# Detection and Removal of Vampire Attack in Wireless Sensor Network

Manish Soni
M. Tech Scholar
Sanghavi Innovative Academy
Indore

Bharat Pahadiya
Asst. Professor
Sanghavi Innovative Academy
Indore

## ABSTRACT
Wireless sensor network is communication network across low cost, low energy sensor node which sense and collects information around physical environment. Sensing and pervasive computing features of WSN opened up various applications which in turn increased research areas. WSN has been implemented with various areas such as in military, forest, health, inventory etc. Energy is an important factor for sensor node, while there is one new type of attack called vampire attack has been discovered which disables network by consuming battery life of sensor network. The proposed work introduces a new methodology based on energy threshold and packet broadcast threshold of sensor node of network. Solution in previous work was limited to packet forwarding phase only but not work with topology change. The proposed solution is simple and also works with topology change in network.

## General Terms
Dynamic vampire attack detection, Security in wireless sensor network.

## Keywords
Vampire attack, wireless sensor network, DOS, Variance, Security

## 1. INTRODUCTION
Due to recent technical advancement, the production of small size and low price sensors became technically and economically feasible. A Wireless Sensor Network (WSN) constructed of large number of these sensor nodes may be in hundreds or thousands. These sensor nodes can transfer information to each other inside network or directly to an outer base-station node. The more sensor nodes make network to sense over more physical areas with higher degree of accuracy. Sensor nodes communicate sensed data to each other and form high-quality useful information about the surrounding environment. Each sensor node bases its decisions on its goal, currently gathered information, and its proficiency of its computation, transmission, and energy assets. 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.

### 1.1 Applications of WSN
Sensor nodes can be used for continuous stable sensing, event recognition, region sensing, and local control of actuators (Akyildiz et al., [1]). Wireless infrastructure and micro-sensing capability of sensor network opens up many new application areas. Wireless sensor networks can be an integral part of military communications, computations, reconnaissance, surveillance, reconnaissance and targeting systems. There are also various applications for environmental phenomena including trailing the movements of animals, birds and insects, Forest fire detection, Bio complexity mapping of the environment and Flood detection. Some of the health applications for sensor networks are providing interfaces for the debilitated, homogenized patient monitoring; drug administration in hospitals; the economic applications are monitoring material strength; building virtual keyboards; managing inventory; monitoring product quality; constructing smart office spaces. There is vast scope for application of wireless sensors network which may be considered endless, limited only by the human imagination.

### 1.2 Routing Protocols in WSN
Generally routing protocols in WSN can be categorized into three categories based on network structure flat-based routing, hierarchical routing and location based routing (Jamal N. Et al., [2]).In Flat-based routing all network nodes poses similar functionalities and equal roles while in hierarchical –based routing node plays different roles assigned to them. In case of location-based routing positions of sensor nodes are exploited for routing data in the network. A routing protocol is said to be adaptive if some of the network parameters can be changed in order to adjust with the present network state and energy capacity of network nodes. Moreover, these protocols can also be classified on the basis of protocol operation namely query-oriented, Multipath-oriented, negotiation-based, QoS-based routing techniques. Protocols can also be classified on the basis of route discovery process from source to destination which are named reactive, proactive and hybrid routing. In reactive protocol on demand route discovery method is used i.e. route is derived just before sending of message, while in proactive routing route are pre-discovered irrespective to time of sending message. Hybrid protocols consist of these two strategies. In case of static nodes, it is preferable to have table driven routing protocols rather than using reactive protocols. In case of reactive protocols, process of route discovery and path setup consumes some amount of energy. One more type of routing protocols has been noticed namely cooperative routing protocol. In cooperative routing, there is one central node where all the data is aggregated from all other network nodes and then that data is further processed, and reduces route cost in terms of energy usage. Many other protocols depend on position and timing information.

### 1.3 Routing Challenges and Designing Issues in WSN
Despite the numerous applications of WSNs, There are several limitations of this network such as lesser energy of

nodes, lesser computing power and shorter bandwidth of wireless interconnection among nodes. The design of routing protocols in WSNs is affected by many crucial aspects. These aspects must be reduced before effective information transfer can be achieved in WSNs. below; we outline some of the routing difficulties and design issues that degrade routing process in WSNs (Jamal N. Et al., [2]).

### *1.3.1 Node Deployment*
Node deployment is dependent on application and plays important role in routing protocol performance. The deployment is divided into two types, deterministic and randomized. In prior case, sensor nodes are positioned manually and the route, through which data flows is pre-discovered, while in later case, sensor nodes are dispersed randomly which create ad-hoc manner structure. For energy efficient operations optimal clustering is required, which depends on uniform distribution of nodes.

### *1.3.2 Limited Energy Capacity*
Sensor nodes in WSN are powered by battery, so that limited by energy capacity. When energy of sensor will cross a threshold level, it will not be possible for sensor to function properly which in turn causes network performance degradation.

### *1.3.3 Heterogeneity of Node/Link*
In many cases, sensor nodes are homogeneous, which means having similar features such as equal battery life, commutation power etc. ,while for some specific applications, it is required for the nodes to have different functionality and capacity. In case of heterogeneous sensors there may be problems while routing data in network.

### *1.3.4 Fault Tolerance*
Sensors WSN must be fault tolerant against node failure may be due to battery exhaustion or environmental conditions or any physical damage. If some nodes fail, MAC and routing protocol must be able to form new links to carry data up to base station.

### *1.3.5 Scalability*
There may be very larger number of sensor nodes required to sense larger geographical area. Routing protocol must have capability to work with very larger number of nodes. Furthermore routing must have such scalability so that it can react against any event in the network.

### *1.3.6 Network Dynamics*
A sensor network usually operates in a dynamic and unreliable environment. There is frequent change in sensors network topology because of node failure new nodes are deleted and added dynamically. Furthermore wireless medium for node connectivity causes noise, errors and also it is time variant. So that routing protocol must be able to support dynamic topology change to avail connectivity and coverage requirements of particular application.

### *1.3.7 Data Aggregation*
Different sensor nodes may produce similar data, so that aggregation of similar data received from different node reduces further transmission of common data. Various routing protocol uses data aggregation technique for optimization of data transfer and saving energy consumption.

### *1.3.8 Quality of Service*
Some applications have importance of time at which data is received, if data is sensed but not reached within a particular time then it has no importance. Therefore for time-constrained application latency bounded data delivery is mandatory condition.

## 1.4 Security Requirements
The objective of security of WSNs is to provide protection for the information and resources against attacks and misuse (Rajkumar et al., [3]). WSN`s security requirements are.

### *1.4.1 Availability*
Availability ensures that the network nodes remain in stable condition and keep network services available even if attacked by denial-of-service attacks.

### *1.4.2 Authorization*
Authorization put restriction that only authorized nodes, are allowed to be part of network and gather information for network operations.

### *1.4.3 Authentication*
This makes sure that the information transfer from one node to another node is real, that is, a malicious node cannot act as any other network node by capturing its identity.

### *1.4.4 Confidentiality*
Confidentiality imposes security such that a given message cannot be interpreted by any node other than the intended receiver.

### *1.4.5 Integrity*
This ensures that a message sent from one network node to another, is not altered by malicious intermediate nodes.

### *1.4.6 Not Repudiation*
Under this any node that sends a message to any other network node, cannot deny later on that this message has been sent by itself.

### *1.4.7 Freshness*
Freshness of message means that the data is latest and ensures that no intruder can resend previous messages.

# 2. BACKGROUND STUDY
Wireless Sensor Networks are sensitive to various types of attack. They can be categorized in three types, attacks on availability of network, attacks on secrecy and authentication of network, and stealthy attack for service integrity: which makes network to allow false data value to enter in network. In these type attacks, it is important to keep network alive until desired goal of network not completes (Jaydip Sen et al., [4]).

DoS attack may cause real world harm to people`s life by affecting WSN surrounding those people. Usually DoS attack aim to destroy or disrupt a network. However, a DoS attack can be any event that declines or completely destroy capacity of network and makes it unable to conduct desired operations (Wood et al., [5]). There are several standard solutions present in the literature to handle with some type of denial of service attacks, although in overall, developing a common defense solution against DoS attacks is still a big issue. Some of the important attacks are briefed below:

## 2.1 Wormhole
A wormhole is low latency link between two portions of a network over which an attacker replays network messages (Karlof et al., [6]). The attacker receives packets at one part of the network, and tunnels them to another part in the network, where the packets are reinitiated into the network. The tunnel among the two conspiring attackers is known as the wormhole. This link may be generated either by a single node

transferring messages among two adjacent but non-neighboring nodes or by two nodes which are located in two different parts of network and having data transfer using tunnel. Radio channel used in sensors network have a broadcast feature which make attacker enable to create wormhole tunnel even for those data packets which are not addressed to it. Routing in WSN will not be possible until some efficient security methods are applied to protect network against such attacks.

## 2.2 Black and Gray Hole

In this attack, a attacker node falsely claims optimal paths (e.g. the shortest path or the most reliable path) to the targeted node during the route detection, or in the route updates messages. The aim of the malicious node could be to disrupt the route detection process or to capture all data packets being sent from sender to the destination node. A finer form of black hole attack is called as the gray hole attack, where the false node irregularly drops the data packets so that its detection becomes even more difficult.

## 2.3 Flooding

Flooding cause's memory depletion, which is very vulnerable in case where a protocol is used to maintain steady condition at any end of the connection (Wood et al., [5]). An attacker continuously try to make new connection request until the all sensor nodes of network consumes all the resources or crosses their threshold limit. In any case, further true node connection requests will be ignored.

## 2.4 Sinkhole

Sinkhole attack refers to a type of attack in which attacker creates a compromised node and frames routing information such that other neighbor nodes have misconception that it is the best node to route data (Karlof) et al., [6]).In this way selective forwarding becomes so simple as large amount of data transfer is conducted through this node.

## 2.5 Vampire

A new class of resource depletion attack has been discovered which permanently disable network by draining energy of network nodes called "**Vampire Attack**" (Vasserman et al., [7]). Vampire attacks are not affect any specific protocol. Vampire attack causes composition and flooding of messages more similar to that generated by an honest node and drains the battery life from network nodes. Basically vampire attack is a variant of DDOS attack, which performs resources consumption on neighbor nodes. Therefore during the vampire attack targeted packets are modified for preparing long routes or misguiding the packets. In addition of that the malicious nodes are making frequent connectivity from the entire neighbor nodes in network using false control message exchange. Due to these neighbor nodes replies the false request for connectivity and draining energy rapidly. On the other hand the malicious host only change a few information of the packets thus it is difficult to locate on network. Thus detecting such kind of malicious host is a complex issue.

### *2.5.1 Effect on Stateless Protocol*

Vampire attack affects stateless routing protocols such as source routing by either of the two types as follows.

#### *2.5.1.1 Carousel Attack*

In this type of attack, malicious node injects packet with path consisting of series of loops which contains same set of nodes many times so that those nodes drain their energy soon. In this attack strategy ,there may exists more than available network nodes in the constructed path which are only limited by allowed number of nodes in source path. For Example as shown in figure 1 honest route is indicated by solid line and false line is indicated by dashed line.

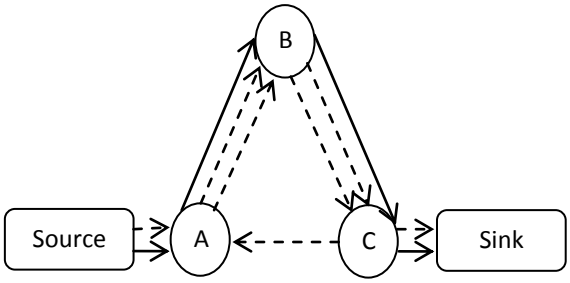


**Fig 1: Example of Carousel Attack**

#### *2.5.1.2 Stretch Attack*

Another Type of vampire attack is called stretched attack, in which advisory node falsely generates larger source path that causes packets to travel more nodes than optimal number of nodes. As shown in figure2, an honest sender of packet selects path source to A, A to sink, while malicious node selects longer root source A B C D to sink, so that it can drain energy of as many nodes as possible.

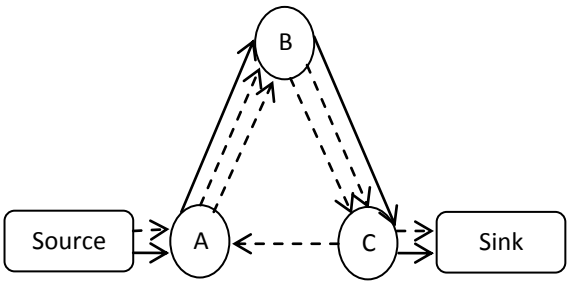


**Fig 1: Example of Stretch Attack**

### *2.5.2 Effect on State Full Protocol*

Vampire attack affects state full protocols e.g. AODV in following manner

In case of state full routing, routes are discovered on–demand basis not pre-discovered like in source routing which makes vampire lesser effective, still vampire can waste energy of network nodes by restarting packets in some part of network. Attacker node tends to divert paths using directional antenna attack which causes energy consumption of network nodes.

Another type of attack that affects both type of routing is fake route discovery request. For discovery of route there is also transfer of route request and response packet, so malicious nodes may falsely generate route discovery process any time and create packet flooding. AODV and DSR are also vulnerable to this type of attack.

# 3. LITURATURE SURVEY

Eugene Y. Vasserman (Vasserman et al., [7]) defined Vampire attacks, 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. The work is limited to packet

forwarding phase only, this solution does not work in topology discovery phase.

