Comparative Analysis of Flooding and Jamming Attacks in Wireless Sensor Networks

Shikha Jindal[1], Raman Maini[2]
[1]Research scholar, Master of Technology, Department of Computer Engineering, Punjabi University Patiala
[2]Professor, Department of Computer Engineering, Punjabi University Patiala

***Abstract* - In the development of the computer networks Wireless Sensor Network (WSN) plays an important role. In recent time, there are many out-of-doors applications like medical and military examination in which wireless sensor networks (WSNs) have been generally used. Therefore it is important to give surety up to the required level of security. Due to some weaknesses like limited processing capability, memory, and because of the broadcast transmission medium Wireless Sensor Networks are mostly susceptible to Denial of Service attacks like jamming and flooding. Since sensor nodes are very resource controlled so security is one of the primary issues in sensor networks. In this paper, we have done comparative analysis of flooding and jamming attack in wireless sensor networks using NS2 simulator. In analysis we found that jamming attacks are harder to detect as compared to flooding attacks because jamming attacks targets or jams a particular region or area.**

Keywords: Denial of service, Flooding, Jamming, Network security, Wireless Sensor Networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are collection of small and cheap sensor nodes which examine the environment. They have some special characteristics like low power utilization, limited processing power and small radio range [1].

WSN are used in many applications and some serious applications such as medical and military applications have need of a high level of security. Sensitive data generated by the sensor network must be protected against unauthorized access or from attackers to prevent unwanted changes. The level of security is defined in terms of requirements, such as confidentiality (preventing the disclosure of information), integrity (prevention of modification), availability (services will be accessible), authenticity (confirming the identity of a person), freshness (message is new, not a replay message) and non-repudiation (used to settle disputes about the occurrence or non-occurrence of an event) [1].
Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network's capacity to perform its expected function [3].

WSNs are especially sensitive to Denial-of-Services Attacks (DoS) such as jamming and flooding because of resource constraints on the sensor node. [2]. Flooding distributed denial of service attacks are launched by multiple attackers or zombies by sending large traffics to the network that is able to bring a network or a service down [12]. In jamming attack an attacker jam the area i.e. Sending and receiving frequencies are jammed or distorted and they cannot sent or receive messages from each other [6].

Because of various resource constraints in WSN providing security is a difficult task. First, sensor nodes generally have limited resources like - battery power, memory, energy and insecure communication medium. Second, sensor nodes are generally deployed unfriendly background and are built without any intrusion detection and avoidance in mind [4].

In this paper in section II an explanation of different DoS attacks, their effects and defense mechanism at each layer is given and then in section III related work survey is done on some existing methods of flooding and jamming attacks. In section IV and V we discuss flooding and jamming attack and their types and their defense mechanism. In section VI a comparative analysis is done on flooding and jamming attack.

II. DENIAL OF SERVICE ATTACK

As compared to Internet, Denial-of-Service attacks targets wireless sensor networks in different way i.e. each layer of the Wireless Sensor network is susceptible to different DOS attacks and has different effect on the network and different defense mechanisms are available for each attack. Different types of DoS attacks on each layer of network are explained as follows: [2].

A. The physical layer

In physical layer, we have two types of attacks i.e. jamming and tampering. Jamming is a type of attack in which attacker send radio frequencies which interferes with the frequencies used by sensor node. Another physical layer attack is tampering. In this attack, sensitive information such as keys used for encryption/decryption or other data can be extorted by the attacker.

B. *The data link layer*

In link layer, there are three types of attacks i.e. collision, exhaustion and denial of sleep. Collision attacks, attacker disturbs the data transmission in WSN by dropping and reordering the packets more frequently. In exhausting floods, communication links are flooded by attacker and make

packets drop. In denial of sleep attacks an attacker keep the sensors busy with fake messages or empty packets so that sensor remains in on mode as much as possible. By keeping the sensor in on mode, it prevents them to go to sleep mode and uses up the battery. Once the battery is used up the sensor goes down.

