WWJMRD 2017; 3(12): 73-75
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Avtar Singh
M.Tech (C.E)-Student
Yadawindra College of Engineering and Technology, Talwandi Sabo, Punjab, India

Correspondence:
Avtar Singh
M.Tech (C.E)-Student
Yadawindra College of Engineering and Technology, Talwandi Sabo, Punjab, India

A Review on Techniques to handle Vampire Attacks

Avtar Singh

Abstract
WSN is wireless sensor network consists of various wireless nodes. Each node is communicating to its environment and collects the data from its environment and sends that to the base station. This base station is a sink node which can be moving or stationary nodes. Each sensor node will be distributed into the area randomly, later on they will be localized in the area. while each node sends the collected data to the sink node. While doing it, identify the route from source to the destination. In this type of network there can various types of attacks. These attacks will destroy the network performance. Vampire attack is again such king of attack deteriorate the performances of the network. There lie various techniques which can control the vampire attack. In current review it is studied that which technique has which type of constraints.

Keywords: Vampire, WSN, Sink, Mobile Sink

1. Introduction
Wireless sensor network consists of various mobile or stationary nodes. These sensor nodes are put into the network area randomly. These sensor nodes basic purposes are to sense the data or collect the data for which they are stationed. These sensor nodes are to send this collected data to the sink node. Sink node collect the data and process the data for later analysis. This type of network is highly prevalent in today's wireless world. Large number of applications stands for this type of network. Source sensor node identifies the path to the sink node by sending the route request. Against the route request various route replies will be received. Out of multiple route replies one route reply will be selected based on number of hops. So that sensor node can arrive at the destination through the shortest path. The utilization of sensor systems is perpetual, constrained just by the human creative ability. Remote sensor systems have turned into a developing territory of innovative work because of the enormous number of uses that can extraordinarily profit by such frameworks and has prompted the advancement of small, shabby, expendable and independent battery controlled PCs, known as sensor nodes or "motes", which can acknowledge contribution from an appended sensor, process this information and transmit the outcomes remotely to the travel organize.

1.2 Attacks in WSN
Some general attacks that are faced in WSN are:

1. Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

2. Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, ―tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

3. Replay Attack: Here, an attacker retransmits the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

4. Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

5. Routing Attacks: The malicious node makes routing services a target in light of the fact that it is a critical service in MANETs. There are two flavors to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The leading is pointed at obstructing the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

6. Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

7. Impersonation: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

1.3 Vampire Attacks: The vampire attack is the resource depletion attacks because that attack the network features like power, bandwidth, and energy consumption and the routing depletion attacks usually only affect the routing path. These attacks are known as "Vampire attacks" because they drain the battery power from the nodes. 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 transmission and composition of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination. 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. Mainly there are two types of vampire attacks, carousel attack and stretch attack.

Related Work

Amee A. Patel *et. al.* [5] Wireless sensor network is the network works for smaller area. Each sensor node part of the network communicates to the sink node through intermediate node. Various kinds of attacks are expected while communication. In current paper they have studied the vampire attack. This type of attacker node deplete the energy and other resource. This paper has identified the vampire attack using threshold energy based technique.

Eugene y. vasserman *et. al.* [2] this paper has studied different type of attacks. And later on focused on to the vampire attack. They have used the technique called as PLGP. This technique is based on backtracking.

Damodhar *et. al.* [8] this paper again has worked on the vampire attack. They have used the technique based on Energy Weighted Monitoring Algorithm. This paper has used to identify the shortest or least hop count path. so that vampire can be identified. As it route the packet on to the longest path.

M. Vidya et al. [11] (2014) described the resource consumption attacks and its types. System survivability is the limit of a system keeping connected under loss and interruptions, which is a major worry to the design and design interpretation of wireless sensor networks.

Ching-Tsung Hsueh *et. al.*[7] this paper is focused on to the secure and reliable communication. It includes the path that has least number of intermediate node and also there will be least probability from any kind of attacks. It is the network having larger reliable communication which has less number of attacker nodes.

