ISSN:0975-9646



# An Approach for Preventing Resource Consumption Attacks: Vampire

**Manish Soni[1], Priya Saxena[2]**

[1]*Mtech Scholar, Sanghvi Innovative Academy*
[2]*Asst. Professor, Sanghvi Innovative Academy*

***Abstract*- The wireless Sensor Network (WSN) needs to develop with the efficient techniques and the resources preservation techniques. Basically the need of efficiency is due to the limited resource availability i.e. power sources and the computational resources. On the other hand a crucial attack is recently introduced which is deployed to consuming the expensive resources from the network. The attack is termed as the Vampire attack is. The proposed work therefore dedicated for finding the solution for the Vampire attack. The proposed solution for detection and prevention of Vampire Attack is developed with the help of two techniques namely set theory and the threshold based decision making. The implementation and demonstration of the proposed secure technique is performed in NS-2 Environment. For implementing the concept of secure routing the AODV technique is used. Moreover the performance of Network in terms Routing overhead, End to End Delay, Packet Delivery Ratio, Packet Drop Ratio, Throughput and Energy Consumption is calculated.**

***Index Terms*- WSN, Vampire, Recourse Consumption, Energy Preserving, Performance Enhancement**

## I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory, have a RF transceiver (usually with a single omnidirectional antenna), have a power source (batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Such systems can revolutionize the way we live and work [1]. Sensor nodes communicate sensed data to each other and form high-quality useful information about the surrounding environment. Each of these distributed sensor nodes has the ability to collect and route data either to other sensors or to an external base station. This base-station node may be a stationary node or a mobile node proficient of connecting the sensor network to the available communication infrastructure or to the web where a user has access to the sensed information [2]. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

### *A. Objectives*

The basic aim of the proposed work is provide security for the wireless sensor network and improve the performance of network during the Vampire attack conditions. Therefore the following objectives are suggested to accomplish.

*1) Study of Wireless Sensor Networks and their routing techniques:* In this phase the wireless sensor network and their applications in different research areas are discussed. In addition of that the different supporting routing protocols are also studied in this phase.

*2) Investigation of different attacks based on the Routing and Vampire Attack:* In this phase the different kinds of routing based attacks are studied additionally a detailed study on the Vampire attack is also conduced.

*3) Implementation of Methodology:* In this phase the key issues based on the Vampire attack is addressed and their solution is designed. Finally the designed solution is implemented with the help of NS2 simulator.

*4) Performance Analysis of the proposed Secure Technique:* In this phase the performance evaluation of the proposed security technique is provided in addition of that with the similar network performance parameters the comparative study is also provided.

### *B. Domain Overview*

The Wireless Sensor Network due to their mobility simulates the ad hoc nature. Due to this the network routing protocols responsibilities are increases. The routing protocol of such network helps to create and manage the routes among two communicating parties (nodes). The route establishment in such network is performed by the route discovery process therefore the source node broadcast the RREQ packets towards the destination node, when the destination node receive the RREQ packet than the destination acknowledge the source router by using RREP messages. But the malicious user continuously broadcast the RREQ packets to a targeted node, by which the network nodes are also need to involve the communication and they loses their energy. This process also increases the routing overhead and decreases the throughput of the network.

Due to the serious effect of the attacker node need to protect the network from the malicious attacker. Therefore in this presented work a new solution is presented. The proposed solution is able to distinguish the attacker node and prevent them for performing the malicious activity by eliminating them from the network. The proposed solution incorporates the attack identification during the route discovery phases therefore the effect of attacker node is reduced. In addition of that proposed solution is an adoptive solution which utilizes the set theory for finding the malicious attacker in the network based on the network behavioral features produced by the normal network and the network during the attack conditions.

## II. BACKGROUND STUDY

A Numerous Researchers have worked on multiple detection and prevention of Vampire Attacks in Wireless Sensor Network, based on the detection mechanism, the existing techniques of detecting and preventing Vampire Attacks can be illustrate in this section.