C. The network layer

In network layer, there are three attacks spoofing, replaying, hello floods and Sybil. In spoofing replaying an attacker generate fake error messages in order to disturb traffic in the network.
Hello flood exploits Hello packets that are used to affirm nodes to their neighbors. In this, attacker overwhelms the node with hello packet requests and congests the network. In Sybil attack, multiple identities are presented by a single sensor node to other nodes in the WSN. This may misinform other nodes, and hence routes believed to be using disjoint node can have the same adversary node presenting a variety of identities.

D. The transport layer

In Transport layer, there are two attacks i.e. flooding and de-synchronization. In flooding attack, attacker floods the network with fake packet requests so that network comes to halt position.
In Desynchronization attack, attacker disrupts the communication by making the sensor node busy in recovering from those errors that are never existed. It wills ultimately wastage of energy of sensor nodes.

E. Application layer

Finally in the application layer, we have the DoS attacks. Since WSNs are intrinsically weak, an attacker can easily deny the service by sending fake empty messages endlessly on the receiving sensor node and this will make it down. Other application layer attacks are Deluge or reprogramming attacks. These attacks are done by specialized insiders. In this attack they send their own encoding using legitimate communication to certain sensors, and this code is like a virus which replicates itself all the way through the network which leads the networks to a halt state [1, 2, 5, 6, and 7]. Table.1 has illustrated the main DoS attacks in different layer of WSNs.

TABLE I

Network layer	DDoS attacks ,effect and defense		
	Attack	Effect	Defense
Physical	Jamming	Interrupt the entire network and blocks the path between sender and receiver.	Spread-spectrum, priority of messages, lower duty cycle, mapping of region , change of mode
	Tampering	Can extract sensitive information such as cryptographic keys or other data on the node.	Tamper-proofing, hiding
Data link	Collision	Packet discarded as invalid.	Error-correcting code
	Exhaustion	Exhaustion of network resources	Rate limitation Anti-replaying
	Denial of sleep	Drain the battery by keeping sensor node busy.	
Network	Spoofing, replaying	Generate fake error messages to disrupt traffic in the network.	Authentication anti-replay
	Hello floods	Overwhelm the node with hello packet requests.	authentication
	Sybil	Mislead other nodes by presenting identities of multiple nodes.	unique shared symmetric key
Transport	Flooding	All available resources are used up and cause DoS.	Client puzzles, Rate Limitation
	Desynchronization	Cause drainage of energy of legitimate nodes.	Authorization
Application	DoS	Deny the service by sending fake messages.	Anti-replay
	Deluge	Attackers send their own programming messages and the network is completely taken over by the attackers.	Authentication

III. RELATED WORK

There are many studies aim to solve the problem how to keep sensor network's security from flooding and jamming attacks.

The authors have described a novel method not just only to detect jamming attacks but distinguish which type of jamming attacks [8]. Jamming attacks are one of the most widespread attacks. In this author gives some detection mechanism like signal strength and packet delivery ratio. But this mechanism does not distinguish its various types. So to distinguish its types author explains a new mechanism i.e. packet send ratio.

The authors represented SPREAD (Second-generation Protocol Resiliency Enabled by Adaptive Diversification) [9]. This technique is used against reactive jammers. Reactive jammers corrupt the transmission with a high rate. So to prevent those disruptions, a more efficient technique is explained by author in this paper.

The author has described a method [10] that helps to detect the flooding attack caused by a single attacker or multiple attackers. He also explains trace back mechanism to detect the source of attack. This method of calculating entropy variation is more efficient as compared to other methods.

In this paper, [11] author tells that Flooding-based distributed denial-of-service (DDoS) attack are dangerous attacks against the stability of the Internet. This paper gives a review of various flooding attack methods. Then tells about their defense mechanism and compare them to check the effective method. Author also explains firewall approach to defend against flooding attacks.

TABLE II

Proposed method in	Comparison of some existing methods	
	Advantages	Disadvantages
[8]	Distinguishing process between the different types helps in counter measurements selection. As in defense strategies, competition strategies specifically are more effective if the jamming mode is known.	This method of detection and differentiation is very slow in effectively taking action against the jamming. As only, after the damage is quite apparent can the sensors counter act.
[9]	It is less complex and more efficient than other methods like spectrum spread. SPREAD framework utilizes the same hardware, only needs fundamental protocol changes and implementations.	Only effective in defending against smart jammers.
[10]	Calculating the entropy variations improves the detection efficiency compared to any other methods.	This detection method is only used for near the victim perspective. It is not used for near attack sources and with in transit network perspective.
[11]	Effective detect and filter approach.	It is not very useful for DDoS attacks of very short durations.

