# A Survey: The Different Attacks and Security Scheme to Secure MANET

Poonam Sahu[1], Prof. S. R. Yadav[2]

*[1]PG Scholar, Mtech(CSE), [2]HOD, CSE*

*Millennium Institute Technology and Science Bhopal, India*

***Abstract:*** ***In Wireless Sensor Networks nodes are energy constrained since nodes operate with limited battery energy. If some nodes die early due to lack of energy, they cannot communicate with each other. Nodes within an ad hoc network generally rely on batteries (or exhaustive energy sources) for power. Since these energy sources have a limited lifetime, availability for surviving in network is one of the most important constraints for the nodes that perform communication in wireless Ad hoc sensor network. Therefore, inordinate consumption of nodes energy should be prevented. In fact, node energy consumption ought to be balanced so as to extend the energy awareness of networks. In this survey of attacks and security scheme some of the solution for different attacks is discuss with including vampire routing attack in WSN. Security is required in WSN because attacker is consumes the useful energy of nodes i.e. necessary for communication in network. The Vampire attacker is flooding the huge amount of packets in network and every node in network is capture and forwards these packets to next neighbour. The packets sending and receiving consume lot of energy. The proposed security scheme function is to detect the attacker on the basis of attacker malicious activities and identified the routing misbehaviour in network.***

***Index Terms— Energy, Vampire attack, Routing, Security, Survey, WSN.***

## I. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of mobile nodes working without any fixed communication infrastructures or base stations to provide connectivity [1, 2]. The nodes also work with base stations but these nodes are not continuously changing their location. Each node in the WSN acts both as a host and a router. If two nodes not among the transmission range of every different, different nodes are required to serve as intermediate routers for the communication between the two nodes. The hosts are free to move around randomly, and hence the network topology may change dynamically over time. One of the first WSNs was designed and developed in the middle of the 70s by the military and defense industries. WSNs were also used throughout the Vietnam so as to support the detection of enemies in remote jungle areas. However heir implementation had many drawbacks. It includes the large size of the sensors, the energy they consume and therefore the limited network capability. Due to absence of a administrative control network security is that the major criteria. The attacker or malicious node like lamia attack [2] has consumed restricted energy resource [1] by that the life time of network is affected. the normal routing protocols have many shortcomings when applied to WSNs, which are mainly due to the energy constrained nature of such network[2]. As an example, flooding could be a technique in which a given node broadcasts data and management packets that it's received to the remainder of the nodes in the network. This process repeats till the destination node is reached. Note that this technique doesn't take under consideration the

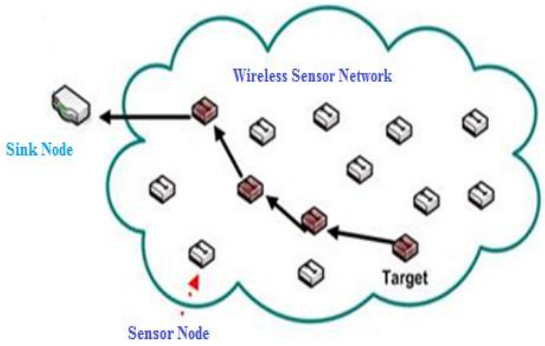


**Fig.1 Example of WSN**

This information is usually created accessible to the user through one or more intermediate nodes [3]. To make the wireless sensor network vision a reality, design should be developed that synthesizes the pictured applications out of the underlying hardware capabilities. WSNs have wide variety of military and civilian applications like battle field surveillance, healthcare applications, environment and habitat monitoring, home automation, traffic control, industry process control etc. Sensor nodes work together, to form a network for monitoring the target region. Through the cooperation of sensor nodes, the WSNs collect and send various types of messages regarding the monitored atmosphere (e.g. temperature, humidity, pressure etc.) to the sink (base) node, which processes the information and reports it to the user. The sensor network consists of sensor nodes which are randomly distributed. It has been assume having the following properties [4]:-

1. All nodes are stationary and the base station is at the centre.
2. All nodes are homogenous and energy constrained.

3. Energy consumed for sensing and processing the data is not considered.
4. Nodes are location unaware. But each node can compute the distance to another node based on the signal strength of received message.
5. Nodes sense the environment continuously and send the data at a fixed rate.