***Eugene Y. Vasserma et al [3]*** defined Vampire attack, an attack which drains energy of network node and makes wireless network permanently disable. They have plot random topology of 30 nodes and created some malicious node and proved that this attack is vulnerable to various routing protocols. Work included study of various ways of vampire attacks for various types of protocols. Solution provided in this paper is PLGPa which is proved first solution against vampire attack in packet forwarding phase of network communication. PLGPa is modified version of PLGP combined with No-backtracking and attestation mechanism. No-backtracking property prevents attack by storing local cost of route at each hope and convey to next hope, next hope checks remaining route cost to destination, if it is lower than it confirms that packet is progressing. Using no-backtracking only is not sufficient because malicious node can always lie and provide wrong route cost. So attestation logic is used to verify the packet progress with no-backtracking property. Whenever a node forwards a packet it attaches a signature. These signatures forms a chain attached to every packet, allowing any node receiving it to validate its path, in this way every node verifies the chain to ensure the packet progress. The work is limited to packet forwarding phase only, this solution does not work in topology discovery phase.

***B. Umakanth et al [4]*** proposed a EWMA (Energy Weight Monitoring Algorithm) method to handle the effects caused by these vampire types of attack during the process of packet forwarding phase. In this method energy of a node reach at threshold level it plays an important role by defending against DOS attack. This method relies on the energy levels of the sensors. This method works in two phases Network Configuring Phase and Communication phase. In the former phase a shortest routing path from source to destination in the network. Basically work in this phase is mainly focused towards balancing the load of the nodes and minimizing energy consumption for data communication and resource sharing. The core job of communication phase is to avoid sending of packets through the same node redundantly to deplete the batteries vastly and leads to network destruction because of vampire attacks. The redundancy is eliminated by aggregating the data packets within the forwarding node and sends the remaining packet using shortest route to the destination. Aggregation is the process of copying the content of the packet and copied content compare with data packet if transmitted packet is same the node stops the data packet transmission. In this way it restricts the duplicate packets transmission through the same node again and again and saves nodes energy and send the required data packets through the establish node safely to the destination from the source. The solution proposed in this paper is also limited up to forwarding phase and does not work in topology or path discovery phase.

V. Subha proposed a system that introduces a new authentication and key management mechanism called Hybrid Key Management ***V. Subha et al., [5]***. It is robust and scalable under limited memory resources. It provides strong security by using Low Power Routing. Elliptic Curve Diffie-Hellman which is more lightweight compared to regular Diffie-Hellman. This approach includes group key establishment for authentication and connecting the network. By using a distributed architecture the load of key management is lowered. Secondly this scheme plots the Modified RSA algorithm for encryption /decryption during data transmission. Specifically, this scheme can be expanded to hybrid structure to improve scalability of network. Hence, the expanded scheme is fault-tolerant and efficient for network integrity and confidentiality. A full solution is not given yet but some amount of damage was avoided.

One of the most complicated attacks in wireless sensor network is energy depletion attack. In which vampire attack and Distributed Denial of Service (DDOS) attack were leading. In this paper ***V.Sharmila et al [6]*** using a newly proposed Enhanced Ad Hoc on-Demand Vector (ENAODV) routing protocol, the link break at distant node is repaired with alternate path selection of shortest route in secure manner. The Adaptive Traffic Coalescing (ATC) scheme and Adaptive Power Aware Multicasting (APAM) Algorithm are used to detect a DDOS attack and an incoming traffic monitoring at least energy consuming path selection at network nodes. As a result of simulation, the performance given is related to the energy level and its packet delivery ratio in respect to time consumed. The attacks of energy depletion are detected and blocked by means of using the effective routing protocol Enhanced Ad Hoc on-demand Vector routing protocol (ENAODV) and save the power by Adaptive power aware Multicasting algorithm. The DDOS attacks are prevented by means of the scheme Adaptive traffic coalescing (ATC). Thus the securing of energy of network node is carried out and finding alternate path for broken route link is done.