IV. FLOODING ATTACK

Flooding distributed denial of service attacks are the most commonly occurring attacks, launched by various attackers by sending a large amount of packets i.e. through the action of sending fake messages and this will cause congestion in the network. Due to this congestion, network resources are used up and network performance comes to halt. Due to this attack, consistency and usability of the services of the Internet is highly intimidated [12].

A. Types of flooding attack

There are two types of flooding attacks: direct attacks and reflector attacks.

A.1). Direct attack: In this attack, an attacker sends a large number of attack packets with the help of a single source or multiple sources directly toward a victim. It is of three types which are explained as: [11].

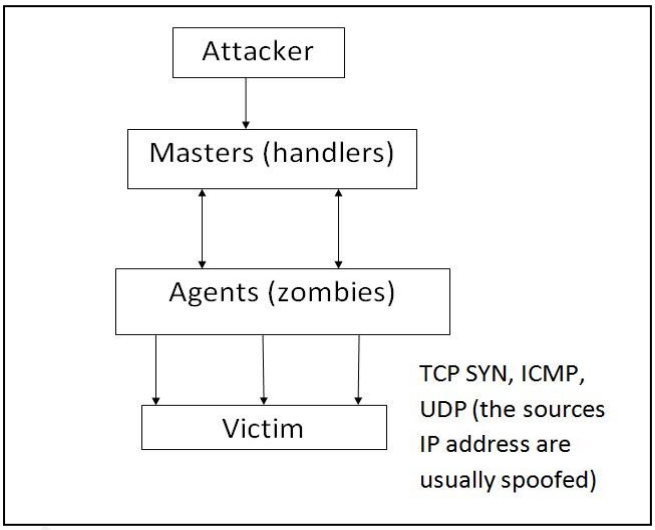

Fig. 1. Direct attack [11]

A.1.1). TCP SYN Flooding: TCP SYN flooding is one of most frequently occurring attacks and had an extensive impact on many systems. In a normal TCP connection when a client wants to establish a connection the server then he starts by sending a SYN message to the server and then responds by sending SYN_ACK message to the client. The client completes the connection by responding with an ACK message. Now a complete connection is set up between client and server and they can exchange messages with each other. This is called three way handshake process. The misuse arises at the half-open state when the server is waiting for the client's ACK message after sending the SYN-ACK message to the client. The server allocates memory for these half open connections till the server receive the final acknowledgment message or the half open connection expires. Attacker can easily spoof source IP addresses and can create half open connections by ignoring SYN-ACKs. The result is that final ACK message will never be sent to the server. Because the server generally only allocates a limited size of space in its process table, too many half connections will soon fill the space and the server becomes congested and cannot accept any new incoming connection. Although these half connection will expire in the end due to time out, but attacker send theses spoofed TCP SYN packets requesting connections at a much higher rate than the expiration rate [12,13].

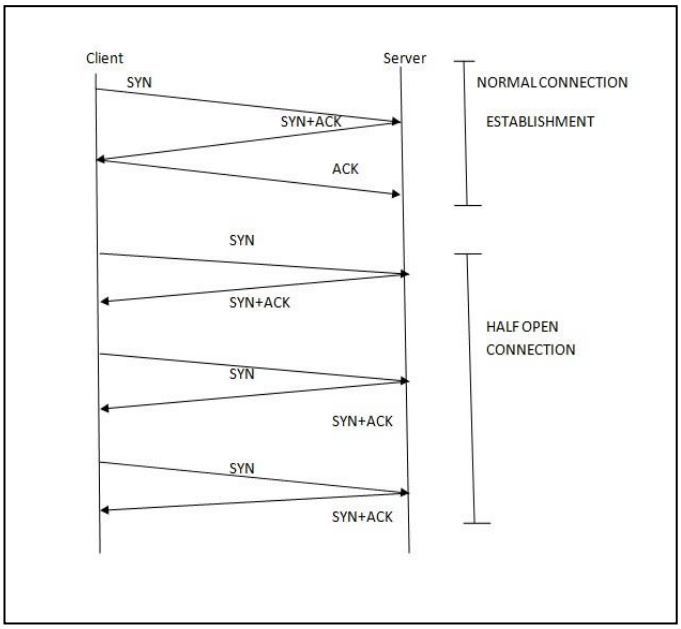

Fig. 2. Normal TCP connection and half open connection [15]