The characteristics of sensor networks and application necessities have a decisive impact on the network style objectives in term of network capabilities and network performance [4].

*A. Network Characteristics*

The traditional wireless networks like Sensor Ad hoc Network (SANET) and Cellular Network (CN) is comparable to wireless sensing element networks have the subsequent distinctive characteristics and constraints:-

- **Densely deployment**: Sometimes Sensor nodes are densely deployed and might be many orders of magnitude on top of that in a SANET. The densely deployed network is reliable but required more resources and constraint.
- **Battery-powered sensing element nodes:** The battery power is consumed for every activity done by sensor. Sensors are unit sometimes hopped up by battery and are deployed during a callous setting wherever it's very sturdy to alter or recharge the batteries.
- **Strict energy utilization, calculation, and storage constraints:** the battery utilization based communication is the critical task in sensor network. Sensors have extremely restricted energy, computation, and storage capabilities.
- **Self-configurable:** Sensors are independently communicated with each other. Sensing nodes are sometimes arbitrarily deployed and separately section themselves into a communication network.
- **Unreliable sensor nodes:** the sensors are unreliable in term of communication. If the node is participating in routing then they're out of range is break the communication and second is energy depletion. Since sensing element nodes are at risk of physical damages or failures because of its readying in harsh or hostile setting.
- **Data redundancy:** The sensor nodes in network collect huge amount of data and the nodes possible to deliver data same information that will to already evaluate. Thus, the data detected by multiple sensing element nodes usually have a particular level of correlation or redundancy.
- **Application specific:** A sensors in network is typically designed and deployed for a particular application or a multiple tasks. The planning necessities of sensors in network modified with its application. The each sensor node energy time collect the information and complete their task.
- **Many-to-one communication manner:** The collected by sensor nodes must be possible to deliver through the single sensor due to not identified the another sensor in range. In most sensor network applications, the data detected by sensing element nodes be due multiple supply sensor nodes to a selected single sink, exhibiting a many-to-one manner.
- **Frequent topology change:** The sensor network is dynamic that means the topology changes frequently because of the node failures, damage, addition, energy depletion, or channel fading.

*B. WSN Challenges And Routing Issues*

The design of routing protocols for WSN is difficult owing to many network constraints. WSN suffer from the restrictions of many network resources, as an example, energy, bandwidth, central process unit, and storage [5, 6]. The planning challenges in networks involve the subsequent main aspects [3, 5, 6]:

Limited Energy Capacity: Since detector nodes area unit battery high-powered, they need restricted energy capability. Energy pretenses an enormous challenge for network designers in hostile environments, for example, a battlefield, wherever it is not possible to access the sensors and recharge their batteries. Moreover, once the energy of a detector reaches a definite threshold, the sensor can become faulty and cannot be able to operate properly, which can have a significant impact on the network performance. Thus, routing protocols designed for sensors ought to be as energy economical as doable to increase their period of time, and therefore prolong the network period of time whereas guaranteeing sensible performance overall.

- **Sensor locations:** Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the possible protocols assume that the sensors either ar equipped with international positioning system (IPS) receivers or use some localization technique [7] to find out about their locations.
- **Limited Hardware Resources:** Additionally to restricted energy capability, sensor nodes have jointly restricted process and storage capacities, and thus will only perform restricted procedure functionalities. These hardware constraints gift many challenges in code development and

network protocol style for detector networks, that should contemplate not only the energy constraint in sensor nodes, but collectively the process and storage capacities of detector nodes.