In a perfect world, there would be no need to hand over sensitive data to agents that may unknowingly or

maliciously leak it. And even if, hand over sensitive data, in a perfect world, distributor could watermark each object so that distributor could trace its origins with absolute certainty. However, in many cases, Distributor must indeed work with agents that may not be 100 percent trusted, and may not be certain if a leaked object came from an agent or from some other source, since certain data cannot admit watermarks. In spite of these difficulties, this paper ***K.Divya Priya et al [7]*** shown that it is possible to assess the likelihood that an agent is responsible for a leak, based on the overlap of his data with the leaked data and the data of other agents, and based on the probability that objects can be "guessed" by other means. This model is relatively simple, author believe that it captures the essential trade-offs. The algorithms presented implement a variety of data distribution strategies that can improve the distributor's chances of identifying a leaker. Paper shown that distributing objects judiciously can make a significant difference in identifying guilty agents, especially in cases where there is large overlap in the data that agents must receive.

Monica Palle give the solution where attacks which is mainly focusing on routing protocol layer that kind of attacker is known as resource depletion attacks. These attacks are causing the impact of persistently disabling the networks by drastically draining the node's battery power. These "Vampire" attacks are not impacting any specific kind of protocols. Finding of vampire attacks in the network is not a easy one. It's very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. And to overcome this vampire attacks proposed an algorithm named optimal energy boost-up protocol (OEBP) is proposed which analyzes the routing table and verify the attacks which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. Authors proposed a EWMA method to bound the damage caused by these vampire types of attacks during the packet forwarding phase. This enhanced work increases the Quality of service in the network and it will regulates all the nodes activity. They discuss some methods to overcome and alternative routing protocols solution will be avoiding some sort of problems which causing by vampire attacks [8].

G. Vijayanand says vampire attacks are causing impacts on persistent disabling the network by draining the battery power. These "Vampire" attacks are not impacting any specific kind of protocols. Finding of vampire attacks in the network is not a easy one. It's very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. They discuss some methods and alternative routing protocols solution will be avoiding some sort of problems which causing by vampire attacks [9].

## III. PROPOSED SYSTEM

### *A. Methodology*

The proposed solution is works in two phases for identifying the attacker node in network during the route discovery of the network. In first phase a normal network is configured without any malicious node. Using this network the threshold values are computed which are used for making decision for malicious activity in network. In next phase the computed network thresholds are used for identifying them and eliminating them. Both the phases of the solution development are reported as:

**Threshold estimation**

In this phase the key work is to prepare a threshold value by which the decision is developed for identifying the malicious nodes in network. Therefore a network with N number of nodes is created ideally. The ideal network contains no malicious node and performs the communication sessions by using the performed communication sessions the threshold values are computed. There are two parameters namely node RREQ broadcast and the consumed energy is preferred for the solution development and threshold development.

$$\mu_{broadcast} = \frac{1}{N}\sum_{i=1}^{N} B_i$$

Where the $B_i$ is the amount of packets broadcast by a node i
In further the threshold values are created using the following formula:

$$V_{t1}^{B} = \frac{1}{N}\sum_{i=1}^{N} (B_i - \mu_{broadcast})^2$$

Where $V_{t1}^{B}$ is a threshold values which is allowed by the network broadcast.

Similarly the energy consumption of network is also estimated, therefore the following formula are used.

$$\mu_{Energy} = \frac{1}{N}\sum_{i=1}^{N} E_i$$

Where the $E_i$ is the amount of energy dropped by a node i
In further the threshold values are created using the following formula:

$$V_{t1}^{E} = \frac{1}{N}\sum_{i=1}^{N} (E_i - \mu_{Energy})^2$$

where $V_{t1}^{E}$ , is a threshold values which is allowed by the network energy consumption.

