International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 6, Nov-Dec-2021, ISSN (Online): 2395-566X

# A Survey on Wireless Network Optimization by Attack Prevention and Detection Techniques

**Lipi Sharma,Dr.Vivek Richariya**
Dept. of Computer Science & Engg.
Lakshmi Narain College of Technology
Bhopal, MP,India

**Abstract- Wireless sensor network are acting as a important portion for implementation, maintains of many application and services. Open network for communication increases its flexibility and vulnerability of attacks as well. It is critical challenge to develop the effective and lightweight security mechanism to detect and prevent various attacks for WSN Attacks were list in the paper and classified as per nature of the activity performed by malicious nodes. This paper has summarized energy dependency of the WSN, paper has list some of techniques to expand life of the WSN network. Many of researcher has proposed different techniques of network attack detection were detailed in the paper. Some of energy optimization papers were also introduced to increase the life span of network.**

**Keywords- Communication Network, WSN, Sensor Node, Energy Optimization.**

## I. INTRODUCTION

Large numbers of tiny sensor nodes in a network make it possible to obtain data about physical occurrences that was difficult or not possible to obtain in more conventional ways. In the coming years, as developments in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, growing deployments of wireless sensor networks are projected, with the networks eventually growing to large numbers of nodes.

After the initial deployment (typically ad hoc), sensor nodes are responsible for selforganizing a proper network arrangement, often with multihop connections between sensor nodes. In wireless Sensor Networks, the nodes use the open air medium to communicate with each other, in doing so they face sensitive security problems as compared to the wired networks.

Wireless Sensor networks are vulnerable to security attacks due to the nature of broadcasting through the transmission medium. Also, wireless sensor networks have an additional vulnerability because of the nodes placement in a hostile or dangerous environment where they are not physically protected. Attacks can either be used to examine the traffic throughout the network or to crash packets selectively or totally to affect the flow of information. The security mechanisms that are used for wired systems such as authentication and encryption are useless under hidden mode of attack because the nodes do not modify their headers but only forward these packets.

But the attack in participating mode is more complicated, because if it once launched, it is difficult to detect. WSN platforms generally have limited processing capability and memory. The design of WSN devices usually favors decreased cost over increased capabilities.

Classifications of security attacks where they are classified as active attacks and passive attack.

**1. Passive attacks:**
The listening of the communication channel by unauthorized attackers and the channel are monitored by the attackers are known as passive attacks. Attacks against privacy are the main privacy problem is not that sensor networks enable the collection of information. Sensor networks may notice one of the privacy problems as they have large volumes of information easily available through remote access. Also adversaries are not required to be physically present to maintain such surveillance. In an anonymous manner, they can collect information at low-risk.

**2. Active attacks:**
In active attacks, the unauthorized attackers first monitors the network, then listens to the channel and then tries to modify the data stream in the communication channel . The following attacks can be considered as active.

## II. ENERGY LOSSES AND TECHNIQUES FOR MANAGEMENT

Reasons of energy loses in WSNs, sensors absorb energy while detecting, handling, transmitting or getting information to satisfy the job done by the sensor device. The detecting subsystem is genetically worked to information collection. It was well known that limiting information extraction from transducer will preserve energy of extremely compelled sensors.

Repetition intrinsic to WSNs will create immense comparative announcing that the system is accountable for routing to the sink. Test results affirm that communication subsystem is a ravenous wellspring of energy scattering. With respect to communication, there is likewise an incredible measure of energy loses in states that are ineffective from the application perspective, for example, [4]:

**1. Overloading:**
When a sender transmits a data unit, all nodes in its transmission area get this data unit regardless of whether they are not the proposed goal. In this way, energy is loses when a node gets data units that are bound to different nodes.

**2. Idle listening:**
Is one of the real energy dispersal reasons. It happens when a node is tuning in to a sit divert with a specific end goal to get conceivable movement.

**3. Control packet overhead:**
An insignificant number of control data units ought to be utilized to empower information transmissions.

**4. Collision:**
When a node gets in more than one data unit in the meantime, these data units get collide. All data units that reason the crash must be disposed of and the retransmission of these data units is required.

**5. Interference:**
Every node situated between transmission range and impedance area gets a data unit yet can't decipher it.

