousel attack ○ Stretch attack

Path:

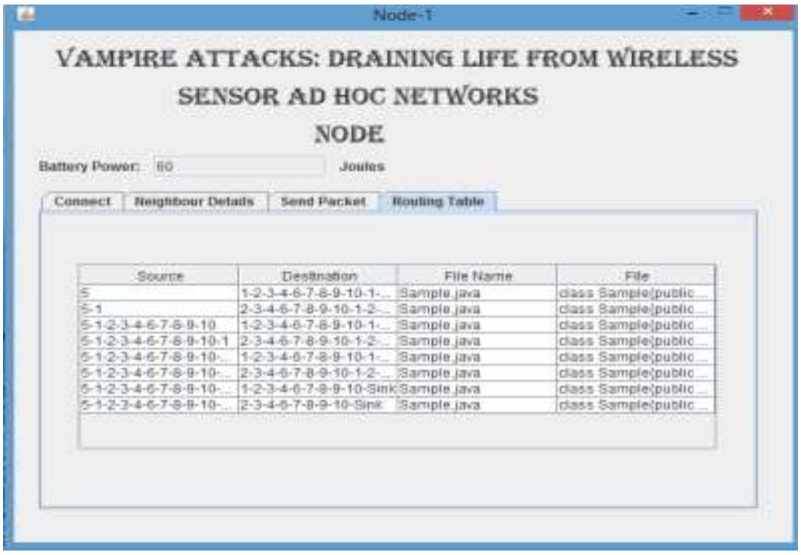
```
5-1-2-3-4-6-7-8-9-10-1-2-3-4-6-7-8-9-10-1-2-3-4-6-7-8-9-1
```

Figure: 6.3 Carousel Attack


Message

Vampire Attack(Carousel) Detected!

Figure: 6.4 Detection of Carousel Attack


Node-1

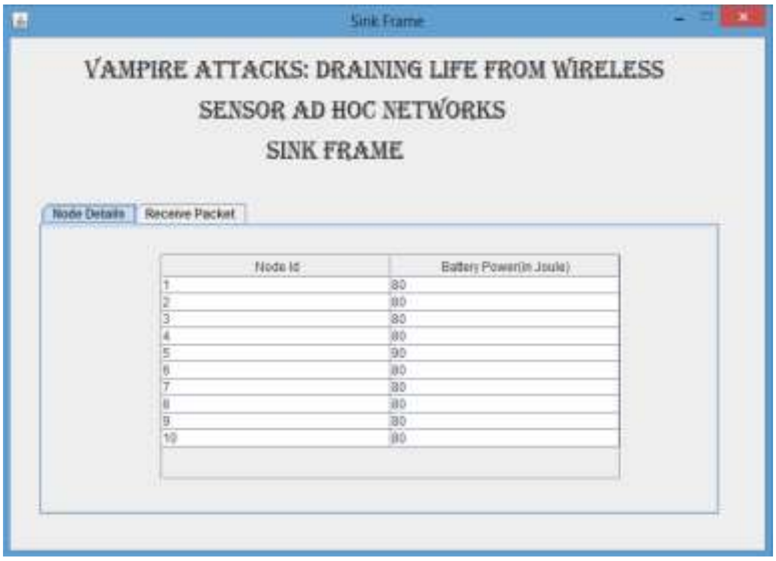
VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR AD HOC NETWORKS

NODE

Battery Power: 60 Joules

Source	Destination	File Name	File
5	1-2-3-4-6-7-8-9-10-1-...	Sample.java	class Sample{public ...
5-1	2-3-4-6-7-8-9-10-1-2-...	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10	1-2-3-4-6-7-8-9-10-1-...	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10-1	2-3-4-6-7-8-9-10-1-2-...	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10-...	1-2-3-4-6-7-8-9-10-1-...	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10-...	2-3-4-6-7-8-9-10-1-2-...	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10-...	1-2-3-4-6-7-8-9-10-Sink	Sample.java	class Sample{public ...
5-1-2-3-4-6-7-8-9-10-...	2-3-4-6-7-8-9-10-Sink	Sample.java	class Sample{public ...

Figure: 6.5 Routing Table Shows Loops in a Path


Sink Frame

VAMPIRE ATTACKS: DRAINING LIFE FROM WIRELESS SENSOR AD HOC NETWORKS

SINK FRAME

Node Id	Battery Power(in Joule)
1	80
2	80
3	80
4	80
5	90
6	80
7	80
8	80
9	80
10	80

Figure: 6.6 Consumption of Battery Power After Carousel Attack

VII. CONCLUSION

In this paper we define vampire attack which is new class of resource consumption attack which uses routing protocol & disable the network permanently by exhausting battery power completely. Simulation results shows consumption of battery power is more in case of carousel attack than normal case/without attack. In this paper we show implementation and detection of vampire attack and for recovery process work is going on by using EWMA technique.

VIII. ACKNOLEDGEMENT

I am Varsha Buktare, would like to take this convenience to explicit our deep obligation and deep view to Dr. Savita R Bhosale, for her excellent advice, beneficial feedback and constant confidence throughout the duration of the project. Her beneficial suggestions were of enormous help throughout my project work. Her discreet criticism kept me working to make this project in a much better way. Working under her was an extremely appreciative experience for me.

REFERENCE

[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, year 2013.

[2] Kirthika.Kand Mr.B.Loganathan, "Vampire attacks in wireless sensor networ k-a survey" IJARCET, vol.3, issue. 7, July 2014.

[3] Trupti A Borgamwar and KanchanDhote,"Review of Resist to Vampire Attack using Wireless Ad-hoc Sensor Network" IJREST,vol.1, issue.4, Sept-2014.

[4] S.Manimala, A.TaskalaDevapriya, "Detection of Vampre Attack Using EWMA in Wireless Ad Hoc Sensor Networks" IJISET,vol.1, issue.3, May-2014.

[5] Tawseef Ahmad Naqishbandi and Imthyaz Sheriff C, "A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT" IJARCSSE, vol.4, issue.2, Feb-2014.

[6] B. Umakanth and J. Damodhar, "Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks" IJER, vol.3, issue23, March-2014.