**Identification of malicious node**

In this phase the similar kind of network is created and the computed thresholds are used for locating the malicious node in network. Therefore during the route discovery process a set of nodes are created that are consumes energy more than$V_{t1}^{E}$. The set of high energy consumption nodes are denoted as:

$$Set_{t1}^{E} = \{N_1, N_2, \dots, N_n\}$$

Additionally the set of nodes those are having higher broadcast between two time intervals or at time $\Delta t$ are given by the following set

$$Set_{t1}^{B} = \{N_1, N_2, \dots, N_n\}$$

By using the set of both the nodes the suspected list of the malicious node is created using the following equation.

$$SS_{t1} = Set_{t1}^{B} \cap Set_{t1}^{E}$$

Similarly at the time t2 the network suspected nodes are computed

$$SS_{t2} = Set_{t2}^{B} \cap Set_{t2}^{E}$$

Using this final set of actually suspected node is computed as:

$$SS_t = SS_{t1} \cap SS_{t2}$$

$SS_t$ is the set of node that are really suspected for the network and consumes higher energy and resources for the network.

In further for detection of malicious node in network and to remove them in further from time t3, the following process is used by temporally removing suspected node from network. compute $V_{t3}^{E}$ and $V_{t3}^{B}$.

1: Compute the difference for time $t_1$ $and$ $t_2$

$$diff_{t1}^{t2} = V_{t2}^{E} - V_{t1}^{E}$$

2: Compute the difference for time $t_2$ $and$ $t_3$

$$diff_{t2}^{t3} = (V_{t3}^{E} - V_{t2}^{E})SS_t$$

3: $if\ diff_{t1}^{t2} > diff_{t2}^{t3}$

4: Remove node from network permanently

5: End if

Hence suspected node turns to vampire node. If there are multiple suspected nodes found in $SS_t$ then same process is repeated by alternative temporary removal and one of them is turned to be attacker node.

.

*B. Implementation*

This section provides the details about the experiments performed on the developed networking system.

*1) Simulation Setup:* To prepare and design the desired simulation model of communication the below given network parameters are listed in table

| PROPERTIES | VALUES |
|---|---|
| Simulation Area | 750 X 550 |
| Routing Protocol | AODV |
| Number of Mobile Nodes | 50, 100, 150, 200 |
| Channel Type | Wireless Channel |
| MAC Protocol | 802.11 |
| Simulation Time | 20.0 Sec |

**Table 1 Simulation Parameters**

*2) Simulation Scenario:* In order to perform the experiments the following different scenarios are prepared for simulation and network performance evaluations with different network sizes.

**a. Implementation of Normal AODV routing protocol:** In this simulation scenario the traditional AODV routing protocol implemented with wireless sensor networks. After that a malicious attacker is deployed on network. Using the generated network trace files the network performance is measured and further used for comparative performance study.

