International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Vampire Attack Detection and Prevention to Defending WSN Based Application

Rajani Jagle[1], Dr. Abhay Kothari[2]

[1]M. Tech Student, Department of Computer Science and Engineering, Acropolis Institute of Technology and Research Indore, India
[2]Assisance Professor, Department of Computer Science and Engineering, Acropolis Institute of Technology and Research Indore, India

Abstract: ***The wireless technologies are growing due to fewer dependencies on fixed infrastructure. Wireless sensor network is applicable in various small scale application developments to large scale application development. WSN provide the missing connections among Internet and physical world. The "Vampire" is a model of malicious activity that is not specific to any specific protocol. That relies on properties of many popular classes of routing protocols. Vampire attack is transmission of a message that causes energy consumption of the network rather than honest node transmitted a message to same destination. The introduced methodology for detection and prevention of Vampire attack is developed using time calculation of sender and receiver when the packet is transferred. The implementation and execution of the proposed concept is implemented through AODV routing protocol modification. Additionally the network simulator 2 i.e. NS-2 is used for simulation of security scheme. The experimental results show the adoptable performance of the algorithm and improve throughput, packet delivery ratio, and energy consumption. Additionally reduces the end to end delay between communicating nodes.***

Keywords: AODV, NS-2, Routing Protocol, RREQ, RREP, Security, Vampire Attack, Wireless Sensor Network.

1. Introduction

Wireless sensor networks have as of late progressed toward becoming noticeable quality since they acquire the possibility to alter many portions of our economy and life, from ecological checking and protection, to assembling and business resource administration, to computerization in the transportation and medicinal services enterprises. The plan, execution, and operation of a sensor organize requires the conjunction of many orders, including signal preparing, systems administration and conventions, installed frameworks, data administration and dispersed calculations. Such systems are regularly conveyed in asset obliged conditions, for example with battery worked hubs running un-fastened. These requirements manage that sensor organize issues are best drawn closer in an unfriendly way, by together considering the physical, systems administration, and application layers and making real outline tradeoffs over the layers [1, 2].

A. Wireless Sensor Network

Wireless sensor networks are collection of nodes where each node has its own sensor, processor, transmitter and receiver and such sensors usually are low cost devices that perform a specific type of sensing task. These are low cost due to this such sensors are deployed opaque throughout the area to monitor specific event. The remote sensor organizes generally work in broad daylight and uncontrolled zone; thus the security is a noteworthy test in sensor applications. Wireless sensor network (WSN) is a collection of tiny devices, inexpensive sensor nodes with several distinguishing characteristics. It has very low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions [3].

Wireless Sensor Network works in environment conditions where wired connections are not possible. Wireless sensor nodes consists of different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of physical and environmental conditions [4].

The WSN is built of "nodes" – from a few hundreds or even thousands, where every node is associated with one (or in some cases a few) sensors. Remote sensor hubs contain exhibit of sensors in the event of different information accumulation. The sensor hub can be put for persistent or specific detecting, area detecting, and movement detecting and occasion location and so on. A base station connects the sensor system to detect, handle and spread data of focused physical situations [5].

Commonly, WSNs contain hundreds or thousands of these sensor hubs, and these sensors can convey either among each other or specifically to an outside base station (BS). A more prominent number of sensors takes into account detecting over bigger land districts with more noteworthy exactness. Figure 1 demonstrates a schematic graph of sensor hub segments. Fundamentally, every sensor hub involves detecting, handling, transmission, mobilizer, position discovering framework, and power units (some of these parts are discretionary, similar to the mobilizer).