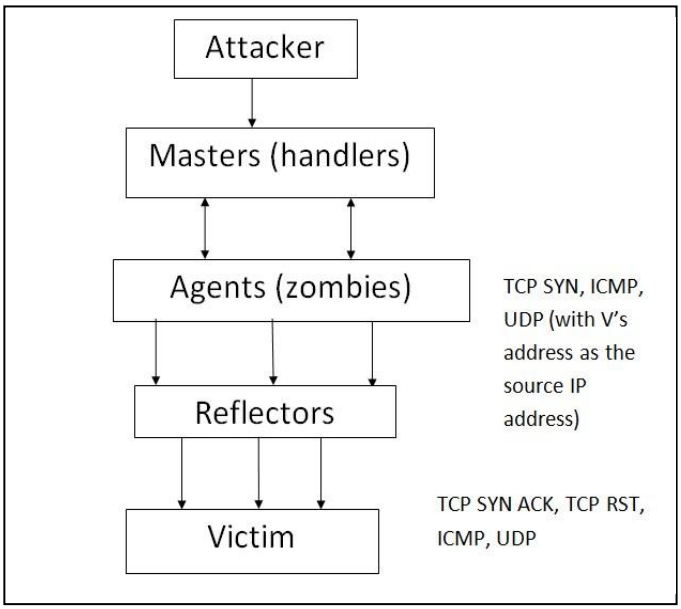

Fig. 3. Reflector attacks [11]

A.1.2). ICMP Smurf Flooding: ICMP is often used to find out that computer in the Internet is responding or not. To accomplish this task, an ICMP echo request packet is sent to a computer. After receiving the request packet, then an ICMP echo reply packet is sent by the computer. In this attack, attacker sends fake ICMP echo requests having the victim's address as the source address and the broadcast address of these remote networks as the destination address. If the firewall is not able to filter these forged packets then they will be broadcast to all computers on the network. Then these computers will send ICMP echo reply message to the source address which is the address of victim carried in the request packet. The victim's network is now comes to halt state [12, 13].

A.1.3). UDP Flooding: in this attack, attackers merely send a large amount of UDP packets towards a victim. Since an intermediate network can distribute large amount of traffic than the victim network can handle, the flooding traffic will use up the all resources of the victim's. Pure flooding can be done with any type of packets. Attackers can also send a large number of service requests which are not handle by the victim with its limited resources [12, 13].

A.2). Reflector attack: A reflector attack is an indirect attack in which there are some intermediary nodes called reflectors are used to launch attack. An attacker sends packets to the reflectors having victim's address as the source address. Reflectors didn't know that the packets are actually address-spoofed; the reflectors return these packets to the victim according to the types of the attack packets. As a result, the attack packets are effectively reflected, to the victim in the form of normal packets, if there are a large number of reflectors then these reflected packets can flood the victim's communication link and this will bring the network in a congested state [11].

B. DEFENSE MECHANISM

B.1). INGRESS/EGRESS Filtering: if INGRESS/EGRESS filtering mechanism is used then it becomes difficult for attackers to launch flooding attacks using spoofed IP address. In this mechanism, there is a firewall which connects the network to the internet thorough interfaces. Some interfaces of firewall are connected to the internal network and some are connected to internet. The firewall applies ingress filtering on the external interfaces and drops all those packets whose source address belongs to internal network because they are spoofed. If those spoofed packets are allowed to pass in to the network then the attacker can pretense as a host in the network. The firewall applies egress filtering on the internal interfaces i.e. on those packets which are coming out of the network. The firewall drops all those packets which do not belong to the network. In this way this filtering mechanism stops an attacker to cause flooding attack. If these two methods are deployed all over the internet then we can stop all attacks that are based on IP spoofing. This method is efficient only when the load on routers is very less [16].