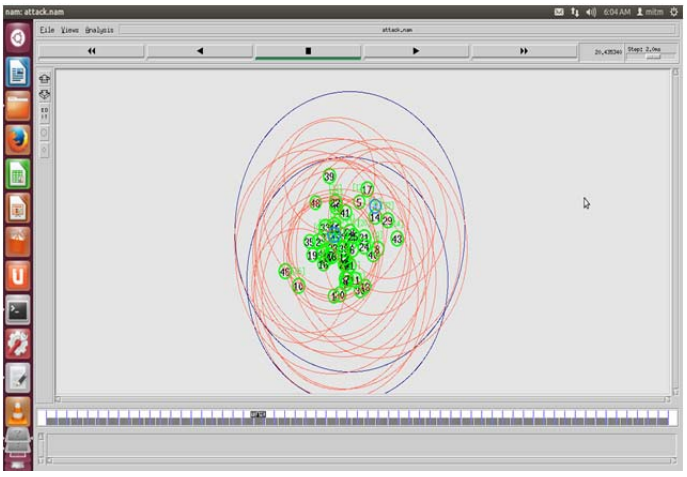

**Figure 1** ***traditional AODV based simulation***

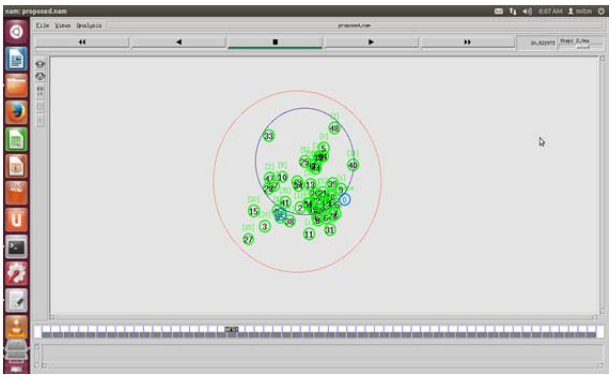

**Figure 2** ***proposed secure routing technique simulation***

**b. Simulation using the proposed secure routing technique:** In this simulation scenario the proposed routing technique which is developed with the help of AODV routing modifications are implemented with wireless sensor network. Additionally a similar kind of attacker node on the network is deployed. The deployed attacker is normalized using the technique and their performance is estimated on the basis of the network trace files.

## IV. Result Analysis

Graphs are plotted and concluded that proposed scheme has improve throughput value and packet delivery ratio also reduces end to end routing delay.

### *A. End to end delay*

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ delay = receiving\ time - sending\ time$$

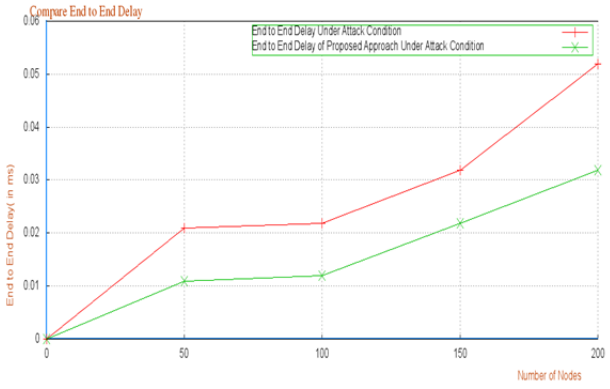


**Figure 3** ***End to end delays***

Above Figure shows the comparative end to end delay of the traditional AODV routing and the proposed secure routing technique. In this X-axis contains the number of nodes in network and the Y-axis shows the performance of network in terms of milliseconds. According to the obtained results the proposed technique is produces less end to end delay as compared to traditional routing technique under attack conditions.

### *B. Packet drop ratio*

The amount of packets that are not successfully delivered to the destination is termed as the Packet Drop Ratio. In this graph the X-axis contains the number of nodes on which the experiments are conduced and the Y-axis contains the percentage of packet dropped. According to the obtained performance as the amount of nodes in network is an increase the packet drop ratio of the traditional routing technique is increases as compared to the proposed technique. Therefore the proposed technique provides higher performance as compared to traditional routing technique.

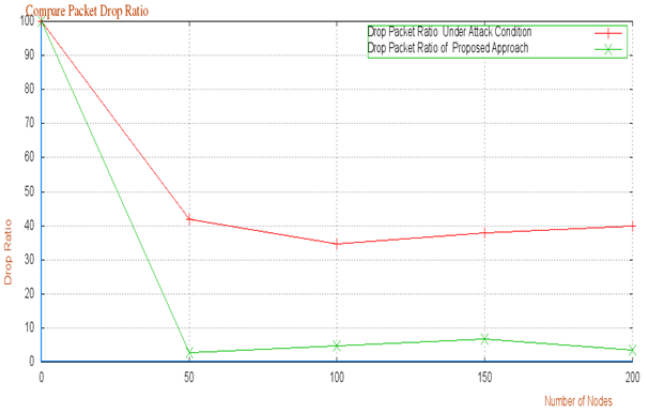


**Figure 4** ***Packet drop ratio***

### *C. Energy consumption*

The energy consumption of the node demonstrates the rate of change in energy level of the node from it is initial energy level. In given graph the performance of traditional algorithm is demonstrated using red line and proposed technique given using the green line. Additionally the X-axis of the figure shows the number of nodes in the network during the experiments and the Y- axis shows the energy consumed in terms Jules. According to the obtained performance of the routing techniques the proposed technique is consumes less energy as compared to the traditional technique. Therefore the proposed technique is more energy efficient as compared to the traditional approach.