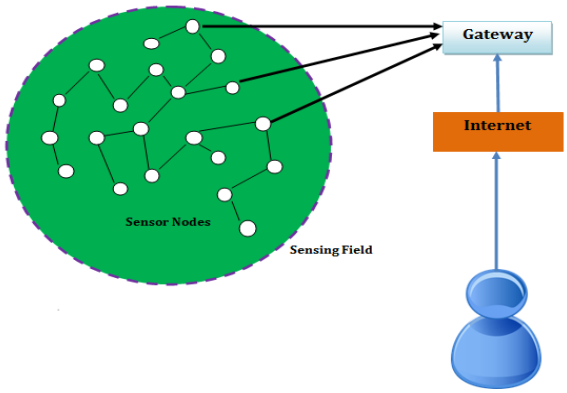

Figure 1: A Typical View of WSN

A similar figure demonstrates the correspondence engineering of a WSN. Sensor hubs are normally scattered in a sensor field, which is a zone where the sensor hubs are sent. Sensor hubs organize among themselves to deliver astounding data about the physical condition. Every sensor hub constructs its choices in light of its central goal, the data it right now has, and its learning of its registering, correspondence, and vitality assets. Each of these scattered sensor hubs has the ability to gather and course information either to different sensors or back to an outside BS(s) [6].

2. Proposed System

a) Methodology

In this research work, we propose a solution for securing network from energy draining attack i.e. vampire attack. In this, we prepare an algorithm for detecting preventing attack. Eventually, attacker node consumes network resources when they establish. For a while source node send a packet to its corresponding destination. If there is attacker node exist, it receive packets and circulate it to long distance rather forward it to destination. Hence, nodes creating an infinite loop and traverse the packet between the nodes.

Our approach is capable to deliver adoptable solution for vampire attack and eliminate from networks. Firstly, we establish a network which is an idle condition i.e. there is node malicious node exist in network. And simply, discover the path to find source and destination node using RREQ and RREP strategy. Once a node starts communicate to each other via sending or receiving packets, there is case when malicious attacker is enter in this network to harm the basis functioning of the network. If there is vampire attacker is entered in network, then now we have to apply our proposed method to prevent this. Firstly, we start to send a packet to destination, append a sending time with packet when it sent. We record the packet sending time from sender and now we also record the receiving time at receiver side when packet arrives at the destination. Therefore, sum the total time of sender and receiver time. We denote this termed as T_1 same process is repeated back from receiver to destination and record this total time asT_2. After that find the difference between two time of sender and receiver noted as T_1 andT_2. If there is difference between this we assume there is availability of vampire attacker. If T_1 is larger thanT_2 that means there is a case of attacker. If it is return false no any attacker is exist, we can remain communication. The proposed work is secure the network and very efficient to adopt, if multiple attacker is exist.

b) Proposed Algorithm

The proposed work is indented to secure the routing technique, thus AODV routing technique is modified to identify the malicious nodes between source and destination. Additionally prevent the network from vampire attacker. . The algorithm is demonstrating using table 1:

Table 1: Proposed Secure Routing Algorithm

Input: Network with N nodes **Output:** identify malicious route R
1. *Process:* 2. *Source send RREQ to destination node* 3. *Sender Notice Sending time* T_{start} 4. *Destination wait till RREQ not received from all neighbour* 5. *Destination Notice receiving time* $T_{receive}$ 6. *Destination acknowledge with RREQ* $+T_{receive}$ *from shortest path and alternate path* 7. *Sender compute* $\Delta TS = T_{receive} - T_{start}$ 8. *Sender compute* $\Delta TA = T_{receive} - T_{start}$ 9. $if(\Delta TS < \Delta TA)$ 10. *Route not contains attacker* 11. *Start communication* 12. *Else* 13. *Route is malicious* 14. *End if* 15. *Return malicious route*

3. Implementation

The simulation is being implemented in the Network simulator [7]. Protocol used here is AODV.

Table 2: Simulation Scenarios

Parameters	*Values*
Dimension	1000X1000
Antenna Model	Omni Antenna
Radio-Propagation	Two Ray Ground
Traffic Model	CBR
Channel Type	Wireless Channel
Number of Nodes	50, 100, 150, 200
Routing Protocol	AODV

1. Implementation of Traditional PLGP-a Routing Approach: In this recreation situation the customary PLGP-a convention actualized with the remote sensor systems. After that a malignant aggressor is conveyed on system. Utilizing the created organize follow documents the system execution is measured and additionally utilized for similar execution examine. The figure 2 demonstrates the AODV based remote sensor connect with the aggressor hub. This recreation comes about demonstrates that PLGP-a working situation which diminishes the system vitality consumption from this causes other parameter is influenced because of one parameter is corrupting.