As system lifetime has turned into the key trademark for assessing WSN, panoply of strategies looks for limiting energy utilization and enhancing system lifetime, were proposed. This work presently gives a scientific categorization of these methods.

## III. WSN ATTACKS

**1. Denial of Service (DoS) attacks:**
Wood and Stankovic have defined a DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function [18]. There are several standard techniques existing in the literature to cope with some of the more common denial of service attacks, although in a broader sense, development of a generic defense mechanism against DoS attacks is still an open problem.

Moreover, most of the defense mechanisms require high computational overhead and hence not suitable for resource constrained WSNs. Since DoS attacks in WSNs can sometimes prove very costly, researchers have spent a great deal of effort in identifying various types of such attacks, and devising strategies to defend against them. Some of the important types of DoS attacks in WSNs are discussed below.

**2. Physical layer attacks**:
The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [12]. As with any radio-based medium, the possibility of jamming is there. In addition, nodes in WSNs may be deployed in hostile or insecure environments where an attacker has the physical access. Two types of attacks in physical layer are (i) jamming and (ii) tampering.

**2.1 Jamming:** It is a type of attack which interferes with the radio frequencies that the nodes use in a WSN for communication [11]. A jamming source may be powerful enough to disrupt the entire network. Even with less powerful jamming sources, an adversary can potentially disrupt communication in the entire network by strategically distributing the jamming sources. Even an intermittent jamming may prove detrimental as the message communication in a WSN may be extremely time-sensitive [11].

**2.2 Tampering:** This sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks. The physical attacks may cause irreversible damage to the nodes. The adversary can extract cryptographic keys from the captured node, tamper with its circuitry, modify the program codes or even replace it with a malicious sensor [15]. It has been shown that sensor nodes such as MICA2 motes can be compromised in less than one minute time [14].

**3. Link layer attacks**:
The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [12]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [11]. When packets collide, they are discarded and need to re-transmit. An adversary may strategically cause collisions in specific packets such as ACK control messages.

A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions. Repeated collisions can also be used by an attacker to cause resource exhaustion [11].

For example, a naïve link layer implementation may continuously attempt to retransmit the corrupted packets. Unless these retransmissions are detected early, the energy

levels of the nodes would be exhausted quickly. Unfairness is a weak form of DoS attack [11]. An attacker may cause unfairness by intermittently using the above link layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

**4. Network layer attacks**:
The network layer of WSNs is vulnerable to the different types of attacks such as: (i) spoofed routing information , (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole, (vi) hello flood, (vii) acknowledgment spoofing etc[25]. These attacks are described briefly in the following: Spoofed routing information: the most direct attack against a routing protocol is to target the routing information in the network.

An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [12]. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

**4.1 Selective forwarding**: In a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [3].

**4.2 Sinkhole**: In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information [13, 12, and 11]. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

**4.3 Sybil attack**: it is an attack where one node presents more that one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-topeer networks [11]. Newsome et al describe this attack from the perspective of a WSN [13].

In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes".

Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

**4.4 Wormhole**: a wormhole is low latency link between two portions of a network over which an attacker replays network messages [12]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

**4.5 Hello flood**: most of the protocols that use Hello packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [12].

Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the Hello packets, attempt to transmit to the attacker node. However, these nodes are out of the radio range of the attacker. Acknowledgment spoofing: some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [12]. In this way, the attacker is able to disseminate wrong information about the status of the nodes.

**5. Transport layer attacks:**
The attacks that can be launched on the transport layer in a SN are flooding attack and desynchronization attack.

**5.1 Flooding**: Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding [16]. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

**5.2 De-synchronization**: De-synchronization refers to the disruption of an existing connection [16]. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

## IV. RELATED WORK

**Nayyar et al. [16]** compared the benefits and drawbacks of each enlisted protocol for UWSN based on several parameters such as routing technique, packet delivery ratio, energy efficiency, packet latency, and localisation.

**John et al. [17]** addressed the operation of different location-based opportunistic routing algorithms proposed for UWSNs and analysed the performance of two key methods, VBF and HH-VBF, using Aqua-Sim simulations, although the performance of these protocols is hampered by network communication voids.

The random walking approach using camouflage packets and genuine packets is also used by **J. Wang et al. in [18].** The real data packets would walk in a random direction to mask the transmission direction, while the camouflage data packets would be inserted into the intersections of two or more shortest paths to prevent the attacker from determining the real path.