B.2). IP trace back: IP trace back method is used to find out source of attacks. It is the process of tracing back the route of fake IP packets to find out the true source address rather than the spoofed IP address that was used in the attack [16]. Three ways of doing IP trace back are as:

B.2.1). Link testing scheme: Trace back process start from that router which is closest to the victim and check its upstream links until they did not find that which router is used to bring the traffic of the attacker. This process is repeated recursively on the upstream router until we cannot get the source router. This process can be executed if the attack is active until the trace is not completed and this technique is not

suitable for those attacks that are detected after the attack. Link testing mechanisms work best only if the attacking source is single and give bad results if there are multiple attackers or there is DDoS attack [17].

B.2.2). Packet marking schemes: In packet marking scheme, when each router forwards a packet then also inserts a mark in the packet. This mark is a unique identifier related to that particular router. As a consequence the victim can find out all the intermediate hops for each packet by observing the inserted marks. But the limitation is that routers are slowed down because they have to do additional work [16].

B.2.3). ICMP trace back message: In this technique routers send newly anticipated ICMP messages to the destination, which also contains information about the previous router. With the help of this scheme we can reconstruct the path but only when multiple packets are forwarded. Overhead is less in this technique as compared to other two techniques [16, 17].

B.3). Rate limiting mechanism: Rate limiting mechanism limit the rate of packet arrivals. This mechanism only limits the rate of flooded packets caused by attacker and do not harm normal traffic. There is no extra overhead of this mechanism as compared to other two. But rate limiting mechanism is not as good as filtering approach. This mechanism is to be used only when we know that the detection process gives many false positives, then it is better to use rate limiting [16].

C. *METRICES*

The false positive ratio (FPR) and false negative ratio (FNR) metrics are used to check effectiveness of the attack detection and filtering technique.

1). False positive ratio (FPR): The FPR is given by the number of packets classified as attack packets (positive) by a detection system that are confirmed to be normal (negative), i.e. false classification done by the detector divided by the total number of confirmed normal packets [11].
If x is the number of packets classified as attack packets that are confirmed to be normal and y is total number of confirmed normal packets, then FPR is calculated using (1).

$$FPR=x/y \quad (1)$$

2). False negative ratio (FNR): The FNR, on the other hand, is given by the number of packets classified as normal (negative) by a detection system that are confirmed to be attack packets (positive), divided by the total number of confirmed attack packets.
If m is the number of packets classified as normal those are confirmed to be attack packets and n is the total number of confirmed attack packets, then FNR is calculated using (2).

$$FNR=m/n \quad (2)$$

An effective DDoS attack detection and filtering technique gives very low ratios [11].

V. JAMMING ATTACK

Jamming is defined as the emission of radio signals which interferes with the transceivers signal and disturbs the communication. In this attack, attacker jams a particular area so that sender and receiver cannot exchange messages with each other. In WSNs, The main difference between jamming and radio frequency interference (RFI) is that jamming is done intentionally and a specific target is set to disrupt the transmission while the RFI is done unintentionally, due to some nearby transmitters that transmit signals in the same or very close frequencies [6].
Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. Wood and Stankovic define DoS attack as "any event that diminishes or eliminates a network's capacity to perform its expected function" [14].

A. *Types of jamming attack*

There are four types of jamming attacks.

1). Constant jamming: In constant jamming, attacker continually emits random and meaningless radio signal to the channel, so that channels are jammed. Sensors cannot send data if the channel is busy i.e. they can send data only when the channel is idle. But when the sensors are constantly jammed they can't send or receive data with another node [8, 14].

Fig. 4 constant jamming [18]

2). Deceptive jamming: In this the attackers don't send random data, but will send a nonstop stream of legitimate packets, which means a legitimate packet header but with no payload or ineffective payload, to the channel. This continuous stream prevents the receiving sensor to go to sleep and energy of node is wasted. There is no gap between the forged packets send by the attacker [8, 14].