- **Massive and Random Node Readying**: sensor node deployment in WSNs is application dependent and may be either manual or random that finally affects the performance of the routing protocol. In most applications, sensor nodes is scattered arbitrarily in an intended space or a massively over inaccessible or hostile region. If the resultant distribution of nodes isn't uniform, best clustering becomes necessary to permit property and modify energy efficient network operation.
- **Network Characteristics and Unreliable Ambiance:** A sensor network sometimes operates in a very dynamic and unreliable environment. The topology of a network, that is outlined by the sensors and therefore the communication links between the sensors, changes topology owing to detector addition, deletion, node failures, damages, or energy depletion. Also, the detector nodes area unit connected by a wireless medium, that is error prone, and time variable. Therefore, routing ways ought to contemplate constellation dynamics owing to restricted energy and detector quality also as increasing the dimensions of the network to keep up specific application necessities in terms of coverage and property.
- **Data Aggregation:** Since in network nodes might generate important redundant knowledge, a similar packet from multiple nodes is collective in order that the quantity of transmissions is reduced. Data aggregation technique has been accustomed come through energy potency and data transfer improvement in a very range of routing protocols.
- **Diverse sensing application requirements:** sensor networks have a large range of varied applications.No network protocol will meet the necessities of all applications. Therefore, the routing protocols ought to assurance data delivery and its accuracy in order that the sink will gather the desired data concerning the physical phenomenon on time.
- **Scalability:** Routing protocols need to be able to scale with the network size. Also, sensors might not essentially have equivalent capabilities in terms of energy, processing, sensing, and significantly communication. Hence, communication links between sensors might not be radial, that is, a try of sensors might not be able to have communication in each direction. This could be taken care of within the routing protocols.

## II. ROUTING PROTOCOLS IN WSN

Routing in wireless sensor network (WSN) differs from conformist routing in fixed networks in various ways. The sensor node done routing without any fixed infrastructure, wireless links are unreliable, sensor nodes possibly will fail, and routing protocols have to congregate stringent resources requirements [8, 9, 10]. Routing paths can be established in one of three ways, namely proactive, reactive or hybrid..

### *C. Proactive (table-driven) Routing Protocol*

The proactive routing protocol is the table driven protocol to managing the table of route information in network. The proactive routing protocol are showing the better performance in fixed or stationary network because the routing table updation is not possible their but in dynamic sensor network the routing information is changes by that the overhead in network is more. The most well-known types of the proactive routing protocol are: - Destination sequenced distance vector (DSDV) routing protocol.

### *D. Reactive (on-demand) Routing Protocol*

The reactive routing protocols re maintaining the connection in a On demand manner means if required then established connection. The routing protocol are flooded the route request and if the destination found data delivery is started but after the completion of routing procedure including data sending route information is completely destroyed in from nodes that has participating in routing. The Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol is the example of that kind of routing.

### *E. Hybrid Routing Protocol*

The hybrid routing protocol as the name suggests have the combine benefits of proactive routing and reactive routing to overcome the defects generated from each the protocol when used one by one. design of hybrid routing protocols ar mostly as hierarchical or layered network framework. during this system at the start, proactive routing is used to collect unfamiliar with routing info, and so at later stage reactive routing is used to keep up the routing info when topology changes.The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [11].

## III. LITERATURE SURVEY

Most of the present solutions however overlook some important aspects in this regard that consequently adversely affects the network performance. These limitations are in brief described as follows: first, enough consideration isn't

given to dynamic detection of packet forwarding misbehavior caused by poor wireless communication quality, harm or broken nodes in network, hardware or software faults and significant level of congestion that prevents nodes to forwards packets successfully. Second, most of trust aware protocols do nothing to optimize the end-to-end route across the network keeping in view important characteristics of WSN such as energy and wireless interference while heavily rely on selecting most trusted neighbors irrespective of their energy resource.

