**A Brief Survey on Vampire Attack in**

**Wireless Sensor Network**

Yesha A. Patel

*Department of Computer Engineering*

*SVM Institute of technology*

*Bharuch 392-001, Gujarat, India*

yesha.patel30@yahoo.com

Nital H. Mistry

*Department of Computer Engineering*

*SVM Institute of technology*

*Bharuch 392-001, Gujarat, India*

misnit\_22@yahoo.com

***Abstract*— Wireless Sensor Network (WSN) is a collection of independent sensor nodes which are basically used to monitor environmental conditions. But those wireless networks suffer from lots of security threats. The proposal considers another class of resource utilization attacks which is characterized as Vampire attack. A vampire attack is caused by the malicious node on the decentralized wireless network. Vampire attacks are not protocol specific rather uses its compliant message. As it uses protocol complaint messages to build an attack which makes them difficult to detect and prevent. Vampire attacks cause more energy consumption while transmitting the message which for all time cripples the entire network by rapidly depleting battery of nodes. Wireless Sensor Networks have been applied to different fields which need to make and recognize answers for counteractive action of the network from these attacks. In this paper, we aim to study and analyze the vampire attacks and its effects in WSN. This paper explores the survey on vampire attacks, which forever impair networks by rapidly depleting nodes' battery power.**

***Keywords— Vampire Attacks; PLGP; Wireless Sensor Networks (WSN)***

# Introduction

The issue of trust point in Wireless Sensor Networks (WSNs) has been step by step concentrated by current research. Research on security in WSNs has likewise advanced, showing cryptography mechanisms, intrusion discovery systems, and productive directing protocols [1]. The basic objective of security in Wireless Sensor Networks (WSNs) is to ensure the system against different attacks like an assortment of strategies, eavesdropping, clones of nodes, modification of packets etc. [1]. Constrained battery power and low memory makes sensor networks infeasible to utilize traditional security arrangements. These types of attacks on the networks are classified as routing attacks and data traffic attacks [2].Attacker can easily inject malicious packets in wireless medium. The biggest challenge of wireless sensor network is to develop the energy-efficient routing protocol that consumes low energy [3].

The rest of Paper is organized as follow: In section II basic introduction to vampire attack is discussed. In section III related works on various methods or techniques to detect and prevent the vampire attack is mentioned and in final section paper is concluded.

# PSO in Localization

The battery power utilization attacks that attack directly on routing layer protocol to crash the network and to consume the node's battery force are called as vampire attacks [3]. Vampire attacks are not relay on particular protocol, in that they don't depend on outline properties of specific routing protocols, yet rather endeavor general properties of protocol classes [4]. These attacks do not harm the network by flooding the system with a lot of information, but instead attempt to transmit the information with the goal of high energy drain in the network [4]. Vampires use protocol complaint messages to build the attack so detection and prevention of these types of attacks is difficult. The ratio of energy usage in ideal case to the energy usage in malicious case is measured as the strength of the attack [5].

Vampire attacks are characterized mainly in two types: Carousel attack and Stretch attack.

* Carousel attack: In this type, a malicious node sends a packet with a route which is having a series of loops, such that the same node shows up in the route more than one time [6].
* Stretch attack: In this type, a malicious node develops fake long route for the packets to reach the destination which navigate the packets to bigger than ideal number of nodes. It causes a node which is not belonging to the optimal path of the packet [6].

A complete detection and prevention of these types of attacks is very difficult but by using some security mechanism harm of the attack can be reduced.

# Related Work

Vasserman *et al.* [4] defined Vampire attacks in Wireless Ad Hoc Sensor Networks. Vampire attacks do not harm or distract the existing path rather it uses protocol complaint messages to harm the Network. Observation of security measures and vulnerabilities of the existing protocols to the vampire attack are described. In the experimental results taken in NS-2, authors take single vampire against different protocols like link-state, distance-vector, source routing etc. and modify the existing protocol to improve the security of packet forwarding task. Proposed method called PLGPa can defense against the attack during some packet-forwarding phase. It is the first sensor routing protocol which can continuously keep track of the forwarding packets towards their destination nodes.

Bhutada *et al.* [7] defined the vampire attack and its effects how it uses the node’s battery power. Authors proposed a system which is used to generate the secure path by using PLGP protocol and transfer the data through path of the topology. Proposed system performed mainly four different tasks which are generation of secured path for data transfer, Key management, identifying the attacked node and path tracking technique. Generation of secured path can be done through the clean – state sensor network routing protocol/ PLGP protocol because Vampire attack cannot catch the data transfer process if it is done through it. In key management, elliptic curve cryptography (ECC) is used which is public key cryptography method based on the structure of elliptic curves. Algorithm for finding attacked node is described. It shows that the node from which the data transfer path is distracted is found as attacked node. To avoid the processing of the same packet, proposed system has the function to maintain the log files which contains the source-destination address and packet id. Simulation Results shows that the energy gap between honest node and attacked is very large. And if the protocol is used in the simulation process than it is proven that the result of PLGP is better than BVR (Beacon Vector Routing) protocol.