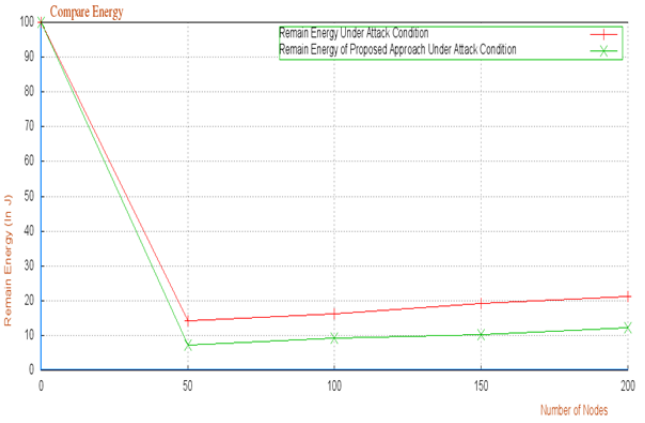


**Figure 5** ***Energy Consumption***

*D.Packet delivery ratio*

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

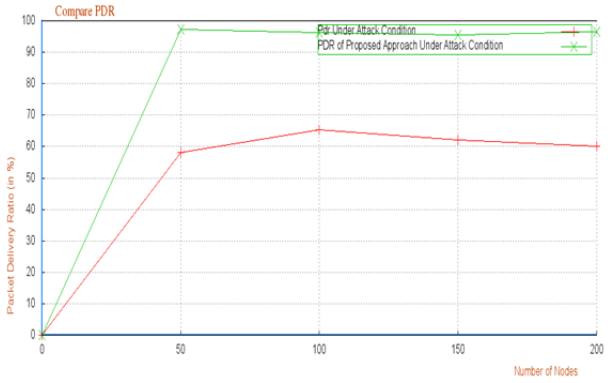


**Figure 6** ***Packet delivery ratio***

In above graph, X-axis shows the number of nodes in the network and the Y-axis shows the amount of packets successfully delivered in terms of the percentage. According to the obtained results the proposed technique delivers more packets as compared to the traditional technique even when the network contains the attacker node therefore the proposed technique able to avoid the attack effect and improve the network performance.

*E. Routing overhead*

During the communication scenarios it is required to exchange the packets for different tracking and monitoring purpose. Therefore the additional injected packets in network is termed as the routing overhead of the network. In given graph X-axis shows the amount of network nodes exist during the experimentation and the Y-axis shows the routing overhead of the network. According to the obtained performance of the techniques the proposed technique produces less routing overhead as compared to the traditional AODV routing under attack conditions.

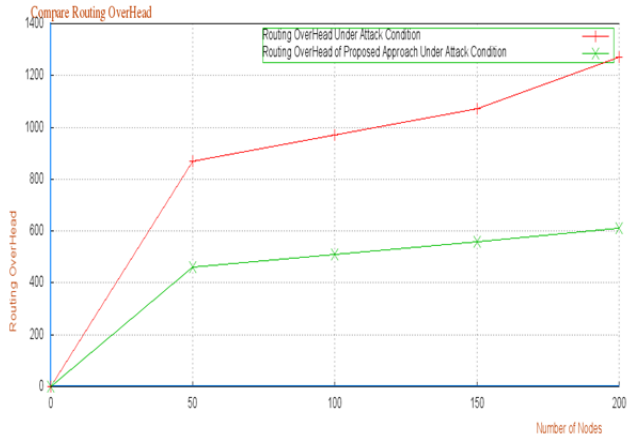


**Figure 7** ***Routing overhead***

*F. Throughput*

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

Here, X-axis shows the number of nodes in network and the Y-axis shows the throughput of the network in terms of KBPS. According to the obtained performance the proposed technique improve the throughput of the network during the attack conditions also therefore the technique is effectively avoid the attack effect as compared to the traditional routing technique.