2. Simulation using the Proposed Secure Routing Technique*:* In this simulation scenario the proposed secure routing technique which is developed with the help of AODV routing modifications are implemented with the 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. Additionally the measured performance is compared with the traditional PLGP-a performance under attack conditions. The figure 3 demonstrates the simulation screen of the proposed secure routing technique for vampire attack

prevention. Similarly Simulation has been performed with different network sizes.

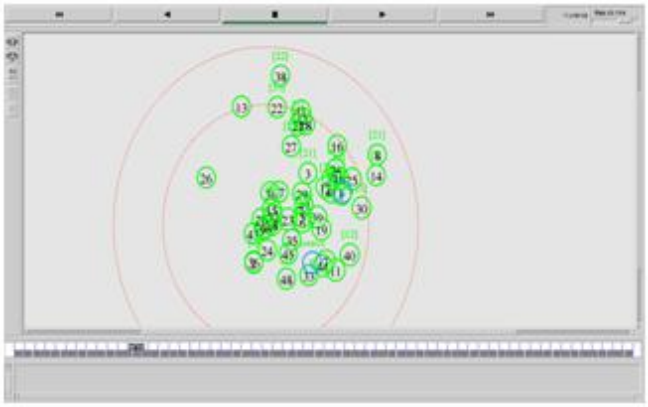

Figure 2: Traditional PLGP- A with 50 Nodes

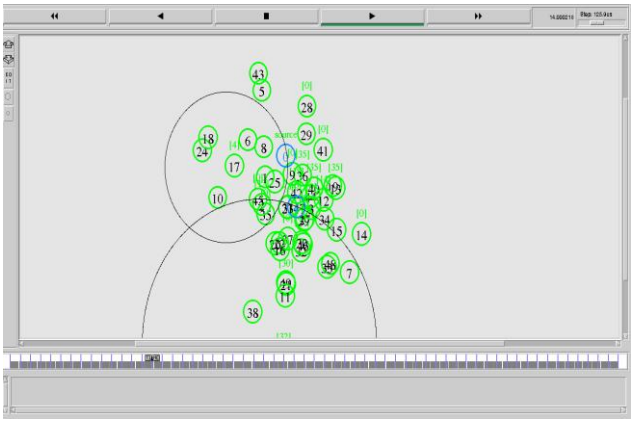

Figure 3: Proposed Secure Routing Techniques With 50 Nodes

4. Result Analysis

4.1 End to End delay

End to end dayalludes to time required, for a packet to be transmitted over a system from source to goal device, this delay is considered using the below given formula.

$$\text{E2E Delay} = \text{Receiving Time} - \text{Sending Time}$$

Figure 4 demonstrates the similar End to End Delay of the conventional PLGP-a directing and the proposed secure steering method. In this figure the X hub contains the quantity of hubs in system and the Y hub demonstrates the execution of system as far as milliseconds. As indicated by the acquired outcomes the proposed system is creates less end to end defer when contrasted with customary steering strategy under assault conditions.