B. Umakanth 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 (Umakanth et al., [8]). 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.

V. Subha proposed a system that introduces a new authentication and key management mechanism called Hybrid Key Management (V. Subha et al., [9]). 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.

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 (V.Sharmila et al., [10]). 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.

# 4. PROPOSED WORK

As we have studied working of vampire attacker which drains network energy by flooding packets and RREQ flooding, so that broadcast rate of vampire node will be hire and also it has hire energy than other network nodes. The proposed work is based on the difference of variance of network node`s energy at different time. Firstly a list is prepared for the suspected nodes on the basis of their broadcast and energy values which are greater than respective variances than suspected nodes are removed from network temporarily and energy consumption is analyzed if energy consumption rate is decreased than suspected node turns to be vampire node and removed. Proposed algorithm is described below which will be scheduled on regular time interval to detect attack.

Calculate the variance of broad cast of all nodes of network at the time $t_1$using the formula

$$V_{B_{t_1}} = \frac{1}{n}\sum_{i=1}^{n}(B_i - \mu)^2$$

Where $V_{B_{t_1}} = variance\ of\ broadcast\ of\ nodes\ at\ time\ t_1$

$$\mu = is\ the\ mean\ value$$

Prepare a set of nodes that are having broadcast more than $V_{B_{t_1}}$this can be denoted using

$$set_{B_{t_1}} = \{N_1, N_2, \dots, N_n\}$$

Calculate the variance of energy levels of all nodes at the same time $t_1$using the formula

$$V_{E_{t_1}} = \frac{1}{n}\sum_{i=1}^{n}(E_i - \mu)^2$$

Where $V_{E_{t_1}} = variance\ of\ broadcast\ of\ nodes\ at\ time\ t_1$

Prepare a set of nodes that are having energy more than $V_{E_{t_1}}$this can be denoted using

$$set_{E_{t_1}} = \{N_1, N_2, \dots, N_n\}$$

In order to find the set of nodes those are suspected in the network at time$t_1$.

$$SS_{t_1} = set_{E_{t_1}} \cap set_{B_{t_1}}$$

Similarly at time $t_2$ energy variance $V_{E_{t_2}}$ is calculated with the degree of their estimated suspected nodes$SS_{t_1}$.

In order to find final set of suspected nodes in the network calculate

$$SS_t = SS_{t_1} \cap SS_{t_2}$$

In further for detection of malicious node in network and to remove them in further from time $t_3$ the following process is used by temporally removing suspected node from network.compute $V_{E_{t3}}$and $V_{B_{t3}}$

Compute the different for time $t_2$ and $t_1$

$$diff_{t2t1} = V_{E_{t_2}} - V_{E_{t_1}}$$

Compute the different for time $t_3$ and $t_2$

$$diff_{t3t2} = V_{E_{t_3}} - V_{E_{t_2}} SS_{t_2}$$

If $diff_{t2t1} > diff_{t3t2}$

Remove node from network permanently

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

# 5. CONCLUSION

This work includes study of security breach of WSN by vampire attack for various stateless and state full routing protocols and different solution provided to deal with vampire attack in literature survey. Proposed methodology supposed to provide dynamic detection and removal of vampire attack from WSN which also work in dynamic topology change in WSN. According to the proposed solution vampire attacker will be detected on the basis of packet broadcast rate and energy parameters among network nodes. In near future a new

technique according to proposed methodology is implemented using NS2 network simulator and the performance of the network under vampire network in terms of energy, PDR and throughput is provided.

## 6. REFERENCES

[1] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci 2001, Wireless sensor networks: a survey, Elsevier Computer Networks.

[2] Jamal N. Al-Karaki Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey.

[3] Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth 2012, A Survey on Security Attacks in Wireless Sensor Network, International Journal of Engineering Research and Applications.

[4] Jaydip Sen, Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses, Innovation Lab, Tata Consultancy Services Ltd.

[5] Wood, A.D. &Stankvic, J.A. 2002 Denial of service in sensor networks. IEEE Computer, Vol. 35, No. 10, pp. 54-62.

[6] Karlof, C. & Wagner, D. 2003 Secure routing in wireless sensor networks: attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications.

[7] Eugene Y. Vasserman and Nicholas Hopper 2013, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. IEEE transactions on mobile computing.

[8] B. Umakanth1, J. Damodhar2 2013, Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks, International Journal of Engineering Trends and Technology (IJETT).

[9] V.Subha1, P.Selvi 2014, Defending against vampire attacks in wireless sensor networks, International Journal of Computer Science and Mobile Computing.

[10] V.Sharmila1 2014, Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network, International Journal of Computer Science and Mobile Computing.