Deshmukh, L.R. *et. al.* [9] this paper is focused on to DO type of attack. They used energy threshold based technique. It is the best technique for identify those node which has highest depleted energy and which participate in every communication.

Different Technique for Identification of Vampire Attack

Author	Paper name	Technique	Constraints
Eugene Y. Vasserman	Vampire attacks: Draining life from wireless ad-hoc sensor networks	This paper has used energy Threshold based technique.	But the energy thresholding can be bypassed by other various kinds of attack.
V.subha	Defending against vampire attacks in wireless sensor networks	They have proposed new protocol called vsp, a valuable and secure protocol is proposed along with the key management protocol to avoid this vampire attack	Energy depletion will be more and life time will be less if key of higher size will be used.
Eugene Y. Vasserman	Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks	This paper has applied the technique called as complexity reduction technique. When more complexity is involved then attack probability will be more	This paper has not considered the threshold for complexity. So sometimes fail to get.
Kahina CHELLI	Security Issues in Wireless Sensor Networks: Attacks and Countermeasures	This paper has put the study for different kinds of attacks and there counter measures	They have not considered vampire resource depletion type of attack.

Conclusion

WSN is the network having fewer infrastructures in terms of any central controller. This type of network is highly vulnerable to various kinds of attack. Any communication can be destroyed by the malicious node such that there will be high amount of resource depletion. Various researcher has applied there algorithms to avoid these malicious nodes specially vampire attack. This attack directly attacks the resource depletion. Various techniques for vampire attack handling have been studied. Such that no information should be destroyed. Each technique has its own advantages and simulteously carries constraints. In current

review it is clear that protection from vampire attack is hard to attain.

References

1. Subha and P. Selvi, “Defending Against Vampire Attacks,” Int. J. Comput. Sci. Mob. Comput., vol. 3, no. 11, pp. 668–679, 2014.
2. E. Y. Vasserman and N. Hopper, “Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks,” IEEE Trans. Mob. Comput., vol. 12, no. 2, pp. 318–332, 2013
3. G. Padmavathi and D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” Int. J. Comput. Sci. Inf. Secur., vol. 4, no. 1, 2009.
4. A. A. Patel and S. J. Soni, “A Novel Proposal for Defending Against Vampire Attack in WSN,” 5th Int. Conf. Comun. Sys. Net. Technol., pp. 624–627, 2015.
5. C. P. Goudar and S. S. Kulkarni, “Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks,” Int. J. Emerg. Res. Manag. &Technology, vol. 4, no. 6, pp. 263–269, 2015.
6. T. Farzana and A. Babu, “A Light Weight PLGP Based Method for Mitigating Vampire Attacks in Wireless Sensor Networks,” Int. J. Eng. Comput. Sci., vol. 03, no. 07, pp. 6888–6895, 2014.
7. C. T. Hsueh, C. Y. Wen, and Y. C. Ouyang, “A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks,” IEEE Sens. J., vol. 15, no. 6, pp. 3590–3602, 2015.
8. B. Umakanth and J. Damodhar, “Detection of Energy Draining Attack Using EWMA in Wireless Ad Hoc Sensor Networks,” Int. J. Eng. Trends Technol., vol. 4, no. 8, pp. 3691–3695, 2013.
9. L. R. Deshmukh and A. Potgantwar, “Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops,” Int. J. Eng. Comput. Sci., pp. 61–66, 2015.
10. J. Anand and K. Sivachandar, “Vampire Attack Detection in Wireless Sensor Network,” Int. J. Eng. Sci. Innov. Technol., vol. 3, no. 4, pp. 639–644, 2014.
11. M. Vidya and S. Reshmi, “A Survey on Energy Depletion Attacks in Wireless Sensor Networks,” Int. J. Eng. Adv. Technol., vol. 3, no. 4, pp. 89–91, 2014.
12. A. R. Qureshi and R. K. Krishna, “Enhancing Energy Efficiency by Detecting and Protecting from Vampire Attack in Wireless Sensor Networks,” Int. J. Innov. Res. Adv. Eng., vol. 2, no. 5, pp. 95–97, 2015.