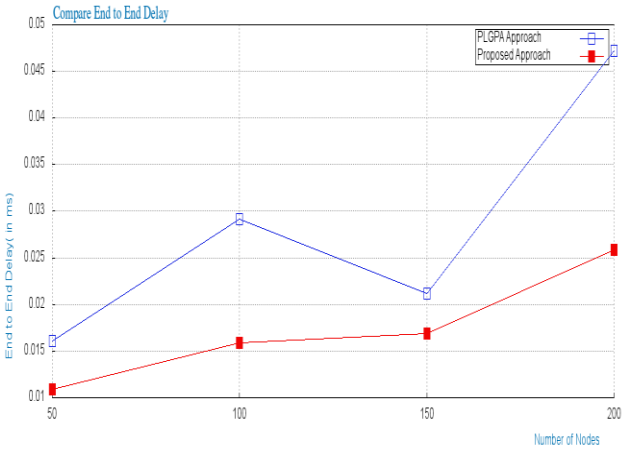

Figure 4: End to End Delay With Number Of Nodes

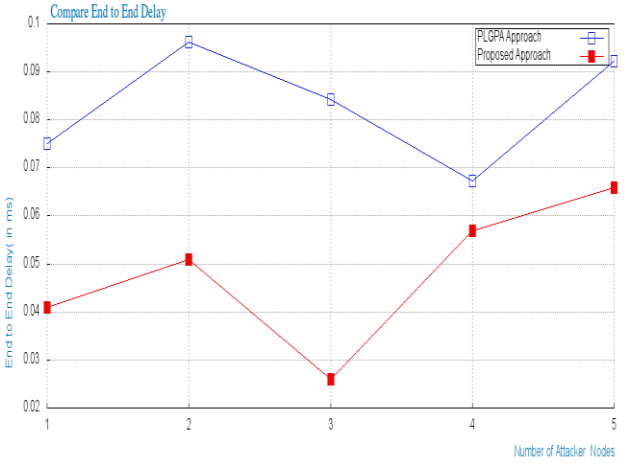

Figure 5: End to End Delays With Number Of Attacker

Figure 5 shows the different attacker node of end to end delay parameter. This figure demonstrates different attack variation on which performance is evaluated for both methods. Therefore the proposed technique is an efficient technique and produces less amount of time.

4.2 Packet Delivery Ratio

The execution parameter Packet conveyance proportion here and there named as the PDR proportion gives data about the execution of any directing conventions by the effectively conveyed bundles to the goal, where PDR can be anticipated utilizing the equation given:

$$\text{Packet Delivery Ratio} = \frac{\text{Total Reveived Packets}}{\text{Total Sent Packets}}$$

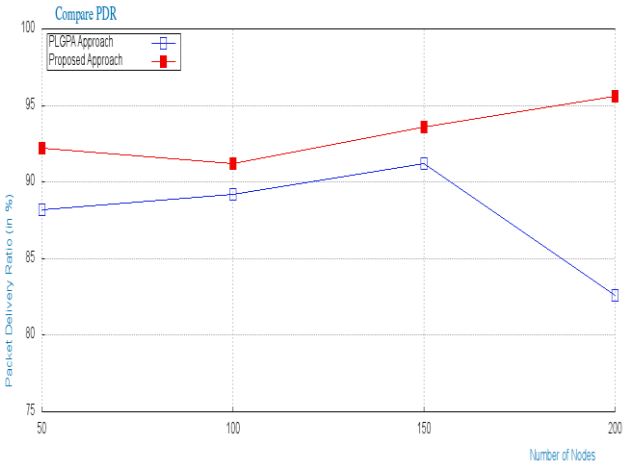

Figure 6: Packet Delivery Ratio with Number of Nodes

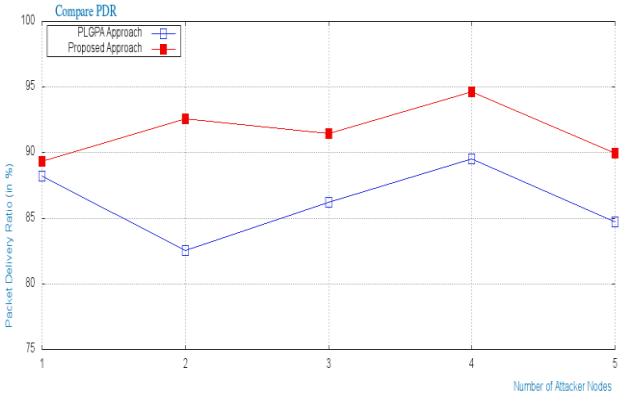

Figure 7: Packet Delivery Ratios with Number of Attacker

The close package movement extent of the frameworks is given using figure 6, in this graph the X point shows the amount of points in the framework and the Y turn exhibits the measure of bundles adequately passed on to the extent the rate. The blue line of graph speaks to the execution of the conventional PLGP-a system and the red line demonstrates the execution of the proposed secure procedure. Likewise figure 7 given the situation of the 5 aggressor hub in the system. As indicated by the acquired outcomes the proposed method conveys more bundles when contrasted with the conventional strategy notwithstanding when the system contains the more aggressor hub accordingly the proposed procedure ready to get away from the assault impact and enhance the system execution.

4.3 Throughput

The throughput is the rate of fruitful correspondence over a channel. This information might be conveyed over a physical or sensible connection, or go through a specific system hub. The throughput is typically measured in bits every second (piece/s or bps), and in some cases in information bundles every second or information parcels per schedule vacancy.

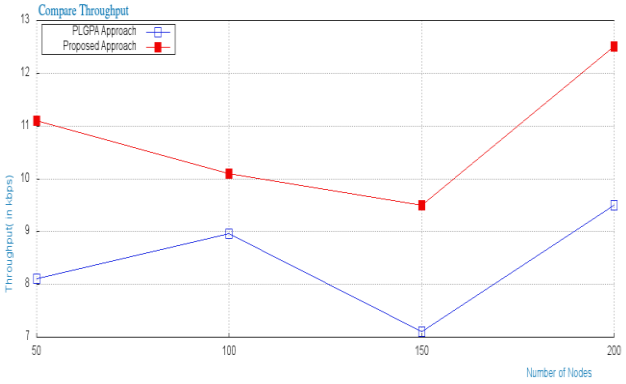

Figure 8: Compare Throughput with Number of Nodes

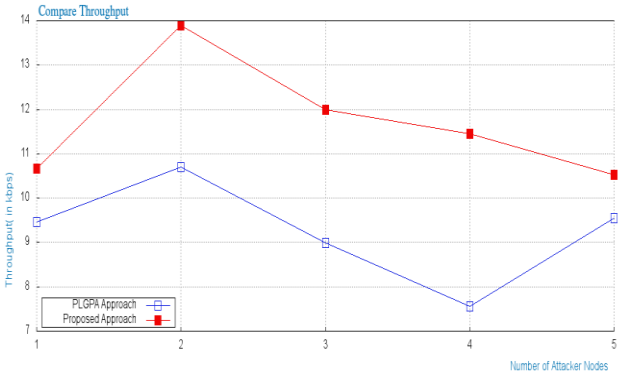

Figure 9: Compare Throughput with Number of Attacker

The similar throughput of the system is exhibited utilizing figure 8, in this chart the X hub demonstrates the quantity of hubs in system and the Y hub demonstrates the throughput of the system as far as KBPS.The green line in this outline demonstrates the execution of the proposed system and the blue line demonstrates the execution of the customary PLGP-a steering. As indicated by the acquired execution the proposed method enhance the throughput of the system amid the assault conditions additionally in this way the procedure is viably keep away from the assault impact when contrasted with the customary directing strategy. Additionally while pernicious hub increments in system execution is declines. In this way our proposed approach is material where there is extensive number of Vampire assaults are exists. This situation result has been appeared in figure 9.

4.4 Routing Overhead

Routing overhead is described as the amount of additional packets injected in network for communication. The key reason behind to compute this parameter is, because the routing overhead reduces the packet delivery ratio and transmission rate of the data. The given figure 10 shows the performance of network in terms of routing overhead. The routing overhead increases the amount of bandwidth consumption.

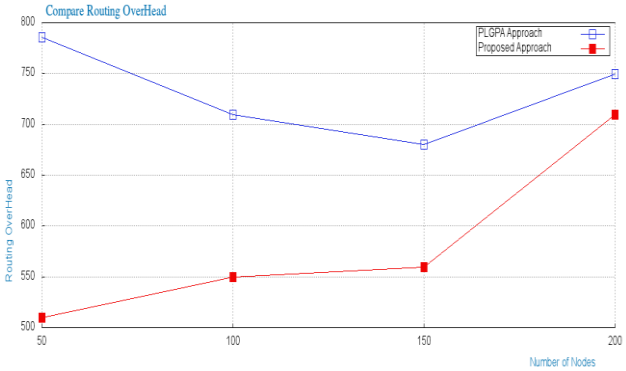

Figure 10: Compare Routing Overhead With Number of Nodes

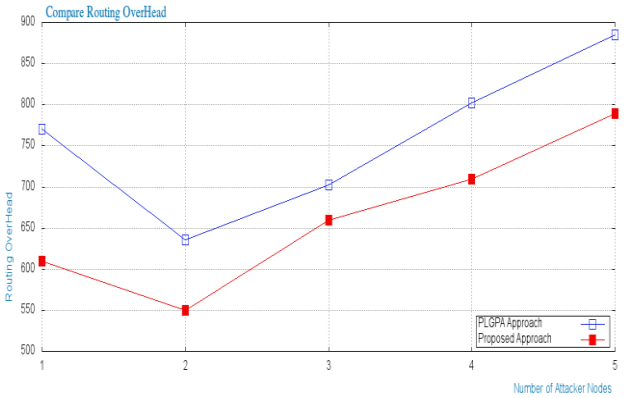

Figure 11: Compare Routing Overhead with Number of Attacker

According to the obtained results the network under the attack condition increases the routing overhead of the network thus the traditional PLGP-a routing protocol shows increasing routing overhead of network. On the other hand when the network is configured through the proposed routing protocol the routing overhead significantly reducing. Therefore the proposed method is able to recover the network from the Vampire attack. Routing overhead is great impact on the network while malicious node is in majority. Since therefore figure 11 demonstrate 5 attacker nodes on x-axis and y-axis show network performance by means routing overhead.

4.5 Energy Consumption

The energy consumption of the node demonstrates the rate of modify in energy level of the node from its initial energy level. The low energy consumption demonstrates the higher performance of network. The network consumes energy at the every event of node such as packet forwarding and others. Therefore the energy consumption is measured with the respect of initial energy of the network node.

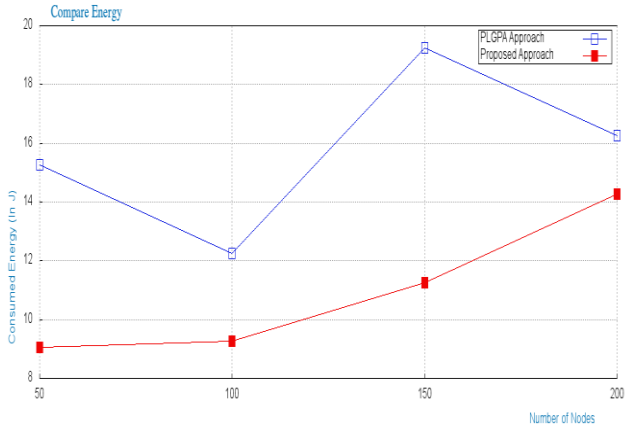

Figure 12: Compare Energy Consumption With Number Of Nodes

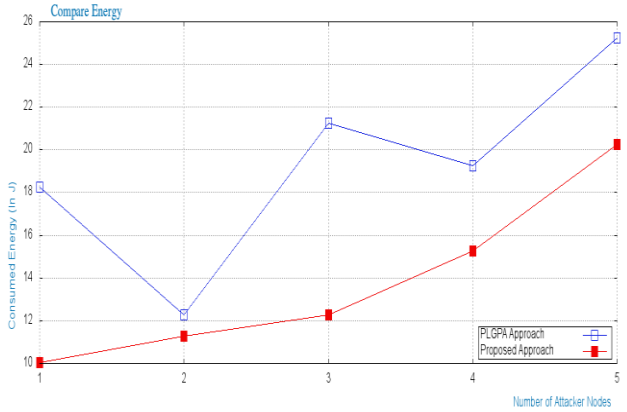

Figure 13: Compare Routing Overhead with Number of Attacker

The relative execution of the proposed strategy and conventional procedure as far as vitality utilization is given in figure 12. In this graph the execution of assault condition is exhibited utilizing blue line and proposed system given utilizing the red line. Furthermore the X hub of the figure demonstrates the quantity of hubs in the system amid the examinations and the Y hub demonstrates the vitality expended in wording Jules. As indicated by the got execution of the directing systems the proposed method is expends less vitality when contrasted with the conventional approach. In this manner the proposed procedure is more vitality proficient. Also, in figure 13 show aggressor diagrams on various quantities of execution levels. This chart portrays specific assailant hub which navigate long way to course the parcel with most extreme separation course. Along these lines, execution is depleting the vitality level of system.

