Detecting Sybil Attack Using Hybrid Fuzzy K-Means Algorithm In Wsn: A Review

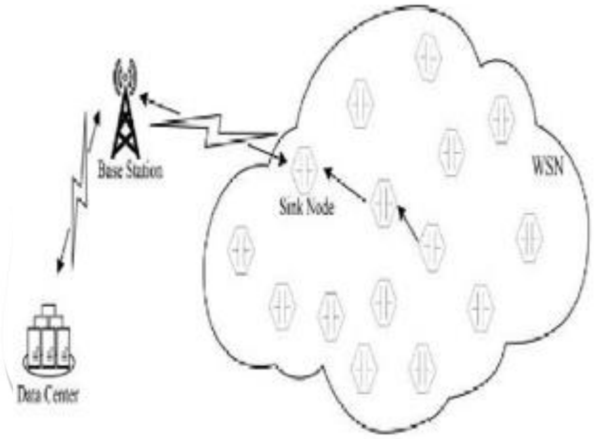
[1]Shipra Diwakar, [2]Manwinder Singh
[1]Student, [2]Head of Department
Rayat Group of Institution

Abstract - Security in Wireless Sensor Networks is an important issue of concern in recent years. Many researchers have proposed various techniques for the detection and recovery of malicious nodes in the network and compared their merits and demerits with the existing approaches. Attacks in the network are caused due to the vulnerability of the nodes in the network which results in the loss of data of the node and the routing data. In the proposed approach a Hybrid Fuzzy K-means algorithm is used for the detection of Sybil attacks. The proposed approach combines the fuzzy approach and the k-means classification approach.

Keywords - Sybil Attack, WSN

I. INTRODUCTION

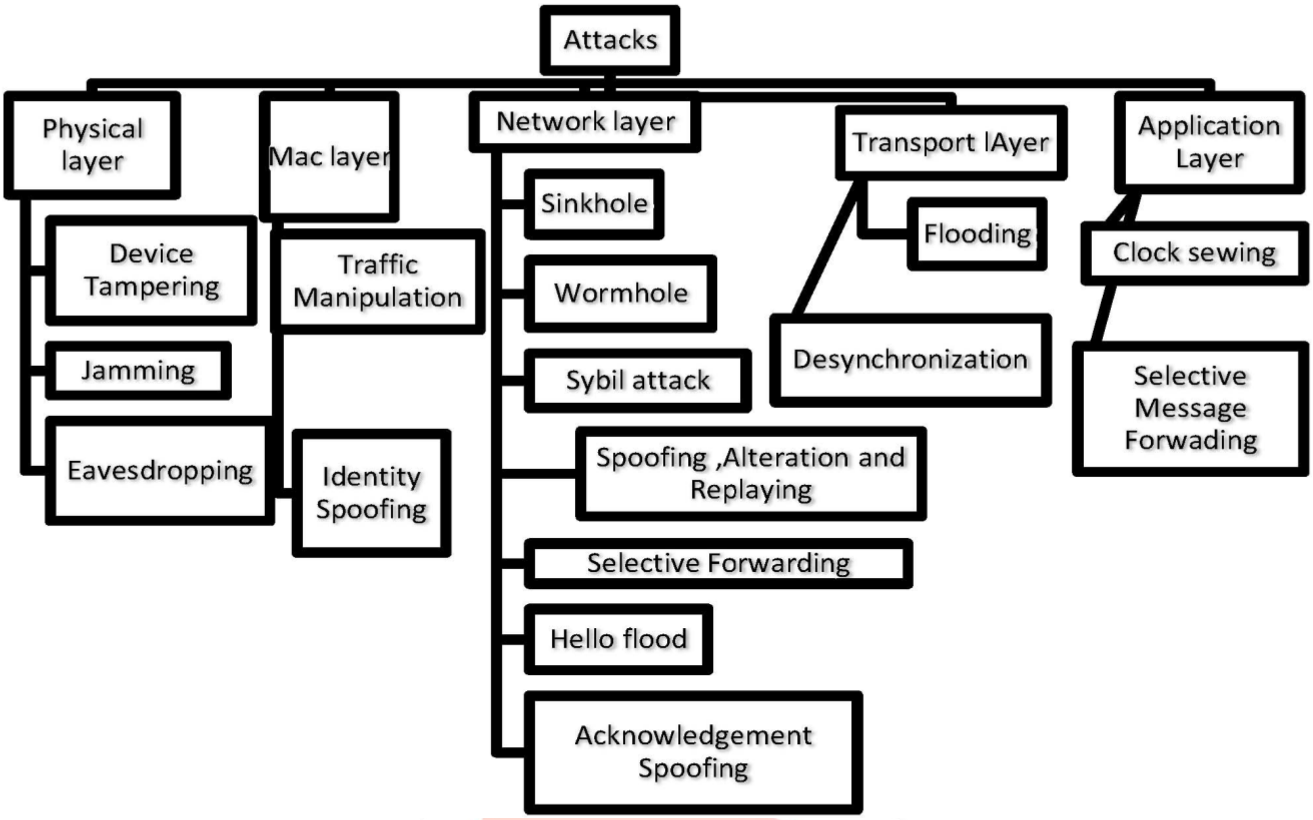
As the wireless sensor network covers a wide area of application like health care, utilities and remote control. It is the most technology which can change the future. This network consists of a large number of wireless sensor devices working collaboratively to complete a particular task. It has one or more base station. These base stations collect data from all the sensors. A large number of sensor nodes can scattered so these networks can operate on a wide area. Each sensor node can monitor, sense or process and display the data and can communicate with other also