**In [19], Osanaiye et al.** focused on one of the most common assaults on WSN, the DoS Jamming attack. This attack operates by flooding the node with fraudulent traffic in order to suffocate legitimate traffic and, as a result, the network. The exponentially weighted moving average (EWMA) technique introduced in this article is used to detect abnormal variations in the strength of jamming attacks.

The defence against dual attacks for BHA and GHA has been described by Pooja Rani et al. in [20] publication using the notion of Artificial Neural Network (ANN) as a deep learning algorithm and the swarm-based Artificial Bee Colony (ABC) optimization technique.

## V. CONCLUSION

Computing services are developing rapidly, so adhoc networks and wireless networks grow in general. However, there are still security concerns when it comes to wireless sensor networks due to its vulnerability to numerous attacks.

In this paper a detail list of various attacks were explained. Paper has summarized techniques adopt by the scholars to prevent or detect such attacks in the network This paper has brief some techniques of energy optimization as well that directly increases the network utilization by routing algorithm. In future scholars can develop some model that protect wireless nodes from attack and optimize nodes as well.

## REFERENCES

[1] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, November 2007.

[2] Maria Sebastian and Arun Raj Kumar P, "A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer" International Journal of Computer Network and Information Security, pp. 28-38, 2013.

[3] Imad Aad, Jean-Pierre Hubaux and Edward W. Knightl "Impact of Denial of Service Attacks on Ad Hoc Networks" IEEE/ACM Transactions on Networking, Vol. 16, No. 4, pp. 791- 802, August 2008.

[4] Yu Zhang, Loukas Lazos and William Jr. Kozma "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks" IEEE Transactions on Mobile Computing (Article in Press), 2012.

[5] M. A. Shurman, S. M. Yoo, and S. Park, “Black hole attack in wireless ad hoc networks,” in ACM 42nd Southeast Conference (ACMSE’04), pp. 96-97, April 2004.

[6] Manish Patel and Dr. Akshai Aggarwal, " Detection of hidden wormhole attack in wireless sensor networks using neighborhood and connectivity information" in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 6, No. 1, January 2016.

[7] Mosmi Tiwari, Deepak Sukheja, Amrita, " Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN" in Communications on Applied Electronics (CAE), vol.3, No.3, October 2016.

[8] Ademola P. Abidoye, Ibidun C. Obagbuwa. “DDoS attacks in WSNs: detection and Countermeasures” IET IEEE, January, 2018.

[9] Ms Nidhi Sharma, Mr Alok Sharma “The Black-hole node attack in MANET" 2012 Second International Conference on Advanced Computing & Communication technologies, 546-550 2012 IEEE.

[10] Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", In Proceedings of IEEE 2nd International Conference on Communications, IEEE 2007.

[11] A.D. Wood and J.A. Stankovic, “Denial of service in sensor networks”, IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[12] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, “The Sybil attack in sensor networks: Analysis and defenses”, In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 259-268, ACM Press 2004.

[14] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems", Technical Report CUCS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.
[15] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.
[16] Nayyar, V. Puri, and D.-N. Le, "Comprehensive analysis of routing protocols surrounding underwater sensor networks (UWSNs)," in Proceedings of the Data Management, Analytics and Innovation, pp. 435–450, Springer, Singapore, August 2019.
[17] S. John, V. G. Menon, and A. Nayyar, "Simulation-based performance analysis of location-based opportunistic routing protocols in underwater sensor networks having communication voids," in Proceedings of the Data Management, Analytics and Innovation, pp. 697–711, Springer, Singapore, January 2020.
[18] J. Wang, F. Wang, Z. Cao, F. Lin, and J. Wu, "Sink location privacy protection under direction attack in wireless sensor networks," Wireless Networks, vol. 23, no. 2, pp. 579–591, 2017.
[19] Osanaiye, Opeyemi and Alfa, Attahiru and Hancke, Gerhard,"A statistical approach to detect jamming attacks in wireless sensor networks," Sensors, Multidisciplinary Digital Publishing Institute, vol. 18, pp. 1691, 2018.
[20] Pooja Rani, Kavita, Sahil Verma, Gia Nhu Nguyen. "Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network". IEEE Access July 16, 2020.