Fig. 5 Deceptive jamming [18]

3). Random jamming: This attack alternated between constant jamming attack and deceptive jamming attack. This type of attack either applies constant jammer or deceptive jammer to jam the signal for some period and then they go to sleep for another period. This saves the energy. The main profit of this jammer is that it requires very less power and processing resources, but timings should be chosen carefully to get effective jamming results [8, 14].

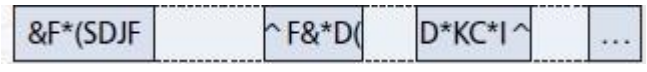

Fig. 6 Random jamming [18]

4). Reactive jamming: This jamming attack is hardest to sense and put into operation. As all previous jamming types are active this is reactive. In this attack, attacker remains quiet

until there is some activity on the channel and then interfere when the data is about to be sent. This attack will target at the receiver. In this attack, attacker have to sense channel again and again so it waste more energy on sensing the channel whereas a less amount of energy is needed to destroy the transmission signal [8, 14].

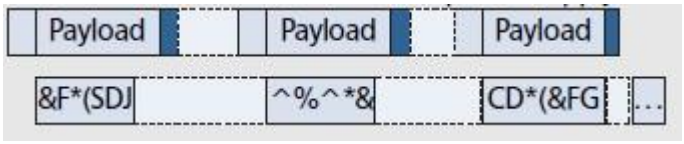

Fig. 7 Reactive jamming [18]

B. *Detection Mechanisms*

1). Signal strength: Signal strength (SS) is first method to detect jamming. With the help of this method we can detect jamming signals from the legitimate signals. If the jamming is present in certain region then signal levels are generally high in that area as compared to signal levels that are without jamming.

2). *Carrier sensing time*: sometimes, the channel might appear all the time busy to the source due to which jammer can stop a genuine source from sending out packets In this case we have to constantly check the amount of time taken by the channel to become idle i.e. the carrier sensing time, and compare it with the time taken by the channel under normal traffic operations to check that whether it is jammed or not.

3). Packet delivery ratio: It is the ratio of packets that are successfully decrypted by destination compared to the number of packets that are actually sent out by the sender. This is used to detect jamming attack in some particular region. If the jamming attack is present then packet delivery ratio is below average and it is drops to zero if the channel is completely disrupt by the jammer [6].

C. *Jamming detection with consistency checks*

Basically, two thresholds are used in consistency checks. Threshold is a boundary beyond which a radically different state of affairs exists. Threshold1 is for the signal strength value, and the PDR which are used to detect jamming. Threshold2 is about PSR, which is used to distinguish which type of jamming attack is applied on the channel.

Step 1: signal strength consistency checks: In the first step, it checks PDR is below threshold1or not, if yes; it checks the signal strength is below threshold1 or not. If no then no jamming had occurred, just interference or noise. If yes then jamming is detected, and the channel is under one of the four types of jamming [8].

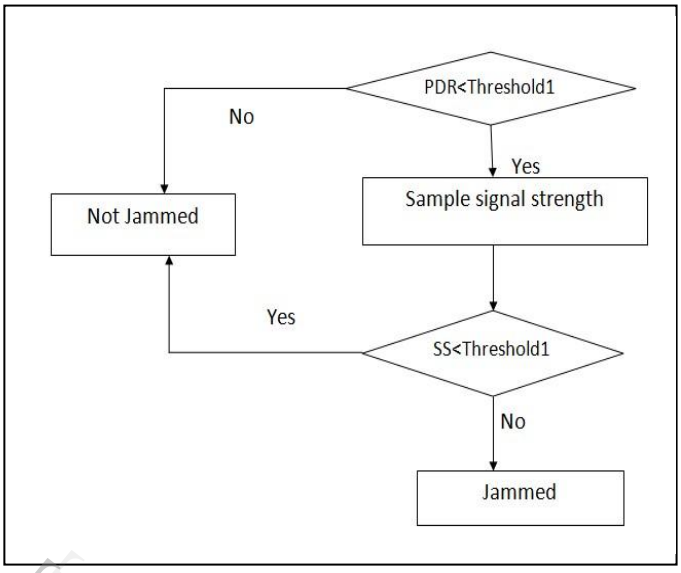

Fig. 8. Signal strength consistency check [8]

Step 2: PSR consistency checks: Second step is to check the PSR with threshold2; if PSR is above threshold2 then it is either reactive jamming or random jamming. If PSR is below threshold2 then it's either deceptive jamming or constant jamming. In reactive jamming PSR is very high, above 60% whereas in random jamming, PSR is below 60% but above threshold2. If PSR is, zero then its deceptive jamming. But, if it is under threshold2 but not zero then it is constant jamming [8].