This paper [12] has only identified that the vampire attacks can be easily executed using even a single malicious intruder, who sends simply protocol complaint message, these attacks are thus destructing and extremely hard to find. in the nastiest condition, an individual attacker has the ability to enlarge the energy usage of the network by a factor of O(N), wherever N is that the quantity of nodes within the network. a new proof-of-concept protocol is a method mentioned to mitigate these types of attacks. This protocol limits the damage caused at the time of packet forwarding done by Vampires.To diminish the Vampire attacks using PLGP-a (parno ,luk, gausted and perrig wih attstations) which identifies malicious attack, certain approaches have also been discussed. PLGP stands for a clean-slate secure sensor network routing protocol by parno ,luk, gausted and perrig.

Vidya.M [13] this paper a innovative approach for routing protocols, have an effect on from attack even those devised to be protected that is brief of protection from these attacks, that we tend to decision energy debilitating attacks, which enduringly disable networks by quickly draining nodes battery power.We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. They also saw how to overcome these attacks by increasing the energy of the node in the network.

In this paper [14], a Trust and Energy aware Routing Protocol (TERP) has been specifically designed to address the limitations of existing trust based routing protocols. Keeping resource-constrained characteristic of WSN in mind, the design of TERP is centered on trustworthiness and energy efficiency. TERP is capable of dynamically detecting and analytic misbehaving nodes throughout trust analysis phase while energy awareness feature is incorporated in route setup phase of routing protocol that helps in better load balancing among trusted nodes.The TERP protocol has been designed to integrate trust based routing but additionally includes mechanisms which ensure that end-to-end routes are selected while keeping in view the current energy levels of the intermediate nodes.

Ambili M.A [15] In this paper we define that a Network survivability is the ability of a network keeping connected under failures and attacks, that is that the most significant issue within the design and performance of wireless ad hoc sensor networks. The paper projects its focus on the approach in which the attack can be overcome in the best possible manner. The proposed system describes some strategies and different routing protocols answer that help to detect and eliminate vampire attack and therefore make the network live.An energy constraint intrusion detection scheme is introduced together with clean state secure routing protocol.

## IV. PROBLEM IDENTFICATION

Vampire attack happens within the network within the sense, any of the nodes within the network that is affected or infected and this nodes behavior is suddenly dynamic for the network behavior, this type of nodes area unit known as “Malicious node”. If malicious nodes gift within the network energy that are exploitation by every and each nodes can be increase drastically. The malicious nodes are place within the network unambiguously. Initialy In between the routing nodes, and therefore the second placed within the supply node itself the possibility of putting a malicious node within the routing path this makes inflicting injury in network. Supply node characterized the actual packets and elect packets square measure known for the routing to the destination. The routing path is discovered by supply node by exploitation shortest path routing algorithmic program and therefore the path shouldn’t be changeable by the intermediate nodes.

## V. PROPOSED METHODOLOGY

AODV belongs to the category of Distance Vector Routing Protocols (DV). in an exceedingly DV each node is aware of its neighbor’s and therefore the prices to get within the direction of them. A node maintains its own routing table, storing all nodes within the network, the space and therefore the next hop to them. If a node isn't approachable the space to that is about to time with no sign of ending. Each node sends its neighbor’s sometimes its complete routing table. in order that they will check if there's a helpful route to a different node exploitation this neighbor as next hop. AODV is associated ‘on demand routing protocol’ with little delay.

### 5.1 Requirement Analysis

When time has been analyzed node die due to lack of remaining battery (i.e., expiration time of nodes) as well as the lifetime of connection which captures the effects of disconnections due to lack of possible routes (i.e., expiration time of connections).

**Table 5.1 Simulation parameters for case study.**

| | |
|---|---|
| Simulator Used | NS-2.31 |
| Number of nodes | 30 |
| Dimension of simulated area | 800m×600m |
| Routing Protocol | AODV |

| | |
|---|---|
| Simulation time | 100 |
| Traffic type | CBR (3pkts/s) |
| Packet size | 512 bytes |
| Number of traffic connections | TCP / UDP |
| Node movement at maximum Speed (m/s) | random |
| Transmission range | 250m |
| Threshold value | 10 joule |
| Transmit power | 1.5 joule |
| Receiving power | 1.0joule |
| Idle power | .17 joule |
| Sleeping power | .047 joule |