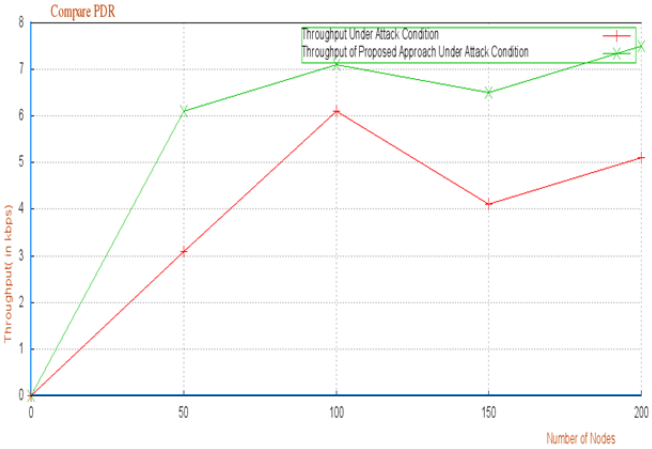


**Figure 8** ***Throughput***

## V. Conclusion and Future Work

The wireless sensor network is one of the most popular network technologies now in these days. A number of critical applications are developed with the help of the wireless sensor networks. In this presented work the security aspects of the sensor network is investigated and a new solution for securing the network against the Vampire attack is proposed. The Vampire attack is a kind of resource consumption attack for the wireless sensor network. According to the obtained performance of the proposed solution for locating the malicious node in network the network performance is improved. Additionally the malicious node and nodes are successfully located in the network. Therefore the proposed solution is effective and efficient for Vampire attack detection and prevention.

**Future Work**

The proposed work is intended to identify the malicious nodes in network by which the security and performance of the network both can be obtainable. The required security solution is developed successfully and their performance is estimated under the attack conditions. The results show the effectiveness of the proposed solution. In near future the work is enhanced more with adding more parameters to distinguish more or different kinds of network attacks also same solution can be modified to defend other protocols against vampire attack.

## REFERENCES

[1] A. Anto Jenifer, V.Thangam, "Maintaining Lifetime of Wireless Ad-hoc Sensor Networks by Mitigating Vampire Attacks", – International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 9 | February 2015

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Caryici, "Wireless Sensor Networks: a survey", Elsevier Computer Networks, December 2001.

[3] 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

[4] B. Umakanth1, J. Damodhar2, "Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks", International Journal of Engineering Trends and Technology, Volume 4, Issue 8, August 2013

[5] V.Subha1 and P.Selvi, "Defending against vampire attacks in wireless sensor networks", International Journal of Computer Science and Mobile Computing, Volume 3, Issue 11, November 2014 [6] Anoopa S, Sudha S K, Vol. 4, April 2014, "Detection and Control of Vampire Attacks in Ad-Hoc Wireless Networks".

[6] V.Sharmila1, "Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network", International Journal of Computer Science and Mobile Computing, Volume 3, Issue 8, August 2014

[7] K.Divya Priya, V.Vijayalakshmi, "Mitigating Vampire Attack in Wireless Ad-Hoc Sensor Networks of Draining Life Using Resource Allocation", International Journal of Emerging Technology in Computer Science & Electronics,ISSN: 0976-1353 Volume 9 Issue, July 2014

[8] Monica Palle, Seelam Sai Satyanarayana Reddy, "Detection Elimination and Overcoming of Vampire Attacks in Wireless Ad hoc Networks", IJRIT International Journal of Research in Information Technology, Volume 2, Issue 6, June 2014, Pg: 224-237

[9] G. Vijayanand, R. Muralidharan, "Overcome Vampire Attacks Problem in Wireless Ad-Hoc Sensor Network by Using Distance Vector Protocols", International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 1, January- 2014, pg. 115-120

[10]The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns