



A New Approach for Defending Against Vampire Attack in Wireless Sensor Networks

V. V. S. S. Balaram*

Professor and HOD, Department of IT, SNIST, Hyderabad,
Teangana, India

Abstract— *Wireless Sensor Network (WSN) is a communication network across the sensors nodes. Sensor nodes collect information about the physical environment. Main issue in WSN is wastage of energy at each sensor nodes. Energy is the one of the most important factor while considering sensor nodes. So WSN require a solution for conserving energy level of each sensor node. There are many attacks possible on WSN for energy draining at each sensor node. One of the new type of attack called vampire attack which drains energy of a node and occurs at network layer. It leads to resource depletion (energy) at each sensor nodes, by reducing the battery power of any node. There are two main types of vampire attack namely, carousel and stretch attack due to which sensor node losses its energy and overall network lifetime reduces. Here we propose a method to mitigate vampire attack. This method focuses on to detect and prevent the vampire attacks. The proposed method is used to prevent the draining of life from network nodes. So that, the problem of vampire attack can be reduced to major extent.*

Keywords— *Wireless Sensor Network, Vampire Attack, Energy Consumption, Carousel and Stretch.*

I. INTRODUCTION

The word ad hoc is from Latin and means “for this (only)”. In the case of computer networks, the ad hoc networks mean wireless network without infrastructure, they can be called spontaneous network. It is useful when infrastructure is not available, impractical [1].

A wireless ad hoc network is a decentralized network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired network or access points in wireless networks. Instead each node participate in routing by forwarding data for other nodes, and so the determination of which nodes forward the data is done dynamically, based on the network connectivity[2].

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 [3].

Vampire attacks are not protocol-specific; it can affect the routing protocols classes as link-state, distance vector and source routing. The large amount of data can be affected by this attack, but further try to transmit a little data for more battery life in the network and the rate limiting solution can prevent. Since Vampire uses the protocol-trouble messages, these types of attacks are very difficult to detect and prevent from their attack [4].

In this paper, we aim to provide a mechanism which is used to detect the vampire attack in WSN. Rest of the paper is organized as follows. Section 2 discusses the recent work carried out followed by problem statement in Section 3. Section 4 presents our proposed scheme in detail. With conclusions in section 6 follows references at the end.

II. BACKGROUND THEORY

A. Vampire Attack

There are two types of attacks in WSN, the routing depletion and resource depletion attack. The routing depletion attacks usually only affect the routing path and the resource depletion attacks are the ones that attack the network features like bandwidth, power, and energy consumption. These attacks are commonly called as “Vampire attacks”. They are called so because they drain the battery power from the nodes. These are a type of Denial of Service since they affect the entire system from performing. They are difficult to be detected since they are protocol compliant and are orthogonal to them. They are not protocol specific. They do not affect a single node they take their time attack one by one and disrupt the entire system. Vampire attacks can be defined as the composition and transmission of a message that cause more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. The strength of the attack is measured by the ratio of network energy used in the benign case to the energy used in the malicious case. Safety from Vampire attacks implies that this ratio is 1.

- If there is a subnet (a collection of nodes that are identified by a common network prefix) that does not use AODV as its routing protocol and wants to be able to exchange information with an AODV network, one of the nodes of the subnet can be selected as their “network leader”. The network leader is the only node of the subnet that sends forwards and processes AODV routing messages. In every RREP that the leader issues, it sets the prefix size of the subnet [7].

III. RELATED WORK

2014, Eugene y. vasserman and Nicholas hopper exposed the Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. PLGP protocol is used to prevent the vampire attacks. It consists of two phases for forwarding the packets in a tree structure such as topology discovery phase and packet forwarding phase. To securely transmit the data, the path tracking technique is used in PLGP. Security is one of the critical issues in networks. To overcome these issues, No-Backtracking property scheme is proposed to achieve high efficiency and secure authentication .But PLGP does not satisfy the no-backtracking property. So this paper provides the PLGPa method which satisfies the no-backtracking property [8].

In 2014, K.Vanitha, V.Dhivya described A Valuable Secure Protocol to Prevent Vampire Attacks in Wireless Ad Hoc Sensor Networks. The Valuable Secure Routing Protocol (VSP) is proposed to prevent vampire attacks. It is compressed of three phases such as network configuration phase, key management and communication phase. The key management phase is used for cryptography to protect the node and data. Elliptic Curve Cryptography (ECC) approach is based on the algebraic structure which is used to achieve the security with smaller key size and minimize the number of calculation in a group. PLGP protocol is used to perform the backtracking method in communication phase [9].

In 2014, Damodhar and Umakant described the resource consumption attacks in wireless ad hoc sensor networks. The Energy Weighted Monitoring Algorithm is proposed for providing the security in network. Two phases are initialized in EWMA for consuming the nodes energy. Network configuration phase establishes an optimal routing path from source to destination and achieved multi hop load balanced network. Communication phase avoids the same data packets and aggregated the data transmission. Simulation results proved that the proposed scheme performs well [10]

In 2014, José Anand and Sivachandar presented the vampire attacks detection in wireless sensor networks. The effect of vampire attacks on AODV is proposed for providing the security. The vampire attacks have the ability to disrupt the AODV protocol. Randomly selected malicious AODV agents are evaluated. Initial energy and final energy are used to calculate the energy level in the networks. The results proved that the proposed scheme increased the network energy during the forwarding phase [11].

IV. PROPOSED WORK

We proposed an approach for detecting and preventing vampire attack for AODV routing protocol in WSN.

A. Flowchart of proposed method

Fig,3. Describes about the proposed system architecture.

B. Implementation steps of proposed method

1. Each node maintains its routing table which contains two fields such as Node_ID, Energy level of the node.
2. Now each node exchanges its energy by hello packet. Now the node establish the routing path, first the traces the next node by computing the threshold energy.
3. The threshold energy is calculated by using following formula:

$$\text{Th}(E) = \frac{\text{EN}(1)+\text{EN}(2)+\dots+\text{EN}(n)}{\text{No of nodes in the range}}$$

Where, EN (i) is the Energy level of node i Th (E) is the Threshold level

4. Now the forwarding node check
 - (A) if $\text{EN} > \text{Th}(E)$ then
Take it as next node and send the packet to that node.
 - (B) if $\text{EN} < \text{Th}(E)$ then
if $\text{Th}(E) - \text{EN} > 0.3$ then
Forwarding node to broadcast the RREQ Message in order to repair or find other Route to the destination.
5. Based on this idea, the AODV protocol uses three types of packets for communication via RREQ (Route Request), RREP (Route Reply), and RERR (Route Error).
6. We also used three more packets R_R (Route Repairing), RR_OK (Route Repair OK), and RR_F (Route Repair Failure).

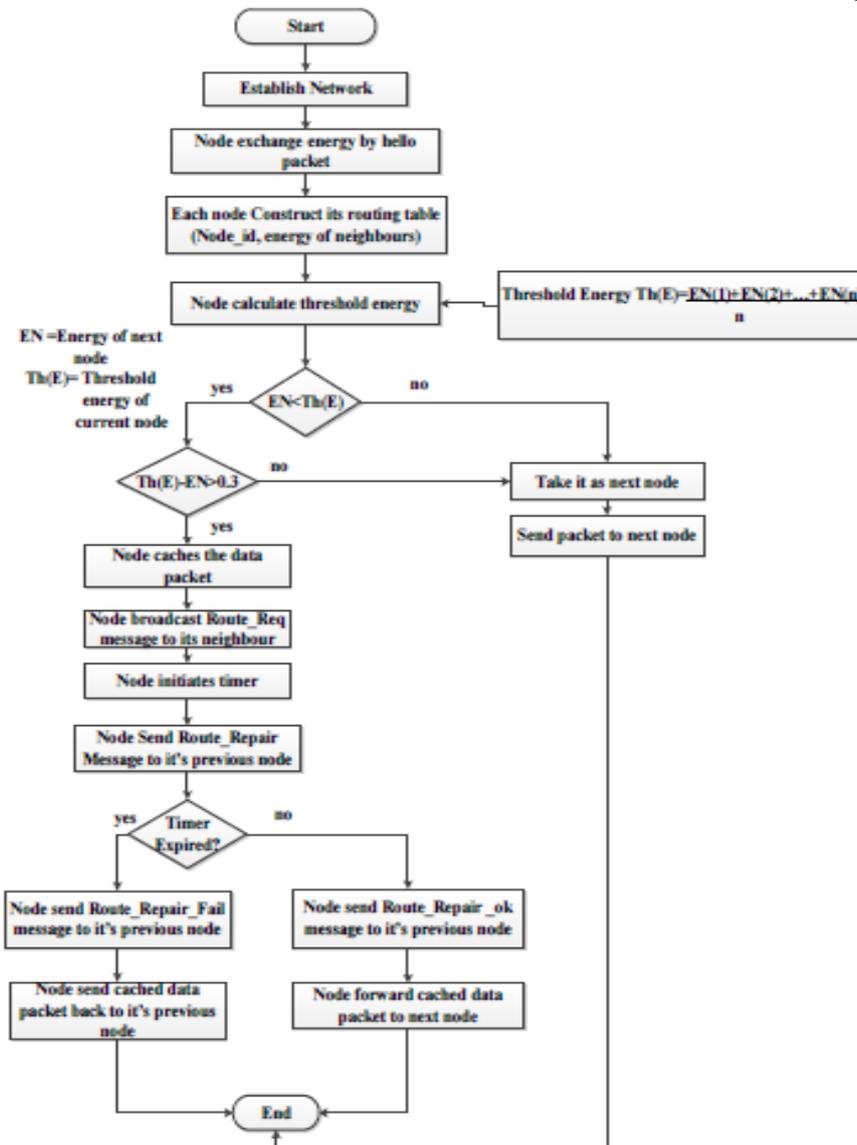


Fig. 3 Proposed System Architecture

- If the data is goes from S to D via nodes A, B, C and the intermediate node B detect that the link is break, then B sends a Route Repairing (R_R) message back to the Pre-hop node A. After sending the Route Repairing (R_R) message to A, B broadcast the RREQ to repair the break route.

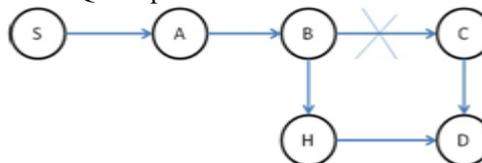


Fig.4. Depicting route invalidation

- If B cannot repair the route in certain amount of time, B sends back a Route Repair Fail (RR_F) message to A also B sends the data packages back to A which store in the cache, back to A. If B repairs the route in time, it sends back a Route Repair OK (RR_OK) message to A.

Once the node A receives a R_R (Route Repairing) message, it caches the data packages sent to the destination. If A which is not the source node of the data has received a RR_F (Route Repair Failure) message from the break node, A sends a R_R(Route Repairing) message back to the Pre-hop of itself and continues the same procedure. On the contrary, if node A receives a RR_OK(Route Repair OK) message which means the break link is repaired by B, it sends all waiting data packages stored in the cache.

V. CONCLUSION

In this paper, we define the vampire attacks, which are the resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes' battery power. The main contribution of this

paper is energy draining of nodes in WSN can be defended against vampire attack and network lifetime can be maximized. Through proposed method we are able to detect the vampire attack which occurs in the network and which reduces the energy level in WSN. In future work, we are going to implement proposed method for AODV routing protocol in Network Simulator 2.

REFERENCES

- [1] Nieminen, Klaus. "Introduction to ad hoc networking." Networking Laboratory, Helsinki University of Technology (2003).
- [2] Praveen Kumar P, " Mobile Ad Hoc Networks".
- [3] Al-Karaki, Jamal N, and Ahmed E.Kamal, " Routing techniques in wireless sensor networks: a survey," Wireless communications, IEEE 11.6 (2004)
- [4] Vidya.M, and Reshmi.S, "Alleviating Energy Depletion Attacks in Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-4, April 2014.
- [5] Farzana TI, and Mrs.Aswathy Babu, " A light weight PLGP based method for mitigating vampire attacks in Wireless Sensor Networks," International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 03 Issue 07 July, 2014 Page No. 6888-6895
- [6] P.Rajipriyadharshini,andV.Venkatakrishnan,S.Suganya,andA .Masanam," Vampire Attacks Deploying Resources inWireless Sensor Networks," (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2951-2953 ISSN:0975-9646
- [7] Tawseef Ahmad Naqishbandi and Imthyaz Sheriff C, " A Resilient Strategy against Energy Attacks in Ad-Hoc WSN and Future IoT," International Journal of Advanced Research inComputer Science and Software Engineering Volume 4, Issue 2, February 2014 ISSN: 2277 128X
- [8] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Network," Ieee Transactions On Mobile Computing, Vol. 12, No. 2, February 2013
- [9] K.Vanitha, and V.Dhivya, "A Valuable Secure Protocol to Prevent Vampire Attacks in Wireless Ad Hoc Sensor Networks," International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14)
- [10] B. Umakant, and J. Damodhar, "Resource Consumption Attacks in Wireless Ad Hoc Sensor Networks," International Journal of Engineering Research ISSN: 2319- 6890(online),2347- 5013(print) Volume No.3 Issue No:Special 2, pp: 107-111 22 March 2014
- [11] Jose Anand, and K. Sivachandar, " Vampire Attack Detection in Wireless Sensor Network," International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, July 2014, ISSN: 2319-5967 (2014)