Deshmukh *et al.* [8] proposed a new protocol PLGP with attestations (PLGPa) which is stated that route history of every PLGP node is must which is used by PLGPa. It uses the tree structure of the PLGP by which every node can proceed towards its destination without any intrusion on the route. PLGPa satisfied the no-bracketing property. Every transmitted node has to approve the attestation chain to verify that the packet is not transferred far away from the destination node. Attacker can modify the fields so that it can only change or alter the attestation field. Authors perform the simulation on different attacks to show the effect of proposed system. And by the result it is shown that PLGPa gives best performance in Carousel attack.

Mariyappan *et al.* [9] presents sensor network encryption protocol to maintain network availability. It uses boundary recognition technique to prevent vampire attack in Ad Hoc Network. In proposed system, four main parts are there 1. Sensor Network Encryption Protocol (SNEP) 2. Boundary Recognition Algorithm 3. Jump Point Algorithm 4. Recursive Grouping Algorithm. It keeps track of the routing table of network address for each node. It merges the recursive grouping algorithm which confirms that each node in the network has unique network address and routing tables. An accurate and shortest path is produced without going through the nodes in less than 3 seconds by using jump point algorithm. This accurate path is used to reduce the harm of the vampire attack and save the battery power of the nodes during packet forwarding phase. For a large number of nodes Boundary Recognition Technique is used to find boundary nodes by using connectivity information. SNEP is providing security and provides authentication between base station and the participated nodes.

Abirami *et al.* [10] described Interior Gateway Routing Protocol (IGRP) and proposed defenses against some forwarding-phase attacks. IGRP is a Cisco-proprietary Distance-Vector protocol which is more scalable than Routing Information Protocol (RIP). By using IGRP limitation of PLGP can be solved. In PLGP, packets don’t know which path is ideal and which one is malicious or they even have the rights to take the decision about choosing the path. In IGRP, as it is a distance vector routing protocol each packet has its routing table which is updated at regular interval. So at some extend packets can take decision about their path discovery. IGRP chooses the best path on the bases of speed of link, packet size, loading and reliability. It prevents the vampire attack by not allowing the attacked packet in to forwarding path. It can calculate the distance from all the destination nodes and preferable for large networks. In proposed system, authors uses the IGRP for detecting the attack then encryption or decryption algorithm is used to verify the attacked file. Experiments are performed in JAVA which shows that the stretch attack is more difficult to detect and prevent.

Ghate *et al.* [11] proposed Group Key Authentication Algorithm which is used to prevent the vampire attacks in wireless sensor network. There are main three phases in this algorithm. First Phase is Pre-Deployment Key Distribution phase in which network is divided in groups having their own group-id. Each node in the network have assigned their own public and private keys, their group’s public and private keys and other group’s public and private keys by using Elliptic Curve Cryptography (ECC) . Another phase is Network Discovery phase in which every node in the network has perform an important task to find their neighbor in the network by sending merge request to all nodes in the network. Last phase of this algorithm is Packet forwarding phase in which the path is discovered and the packets are sent from source to destination. Authors perform the simulation using JAVA Jung tool in which 10 to 50 nodes network is created. Proposed system have the process of too many key exchanges so as the number of nodes increases the time required for key exchange also increase.

Deshmukh *et al.* [12] Authors proposed defenses against some of the forwarding-phase attacks and described PLGPa. It satisfied No-backtracking property in which the packet is consistently makes progress toward its destination in the logical network address space and it is used to vampire resists. In proposed System every packet traverses the same number of hops whether an adversary is present in the network or not. PLGP Packets are forwarded from the shortest route and does not satisfy No-backtracking property. Every packet in the network has the path history which is used by PLGPa so that every packet can significantly traverse through at least one ideal node in the path. It uses the signature system to authenticate a node to its routing path through which it will take care of the packet’s routing history. It uses one-way signature chain construction to prevent truncation. It never floods and it is the most equitable routing load distribution and path diversity technique.

Reddy *et al.* [13] proposed system a system in which authors change the existing routing protocols to limit the effect of vampire attacks in packet forwarding phase. First they found the vulnerabilities of existing protocols which are energy consumption, loss the information, lost productivity, various DOS attacks, security level etc. Existing protocols concentrate on secure path for packet forwarding but vampire attack will not delete or alter the existing path it only build a vampire in the network. Instead it uses valid path of the network and use protocol complaint message. Simulation is performed on different protocols in the presence of a single vampire. There are three modules such as data verification, denial of service and user module. Data verification module verifies the path by which it can have the knowledge about whether the packet is from malicious node or from honest node. DOS module is used to attempt network resource unavailable from its authenticated user. Purpose of user module is to lock the path by suggesting a wrong path.