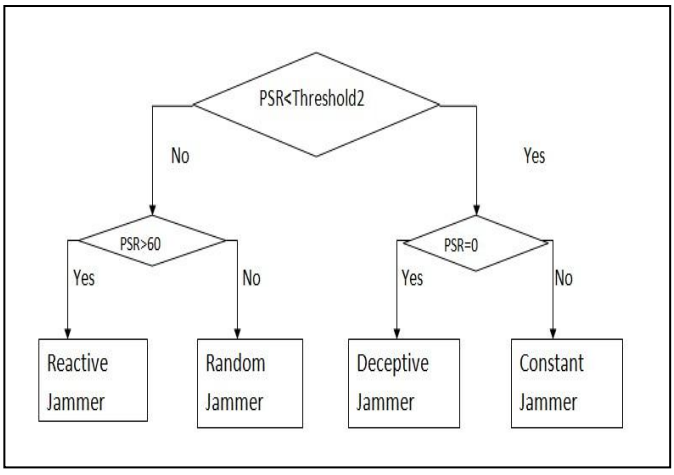

Fig. 9 PSR consistency checks [8]

D. METRICS

There are two metrics to check effectiveness of detection mechanism i.e. PSR and PDR.

1). Packet send ratio (PSR): It is the ratio of packets that are truly sent into the channel from a node compared to number of packets that are proposed to be sent into the channel [8].
If sender wants to send out 'q 'messages, but only 'p' of them go, then PSR is calculated using (3).

$$PSR = p/q \quad (3)$$

2).Packet delivery ratio (PDR): It is the ratio of packets that are successfully decrypted by destination compared to the number of packets that are actually sent out by the sender [8].
Even after the 'p' messages are sent out by sender, receiver is able to decipher only 'r' packets correctly, and then PDR is calculated using (4).

$$PDR=p/r \quad (4)$$

If no packets are received by receiver, then PDR is equal to 0.

VI. COMPARISON OF FLOODING AND JAMMING ATTACKS

TABLE III

Parameters	Comparison of flooding and jamming attacks	
	Flooding	Jamming
1. Definition	Flooding is a Denial of Service (DoS) attack that is designed to bring a network or service down by flooding it with large amounts of traffic.	Jamming attacks are representative energy consumption DoS attacks in WSN. The attacker deploys the jammers randomly to jam the area. A jammer prevents the sender from sending out packets or prevents the receiver from receiving packets.
2. Types	TCP, ICMP, UDP, or a mixture of them	Constant jamming, Deceptive jamming, Random jamming, Reactive jamming
3. Layer	It is done at physical layer.	It is done at transport layer.
4. Effect	All available resources are used up and cause DoS.	Blocks the path between sender and receiver.
5. Defense/ detection mechanism	INGRESS/EGRESS Filtering, IP trace back, Rate limiting mechanism	Signal strength, carrier sensing time, packet delivery ratio
6. Metrics	False positive rate, False negative rate	Packet sent ratio, packet delivery ratio

VII. CONCLUSION

Wireless sensor networks are widely used in various civilian, industrial, scientific, medical and military applications. As we are more dependent on such networks we cannot afford to compromise the availability and security of such networks. Due to the low cost design of sensor nodes and the simplicity with which they can be easily reprogrammed, security issues arises and sensor networks will be vulnerable to flooding and jamming types of attacks. Due to large dependency on these networks, there is a need for the detection of these attacks rapidly and perfectly.
In this paper, we have discussed two attacks flooding and jamming. In flooding attack, we explain its types and how they affect sensor networks. Then we propose some defense mechanism to prevent flooding attack. There are two metrics in flooding attack to check effectiveness of detection mechanism i.e. false positive ratio and false negative ratio. Detection accuracy is high if the ratio is low. In jamming attack also we explain types and detection mechanism. In jamming metrics used to check effectiveness are packet send ratio and packet delivery ratio. Detection mechanism is more effective if the PSR and PDR ratio is high. Then we have done a comparative analysis of both attacks. Finally we analyze that jamming attacks are harder to detect as compared to flooding attacks. After detecting jammed area we have to also find out type of jamming attack also.
Finally, in the future we anticipate that WSN, are designed with security in mind so that they didn't lack in security. As more secure WSN will be in the future, more possibilities and applications are sure to use WSNs.