II. APPLICATIONS OF WIRELESS SENSOR NETWORK

Because of a large number of advantages of wireless sensor network like easy to use, less failure risk ,enhanced mobility it has wide area of applications like in health care, environmental sensing and industrial uses also. Some of them are explained below.
1.Application of wireless sensor network in health care.
2.Application of wireless sensor network in environmental sensing.
3.Application of wireless sensor network in Industrial area.

III. NETWORK ATTACKS



There are different types of attacks which are a threat to computer network communication these are categorized on the basis of their effect. Including data Integrating and confidentially, power consumption, routing, identity, privacy, and service availability. Some of them are discuss below.

1.Data integrity and confidentially related attacks
Generally, this type of attack reveal the confidentiality of the transmitted data.
a. Denial of service (DOS) attack

Each server has a limit up to which is can accept or process on request. But when an attacker overloads the server sending more requests than its limit at that time this type of attack succeeded. Now when the legitimate user send the data he get unavailable network. Sometimes attacker tempers with data before it is read by the sensor by node.[14]

b.Node Capture Attack:
In Node Capture Attack an attacker physically captures sensor nodes and compromises them so that sensor readings sensed by compromised nodes are inaccurate or manipulated. The attacker may also attempt to extract essential cryptographic keys like a group key from wireless nodes that are used to protect communications in most wireless networks[9].

c. Eavesdropping attack:
Eavesdropping is the process of gathering information from a network by snooping on transmitted data and to eavesdrop is to secretly overhear a private conversation over a confidential communication in an unauthorized way[27]. The information remains the same but its privacy is compromised. An attacker eavesdrops secretly between any two nodes and may collect the necessary information regarding connection such as MAC address and cryptographic information. An attacker may also steal the User Id and password information.

2.POWER CONSUMPTION ATTACKS:
One of the most valuable asset in wireless network is the power supply. In power consumption related attacks an attacker tries to exhaust the wireless device’s power supply and it may degrade the lifetime of the network. A worst case scenario may even collapse the network communication.

a. Denial of Sleep Attack:
In a wireless network whenthere is no radio transmission, the MAC layer protocol reduce the node’s power consumption by regulating the node’s radio communications. An attacker may use this scenario and try to drain a wireless device’s limited power supply (especially sensor devices) so that the node’s lifetime is significantly shortened .Thus, the attacker attacks the MAC layer protocol to shorten or disable the sleep period. If the number of power drained nodes is large enough, the whole sensor network can be severely disrupted. Even with power management tools in place, unless a MAC protocol can create opportunities to sleep for long durations, the platform cannot achieve extended network lifetimes.

b.Collision Attack:
In collision attack, attacker tries to corrupt the octet of transmitted packets. If attacker succeeds in doing so; then, at the receiving end; the packets will be discarded due to checksum mismatch. The retransmission of packets could cause exhaustion of necessary resources i.e. energy of the sensor nodes.[15]

c. De-Synchronization Attack:

In de-Synchronization Attacks, attacker forges messages between endpoints. Modification in control flags or sequence numbers are usually made. If the attacker is lucky and got the control at right timing, then he might prevent the endpoints from ever exchanging messages as they will be, by continuously requesting retransmission of lost message. This attack leads to an infinite retransmission cycle that exhausts lot of energy[18].

3. SERVICE AVAILABILITY AND BANDWIDTHCONSUMPTION RELATED ATTACKS:

These attacks mainly aim to devastate the forwarding capability of forwarding nodes or consume meagerly available bandwidth; they are more likely related to availability of service and bandwidth consumption. These attacks can also be categorized as power consumption-related attacks. If these attacks result in a denial of service to legitimate members, they can also be referred to as a variant of denial-of-service (DoS) attacks.

a. Flooding Attack:

There are various kinds of denial of service attacks which are planned in different manner and decreases network lifetime in different ways. One among them is the flooding kind of Denial of Service attack. An attacker using this kind of attack normally sends a large number of packets to the victim or to an access point to prevent the victim or the entire network from establishing or continuing communications .This process is analogous to TCP SYN attacks where, attacker sends many connection establishment requests, forcing the victim to store the state of each connection request. The primary aim of flooding attacks is to cause exhaustion of resources on victim system.

b. Jamming (Radio Interference) Attack:

Jamming is one of many activities used to compromise the wireless environment. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions. In the simplest form of jamming, the attacker corrupts the transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers. An attacker can commendably cut off the link among nodes by communicating continuous radio signals so that other sanctioned users are not allowed to access a particular frequency channel. The attacker can also send jamming radio signals which intentionally collide with legitimate signals originated by target nodes.

c. Replay Attack:

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an attacker who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack). An attacker copies a forwarded packet and later sends out the copies repeatedly and continuously to the victim in order to exhaust the victim's buffers or power supplies, or to base stations and access points in order to degrade network performance. In addition, the replayed packets can crash poorly designed applications or exploit vulnerable holes in poor system designs.

d. Selective forwarding attack:

This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behaviour causes a DoS attack for that particular node or a group of nodes as shown in Fig 3. A forwarding node selectively drops packets that have been originated or forwarded by certain nodes, and forwards other irrelevant packets instead. They also behave like a Black hole in which it refuses to forward every packet. The malicious node may forward the messages to the wrong path, creating unfaithful routing information in the network.

4. ROUTING ATTACK:

In general these attacks attempts to change routing information.

a. Unauthorized routing update attack:

An attacker attempts to update routing information maintained by routing hosts, such as base stations, access points, or data aggregation nodes, to exploit the routing protocols, to fabricate the routing update messages, and to falsely update the routing table. This attack can lead to several incidents, including: some nodes are isolated from base stations; a network is partitioned; messages are routed in a loop and dropped after the time to live (TTL) expires; messages are perversely forwarded to unauthorized attackers; a black-hole route in which messages are maliciously discarded is created; and a previous key is still being used by current members because the rekeying messages destined to members are misrouted or delayed by false routings.

b.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. An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet which traverses through the usual routes. Such a tunnel can be created by several means, such as by sending the copied packet through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low-latency route, or using any out-of bound channel. The wormhole attack poses many threats, especially to routing protocols and other protocols that heavily rely on geographic location and proximity, and many subsequent attacks .

c. Spoofing Attack:

In spoofing attack attacker complicates the network by creating routing loop, attracting or replaying the routing information.

d. Sinkhole attack:

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack, a compromised node tries to draw all or as much traffic as possible from a particular area, by making itself look attractive to the surrounding nodes with respect to the routing metric as shown in Fig 5. As a result, the adversary manages to attract all traffic that is destined to the base station by advertising as having a higher trust level and as a node in the shortest distance or short delay path to a base station. By taking part in the routing process, it can then launch more severe attacks, like selective forwarding, modifying or even dropping the packets coming through.

5.IDENTITY RELATED ATTACKS:

In general, these attacks cooperate with eavesdropping attacks or other network-sniffing software to obtain vulnerable MAC and network addresses. They target the authentication entity.

a.Impersonate attack:

An attacker impersonates another node's identity (either MAC or IP address) to establish a connection with or launch other attacks on a victim; the attacker may also use the victim's identity to establish a connection with other nodes or launch other attacks on behalf of the victim.

b.Sybil attack:

A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted.

6. PRIVACY RELATED ATTACKS:

In general, this type of attack uncovers the anonymity and privacy of communications and, in the worst case can cause false accusations of an innocent victim.

a. Traffic analysis attack:

An attacker attempts to gain knowledge of the network, traffic, and nodes behaviors. The traffic analysis may include examining the message length, message pattern or coding, and duration the message stayed in the router. In addition, the attacker can correlate all incoming and outgoing packets at any router or member. Such an attack violates privacy and can harm members for being linked with messages (e.g., religious-related opinions that are deemed provocative in some communities). The attacker can also perversely link any two members with any unrelated connections. If a group of attackers collude to launch any type of attacks, it is referred to as a collusion attack.

IV. UWB transmission provides a security of the physical layer for wireless sensor network as a result of their huge bandwidth [1]. Certainly, wireless sensor network which depend on the UWB radio signals are essentially safer due to its low output power and short pulses of these signals. However, UWB signals can be snuffled by a strong-minded attacker, who is located nearer to the transmitter and it enable the latter to initiate an attack against the sensor network [2]. Thus, every class of wireless sensor network needed a strategy for security which is implemented at each layer of the network protocol stack. Recently, the main focus is providing for security of wireless sensor network and the parameters on which main focus is given is routing, authentication, and key management, secure localization and secure aggregation [3]. Some secure ranging and localization protocols were particularly designed for preventing the integrity of ranging and for addressing location-related attacks in UWB WSNs. Signaling strategyare used to improve physical layer security of UWB systems. In last, a number of routing and clustering protocols attempt to address networking issues in UWB WSNs, lacking however advanced security features in their design [4]. Intrusion detection systems (IDSs) represent an significant in the arsenal of security experts against this type of attack [5]. Generally, IDS are categorized in two types:

1. Signature based intrusion detection systems.
2. Anomaly based intrusion detection systems.

According to latest researches, anomaly-based intrusion detection systems (ADSs) are well suited to wireless sensor network due to its flexibility and resource friendly behavior. Further, Anomaly-based techniques can be widely classified into prior-knowledge based andprior-knowledge free. In the framework of sensor network, rule-based detection appears to be very attractive, in the sense that the detection speed and complexity certainly benefits from the absence of an explicit training procedure [6]. A number of rule-based Sybil attack detection ADSs have been proposed so far that come with different analytical accuracy and varying degree of complexity. The fundamental detection mechanisms of these expert systems have based on an identity-based solution, a location verification approach or a visual-based method. While a number of anomaly detection algorithms exists in the literature, to the best of our knowledge, none of them is specifically designed for the emerging UWB transmission technology, the high precision ranging capability of which enables the ADS to not only detect, but also to localize the adversarial nodes by relying on internal tools, namely on accurate time-of-arrival (TOA)-based UWB distance measurements.

V. LITERATURE SURVEY

Karapistoli, Eiriniet al [1] presented a anomaly-based detection and location-attribution algorithm for cluster-based UWB WSNs. The presented approach defined a procedures for secure cluster formation, periodic re-clustering, and efficient cluster member monitoring.

Sarigiannidis, Panagiotiset al. [2] proposed a rule-based anomaly detection system. This proposed system helps to monitor and detect the Sybil attacks in wireless sensor network. This rule based system depends on the ultra-wideband (UWB) ranging-based detection algorithm which operates in a distributed. The result indicates that the proposed algorithm attains high detection accuracy and low false alarm rate.

Wang, Jiangtao, Geng Yanget al. [3] a new method of Sybil attack detection in wireless sensor network (WSN) has been presented which is depending on received signal strength indication (RSSI). This process employed Jakes channel model by emulating real network space situation of sensor network. In this paper two ways are discussed to verify the raised efficiency and refinement of Sybil attack. The process attains the detection rate and provides several applications.

Lu, Aidong, Weichao Wanget al. [4] in this paper, a robust intrusion detection approach has been proposed for wireless sensor networks that is depending on a new multi-matrix visualization method with a set of pattern generation, evaluation, organization and interaction functions. The results indicates that the proposed detection approach can detect the Sybil attacks under distinct parameters

Piro, Chris, Clay Shieldset al. [5] In this paper, detection mechanism has been proposed which indicates the mobility which may be enhance the security. Particularly, the proposed scheme indicates that nodes can monitor traffic in the network and can locate a Sybil attacker that uses a number of network identities simultaneously.

Ghose, Sarbani et al. [6]in this paper omnipresent wireless medium provides high mobility, yet the very nature of open medium introduces vulnerability. Earlier designs of security mechanisms concentrated more on the upper layers, but physical layer techniques have recently gained popularity. Security is taken care of by maximizing the information rate of the signal sent from the source to the receiver, with an assumption that the eavesdropper's channel is worse than the main channel.

Douceur, John Ret al. [7] in this paper, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements.

Demirbas, Murat, and Youngwhan Songet al. [8] proposed a robust and lightweight solution for sybil attack problem depending on received signal strength indicator (RSSI) readings of messages. The results of this proposed approach is robust as it locates all the sybil attacks. The performance indicates that the proposed approach is unreliable and time varying and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems.

VI. PROPOSED METHODOLOGY

In order to solve the problem of security in wireless sensor networks, a hybrid approach is used. The hybrid approach is a combination of Fuzzy algorithm and the K- means classification algorithm. The fuzzy approach is used to create a relationship between the attributes and the labels (source node and targeted node) on the basis of objective function. The K-means algorithm computes the mean value of the distance between the nodes and shifts the solution towards the calculated value. The combination of both the approaches helps in detecting the Sybil attack. The objective function used in the calculation can be computed as

$ff = \sum w_1.R_i + w_2\, .E_j + w_3.D_{i,j}$

Where R_i is the range of the source node

$E_j$are the residual energy of the target nodes and

$D_{i,j}$ is the distance between the source and the target node

The distance between the nodes is calculate using the Euclidian distance formula which is given by

$$D_{i,j} = \sqrt{((x_1 - x_2)^2 + (y_1 - y_2)^2\,)}$$

Where $x_i and\ y_i$are coordinates of a node.

Fig 1 shows the flow diagram of the proposed approach.

VII. HYBRID APPROACH

In order to solve the problem of security in wireless sensor networks, a hybrid approach is used. The hybrid approach is a combination of Fuzzy algorithm and the K- means classification algorithm.

Fuzzy Algorithm is a approach based on degrees of truth rather than 0 or 1. It is used to create the relationship between the attributes and labels and differentiate them on the basis of objective function value. The objective function is calculated on the basis of various node parameters stated in the further sections

VIII. CONCLUSION

Security related application in Wireless Network are the major area of concern in recent years. Many approaches have been proposed for various types of attacks in the network. In the proposed approach a hybrid of Fuzzy and K-means classification is proposed which detects and works against the Sybil attacks. The proposed methodology is implemented using NS2 and the results shows that the proposed approach outperforms the basic approach by a significant value. The comparison parameters are end to end delay, packet delivery ratio and the throughput of the network and the approaches are compared against the simulation time. In future other machine learning approaches must be proposed and compared with the existing approaches.

REFERENCES

[1] Karapistoli, Eirini, and Anastasios A. Economides. "ADLU: a novel anomaly detection and location-attribution algorithm for UWB wireless sensor networks." *EURASIP Journal on Information Security* 2014, no. 1 (2014): 1-12.

[2] Sarigiannidis, Panagiotis, Eirini Karapistoli, and Anastasios A. Economides. "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information." *Expert Systems with Applications* 42, no. 21 (2015): 7560-7572.

[3] Wang, Jiangtao, Geng Yang, Yuan Sun, and Shengshou Chen. "Sybil attack detection based on RSSI for wireless sensor network." In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pp. 2684-2687. IEEE, 2007.

[4] Lu, Aidong, Weichao Wang, Abhishek Dnyate, and Xianlin Hu. "Sybil attack detection through global topology pattern visualization." *Information visualization* 10, no. 1 (2011): 32-46.

[5] Piro, Chris, Clay Shields, and Brian Neil Levine. "Detecting the sybil attack in mobile ad hoc networks." In *Securecomm and Workshops, 2006*, pp. 1-11. IEEE, 2006.

[6] Ghose, Sarbani, and Ranjan Bose. "Physical layer security in UWB networks." In *Microwaves, Communications, Antennas and Electronics Systems (COMCAS), 2011 IEEE International Conference on*, pp. 1-5. IEEE, 2011.

[7] Douceur, John R. "The sybil attack." In *Peer-to-peer Systems*, pp. 251-260. Springer Berlin Heidelberg, 2002.

[8] Demirbas, Murat, and Youngwhan Song. "An RSSI-based scheme for sybil attack detection in wireless sensor networks." In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, pp. 564-570. IEEE Computer Society, 2006.