## VI. CONCLUSION

This analysis is extremely helpful in field of engineering to gauge the network performance just in case of attack Wireless device network may be a quite ad-hoc network. There a brand new quite internal attack known as vampire attack drain the energy of every device within the network, during this planned work an evil spirit attack is investigated and applicable methodology is planned for implementation for rising security and performance in network by distinguishing and removing suspicious node from the network. supported the recently developed techniques a replacement security technique is meant and enforced for simulating the impact of attack preparation and therefore the performance improvement once security theme implementation. In addition, for justifying the answer and their increased performance ancient routing protocol is needed to check with the developed routing protocol. In terms of outturn, finish to finish delay, stay energy and packet delivery magnitude relation.

In networking the communication between the sender and receiver is possible if link between then is available. That means the distance don't matter. In Wireless Sensor Network (WSN) having large numbers of tiny, low-powered wireless nodes with limited computation, communication, and sensing abilities, in a powered sensor network, energy and communication bandwidth are precious resources. This survey of attacks and preventions is extremely helpful in field of engineering to gauge the network performance just in case of attack Wireless device network may be a quite ad-hoc network. There a brand new quite internal attack known as vampire attack drain the energy of every device within the network, during this planned work a evil spirit attack is investigated and applicable methodology is planned for implementation for rising security and performance in network by distinguishing and removing suspicious node from the network. supported the recently developed techniques a replacement security technique is meant and enforced for simulating the impact of attack preparation and therefore the performance improvement once security theme implementation. In addition, for justifying the answer and their increased performance ancient routing protocol is needed to check with the developed routing protocol.

## VII. EXPECTED OUTCOME

Purpose to implement planned Technique in NS-2 [16] and find malicious node that causes vampire attacks and take away the vampire node from the network. It is identify to compare planned work with normal routing performance. Will be detected vampire attack on the basis of heavy flooding of packets and these packets are consumes the un-necessary energy of other normal nodes because in every action perform by node is consumes limited source of energy.

## REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks, Elsevier, pp. 2292–2330, 2008.

[2] A.Vincy, V.Uma Devi, "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014

[3] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[4] S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.

[5] Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Communications Magazine, vol 11, no. 6, pp. 6-28, Dec. 2004.

[6] Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices", IEEE Personal Communication Magazine, vol. 7, no. 5, pp. 28-34, Oct. 2000.

[8] Clement Ogugua Asogwa, Xiaoming Zhang, Degui Xiao, Ahmed Hamed, "Experimental Analysis of AODV, DSR and DSDV Protocols Based on Wireless Body Area Network" Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg,Volume 312, pp 183-191, 2012.

[9] Faleh Rabeb, Nasri Nejah, Kachouri Abdennaceur,Samet Mounir, "An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network" IEEE, International Conference on Education and e-Learning Innovations, 2012.

[10] Nasrin Hakim Mithila, "Performance analysis of DSDV, AODV and DSR in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and

Electronics Engineering (IJARCSEE) Volume 2, Issue 4, pp.395-404, April 2013.

[11] Z. Haas and M. Pearlman, "The Performance of Query Control Schemes for the Zone Routing Protocol," ACM/IEEE Transactions on Networking, Vol.9, No.4, pp.427-438, August 2001

[12] Lina R.Deshmukh, Prof. A. D. Potgantwar, "Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops", IEEE International Conference on Advance Computing (IACC), pp. 61 - 66, 12-13 June 2015.

[13] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network", IEEE Sensors Journal, Vol. 15, No. 12, December 2015.

[14] Ambili M.A, Biju Balakrishnan, ‘‘Vampitr Attack: Detection and Elimination in WSN”, IJSR Vol- 3 April 2014.

[15] Vidya.M, 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.

[16] The CMU Monarch Project, The CMU Monarch Extensions to the NS Simulator, URL: http://www.monarch.cs.cmu.edu/. Page accessed on February 20th, 2010.