5. Conclusion

Wireless sensor networks comprise of little hubs with detecting, calculation, and wireless interchanges abilities. Many directing, control administration, and information dispersal conventions have been particularly intended for WSNs where vitality mindfulness is a basic plan issue Nodes can be effectively conveyed in irregular or deterministic form and are ordinarily battery worked. So, energy consumption is one of the most important factors. In this presented work the vampire attack is targeted for the investigation and research study. The Vampire attack is a kind of resource consumption attack for the wireless sensor

network. In this attack the attacker node continuously flood the RREQ packets to consume the resources of a targeted node. By which the node frequently consumes their energy and leave the network. Thus that is a serious kind of attack for the wireless sensor network. The implementation of the required secure solution is performed using NS-2 network simulation environment, additionally AODV routing protocol is modified for incorporating the concept of security in sensor network. The proposed technique is implemented and simulated with the 50, 100, 150 and 200 nodes. Additionally we performed two network scenarios. In first scenario we consider generalize network where vampire attacker is exists. Similarly, in second scenario, we consider there is multiple vampire attackers are exists i.e. 1, 2, 3, 4 and 5. So the given solution is capable to detect and prevent network from the attacker.

References

[1] Ashish Patil and Rahul Gaikwad. (2015, July). "Preventing Vampire Attack in Wireless Sensor Network by using Trust Model", IJERT, Vol. 4 Issue 06
[2] D K Singh, M P Singh and S K Singh. (2010,Nov). "Routing Protocols in Wireless Sensor Networks – A Survey", IJCSES, Vol.1, No.2
[3] Jun Zheng and Abbas Jamalipour. (2009) "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE
[4] Anjali Potnis, and C S Rajeshwari. (2015). "Wireless Sensor Network: Challenges, Issues and Research", Proceedings of ICFCT'2015, pp. 224-228, March 29-30, Singapore
[5] S. Tilak, N. Abu-Ghazaleh, W. Heinzelman. (2002, April) "A Taxonomy of Wireless Micro-sensor Network Models," ACM SIGMOBILE Mobile Computer Communication Rev., vol. 6, no. 2, pp. 28–36
[6] By JeongGilKo, John A. Stankovic, Andreas Terzis, and Matt Welsh. (2010, November). "Wireless Sensor Networks for Healthcare", Proceedings of the IEEE, Vol. 98, No. 11
[7] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/
[8] E. Y. Vasserman, N. Hopper. (2013, Feb). "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks,"IEEE, vol. 12
[9] Sushma Thakur1, Sandeep Raskar. (2016, June). " Avoidance of Vampire Attacks in Wireless Ad hoc Sensor Network", International Journal of Engineering Science and Computing
[10] Chahana B. Thakur V.B.VaghelaAssot "Detection and Elimination of Vampire Attack in Mobile Ad hoc Network",.
[11] Harpreet Kaur,Jasmeet Singh Gurm. (2016, Sep). "Time Based
[12] Detection and Prevention of Vampire Attacks in Wireless Sensor Network" IRJET
[13] Vishal Lokhande , Sanjay D. Deshmukh , Surendra T. Sutar. (2016). "Vampire Attacks Prevention In Wireless Sensor Network", Issn (Print): 2393-8374, (Online): 2394-0697, Volume-3, Issue-1
[14] A. Sanofer Nisha ,V. Vaishali ,T. Shivaranjani. (2016, Sep). "The effect of vampire attacks on distance vector routing protocols for wireless ad hoc sensor networks"
[15] Amee A. Patel, Sunil J. Soni. (2015). " A Novel Proposal for Defending Against Vampire Attack in WSN", Fifth International conferenceon Communication Systems and Network Technologies