Manimala et al. [14] define EWMA the first sensor network routing protocol which limits the damage from vampire attacks by verifying the packets towards the destination. It is used against vampire attack by verifying that if the packets are continuously moved towards their destination node or not. There are mainly two phases in proposed system one is Network configuring phase and other is Communication phase. In first phase path for the packets from source to destination is established. The main functions are load balancing of the nodes and maximum try to minimize the energy consumption for data communication. First it calculates the energy required to transmit the data packet and the shortest distance node from the source node. By these two criteria it will choose the routing path that consumes less energy. Load balancing is the most important task of this algorithm and it is balanced upon the capacity of the nodes. Simulations are performed on the network made from 20 nodes in FEDORA 10 and use NS2 for coding and result graph. It shows that the energy consumption is totally based on the location of the malicious node.

Mahajan *et al.* [15] introduce a method by which the detection and security level against vampire attack is increased. It is a routing protocol which is used to verify that if the packets are continuously move towards their destination node or not and limit the damage of vampire attack. It is a combination of positives of two independent routing protocols one is DSDV (destination-sequenced distance vector routing) routing algorithm and other is DSR algorithm. Proposed system is used to use the bandwidth in such a way that it can scale the large number of nodes without changing the topology. It takes the on demand approach of DSR so that the route of packet cannot be fix rather when the node needs to send packets it will allocated a route to its destination. So the energy of the network can be saved by not being alive all the time. Packet can be travel node to node by having their own routing table and it updates its routing information when it is needed. Proposed system uses this feature from DSDV. For route discovery it uses RREQ-route request, to send as a reply to the RREQ it uses RREP-route reply and for an error unreachable node it uses RERR-route error. It can save the routing overheads and also have the strength to change the network dynamics because it uses the on-demand routing scheme.

# conclusion

A new form of attacks called vampire attack which consumes the battery life and energy from the nodes in the network is discussed. Vampire attacks are characterized in two types one is carousel attack and other is stretch attack. There are different protocols where the vampire attack can be identified during the topology discover phase and packet forwarding phase. It is difficult to detect the vampires in the network though it uses protocol complaint messages to build an attack. Vampire attack is not protocol specific so one cannot predict its presents in the network. In this paper, techniques by which the network can resist vampires are discussed.

##### REFERENCES

[1] Yu, Yanli, et al. "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures." *Journal of Network and Computer Applications*35.3 (2012): 867-880.

[2] Patel, Manish M., and Akshai Aggarwal. "Security attacks in wireless sensor networks: A survey." *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*. IEEE, 2013.

[3] Vanitha, K., and V. Dhivya. "A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks."

[4] Vasserman, Eugene Y., and Nicholas Hopper. "Vampire attacks: draining life from wireless ad hoc sensor networks." *Mobile Computing, IEEE Transactions on* 12.2 (2013): 318-332.

[5] Arjunkar, Mrunal R., A. S. Sambare, and S. R. Jain. "A Survey On: Detection & Prevention of Energy Draining Attacks (Vampire Attacks)." *International Journal Of Computer Science And Applications* 8.1 (2015).

[6] Chumble, Mr Shrikant C., and M. M. Ghonge. "Mitigation of Vampire Attack in Wireless Ad-hoc Sensor Network."

[7] Bhutada, Sunil, K. Kranthi Kumar, and K. Manisha. "A novel approach for secure routing protocol: To improve life of network." *Contemporary Computing and Informatics (IC3I), 2014 International Conference on*. IEEE, 2014.

[8] Deshmukh, Lina R., and A. D. Potgantwar. "Ensuring an early recognition and avoidance of the vampire attacks in WSN using routing loops." *Advance Computing Conference (IACC), 2015 IEEE International*. IEEE, 2015.

[9] Mariyappan, E., and C. Balakrishnan. "Power draining prevention in Ad-Hoc Sensor networks using sensor network encryption protocol." *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014.

[10] Abirami, R., and G. Premalatha. "Depletion of vampire attacks in medium access control level using interior gateway routing protocol." *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014.

[11] Ghate, Shweta, Vivek Deshpande, and Anil Hiwale. "Group Key Authentication against Vampire Attacks in WSN."

[12] Deshmukh, Lina R., and Amol D. Potgantwar. "Prevention of vampire attacks in WSN using Routing Loop." *proceedings of IRF International conference, 5th& 6th Feb*. 2014.

[13] Reddy, K. Shyam Sundar, and GS Prasada Reddy. "Securing Data Packets from Vampire Attacks in Wireless Ad-hoc Sensor Network."

[14] Manimala, S., and A. Taskala Devapriya. "Detection of Vampre Attack Using EWMA in Wireless Ad Hoc Sensor Networks." *IJISET-International Journal of Innovative Science, Engineering & Technology* 1.3 (2014).

[15] Mahajan, Snehal, et al. "Counter vampire attacks in wireless ad-hoc sensor networks by using AODV."