VIII. ACKNOWLEDGMENT

The authors would like to acknowledge the Department of Computer Engineering, Punjabi University Patiala, for the facilities provided during this research.

REFERENCES

1. Razvan Rughini, Laura Gheorghe" Storm Control Mechanism in Wireless Sensor Networks" published in 9th RoEduNet IEEE International Conference 2010
2. Ouyang Xi, Tian Bin, Li Qi, Zhang Jian-yi , Hu Zheng-Ming, Xin Yang "A Novel Framework of Defense System Agaist DoS Attacks in Wireless Sensor Networks**"** published in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference.
3. A. D. Wood and J. A. Stankovic, "Denial of Service in sensor networks", in Computer, vol.35, no.10, pp.54-62, 2002
4. Boris Mihajlov and Mitko Bogdanoski " Analysis of the WSN MAC Protocols under Jamming DoS Attack" published in International Journal of Network Security, Vol.16, No.4, PP.304-312, July. 2014
5. Tian Fu" modeling and simulation of jamming attacks in WLAN"thescholarship.ecu.edu/bitstream/handle/.../Fu_ecu_0600M_10649.pdf?
6. Abdulaziz Rashid Alazemi "Defending WSNs Against Jamming Attacks, American Journal of Networks and Communication" published in Vol. 2, No.2, 2013, pp. 28-39. doi: 10.11648/j.ajnc.20130202.12
7. Huda Bader Hubboub" Denial of Service Attack in Wireless Sensor Networks" library.iugaza.edu.ps/thesis/92125.pdf
8. Le Wang and Alexander M. Wyglinski " A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks" In the Proceedings of the Conference on Communications,

Computers and Signal Processing Pacific Rim, pp.809-814, 23-26 IEEE, Aug. 2011.
9. Xin Liu, Guevara Noubir, Ravi Sundaram, San Tan, "SPREAD: Foiling Smart Jammers using Multi-layer Agility" IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings, IEEE 2007.
10. K Munivara Prasad, Dr A Rama Mohan Reddy, Dr K Venugopal Rao "An Efficient Detection of Flooding Attacks to Internet Threat Monitors (ITM) using Entropy Variations under Low Traffic" published in Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference
11. Rocky K. C. Chang," Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial" in IEEE Communications Magazine • October 2002
12. Khadijah Wan Mohd Ghazali and Rosilah Hassan "Flooding Distributed Denial of Service Attacks-A Review" in Journal of Computer Science 7 (8): 1218-1223, 2011 ISSN 1549-3636 © 2011 Science Publications
13. Qijun Gu, Peng Liu" Denial of Service Attacks" s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf
14. Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou" A Survey on Jamming Attacks and Countermeasures in WSNs" in IEEE communication surveys and tutorials, VOL. 11, NO. 4, fourth quarter 2009
15. Ahmad Sanmorino1, Setiadi Yazid2 "DDoS Attack Detection Method and Mitigation Using Pattern of the Flow" in 2013 International Conference of Information and Communication Technology (ICoICT)
16. Puneet Zaroo "A Survey of DDoS attacks and some DDoS defense Mechanisms" P Zaroo - Advanced Information Assurance (CS 626), 2002 - users.cs.jmu.edu
17. Stefan Savage, David Wetherall, Member, IEEE, Anna Karlin, and Tom Anderso " Network Support for IP Traceback" in IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 9, NO. 3, JUNE 200
18. Wenyuan Xu, Wade Trappe, Yanyong Zhang, "Jamming Sensor Networks: Attack and Defense Strategies" Published in *IEEE Network*, Volume 20, Issue 3, Spring 2006, pages 41-47.