Efficient early detection technique of DDoS in Wireless Network

A.Saraswathi,
Research Scholar & AssistantProfessor,
P.G. and Research Department of Computer Science, Government Arts College (Autonomous),
Karur, Tamil Nadu, India

Dr.K.Thangadurai,
Assistant Professor,
P.G. and Research Department of Computer Science,
Government Arts College (Autonomous),
Karur, Tamil Nadu, India.

***Abstract*- In recent wireless communication has become more fashionable because of its agility. For making wireless network, no need of large and complex physical establishment and can connect using radio waves. But on the other hand it increases the chance for unauthorized users to misuse. The unauthorized access is called intrusions. DoS (Denial of Service) attacks are dangerous attacks which send extreme amount of fake packets in order to squash and make congest in the network. In this paper describes the early detection techniques of DDoS attack in WSN and this paper analysis the technique which is prevented the DDoS attack as performance scheme. It has been seen the basis of throughput, Number of data packets transferred and packet delivery ratio.**

Keywords: Wireless Network, Intrusion Detection System, DDoS, Packet delivery ratio, Data packets, Throughput

1. INTRODUCTION

A wireless network uses high frequency of radio waves. It may consists of access point (AP) and hardware devices which allows wireless communication enabled devices to connect to the network mostly called infrastructure based network and network without any physical setup is known ad-hoc network. Now-a-days the knowledge of ad-hoc network is immensely applied in WSN. Sensor nodes are simple, constrained in energy, processing power, memory, and communication capabilities. Figure 1 presents the overall scenario of proposed intrusion detection system.

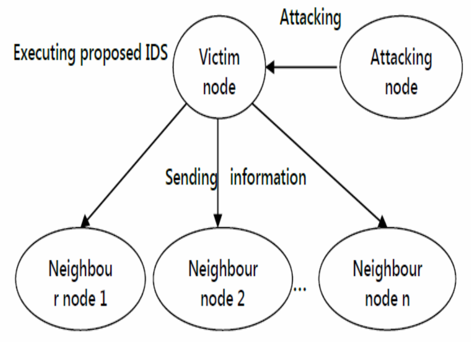

Figure 1. Overall Presentation of IDS

Layered network architecture can develop stoutness by restricting layer interactions and interfaces. Each layer is susceptible to different DoS attacks and has diverse options obtainable for its defense. Some attacks crosscut numerous layers or utilize communications between them.

Physical Layer:

Nodes in a sensor network exploit wireless communication because the network's ad hoc, large-scale deployment formulates anything else unfeasible. Base stations or uplink nodes can exploit wired or satellite communication, but limitations on their mobility and power make them more inadequate.

Table 1. depicts the layers of a typical sensor network

Layer	Attacks	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding
Link	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Neglect and greed	Redundancy, probing
	Homing	Encryption
	Misdirection	Egress filtering, authorization, monitoring
	Black holes	Authorization, monitoring,

		redundancy
Transport	Flooding	Client puzzles
	Desynchronization	Authentication

Link Layer:

The link or media access control (MAC) layer affords channel adjudication for neighbor-to-neighbor communication. Supportive schemes that rely on carrier sense, which let nodes identify if other nodes are transmitting, are particularly susceptible to DoS.

Network Layer:

Superior layers may not need fully consistent transmission streams, but the network layer provides a critical service nevertheless. In a large-scale deployment, messages may pass through many steps before reaching their destination. Unfortunately, as the cumulative network cost of relaying a packet increases, so does the probability that the network will plummet or misdirect the packet along the way. The nonexistence of pre-existing infrastructure in sensor networks means that most if not all the nodes will provide as routers for through traffic. Since each node is potentially a router and it adds fresh vulnerabilities to the network-layer harms veteran on the Internet. Routing protocols must be simple enough to scale up to large networks, yet vigorous sufficient to cope with failures that arise many hops away from a source.

Transport Layer:

This layer handles end-to-end associates. The layer supply's can be as simple as an changeable area-to-area any cast, or as complex and costly as a trustworthy sequenced-multicast byte stream. Sensor networks have a tendency to use simple protocols to diminish the message overhead of acknowledgments and retransmissions. Protocols that afford sequencing share several DoS vulnerabilities with the Internet transmission control protocol.

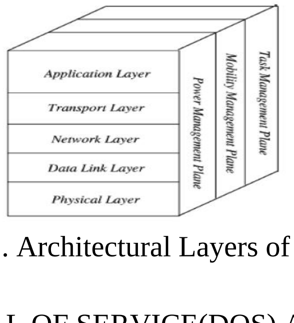

Figure 2. Architectural Layers of a WSN

2. DENIAL OF SERVICE(DOS) ATTACKS

DoS attacks can be categorized into three types:

1. Consumption of scarce, limited or non-renewable resources.
2. Destruction or alteration of configuration information.
3. Physical destruction or alteration of network resources.

DoS attack targets network resources. The hardware of sensor nodes is classically inhibited and attackers can try to excess them. The DoS attack is one of the most important energy expenditure attacks in WSN. DoS attacks are reliant on the vulnerabilities of every layer in the layered architecture of wireless networks. The physical layer is lowest layer and it attacked by jammers. This physical layer is responsible for carrier frequency generation, frequency selection, modulation, signal detection and data encryption. As an outcome of DoS attack, the sensor node fails to task when the energy is worn out. Sensor nodes are susceptible against this type of physical attack. DoS attacks are very grave such as jamming attack and tinker attack. Jamming is the intentional intrusion of the wireless communication channel. Tampering is another type of physical attack, which targets the tangible hardware of the sensor nodes. In this attack, it is complex to know whether any exacting DoS situation is caused deliberately or unintentionally. The WSN's denial of snooze attack is a subset of the Denial of Service class of network attacks.

3. LITERATURE REVIEW

R.Ragupathy and Rajendra Sharma et.al proposed to detect intrusions by analyzing the network traffic pattern against suspicious pattern. The proposed model was implemented in three different systems of virtual pc environment. Two of them were considered as authorized system and one as an intruder system. The intruder was had windows xp or ubuntu operating system. The victim node has windows 7 OS. And the neighbouring node has windows xp operating system. Apart from this virtual environment have implemented in three different laptops. The proposed network intrusion detection system was implemented according to the following five steps. They are listening to the Network and Capturing the Packets, Decoding the Packets, Categorization of Network Traffic, Detecting

Specific Attacks (Pattern Matching) and Sending the Information (multicasting).

Aruna Rantore, Kapil Vyas et.al inspects the threat posed by the replication attack and several novel techniques to detect and defend against the replication attack, and analyzes their effectiveness in both static and mobile WSN. Distributed detection approach is more advantages than centralized approaches since single point failure. In bystander based strategy of distributed approaches, randomness introduced in choosing witnesses at various levels like whole network and limited to geographical grids to avoid prediction of future witnesses. If chosen witness node itself compromised node or cloned node then detection of replication attack is uncertain. There may be trade-off between communication cost overhead and detection rate. All the approaches dealt with static WSN. With the deployment knowledge (like order, neighborhoods, and group members with locations) all the nodes in the network should know highest deployed generation which impractical and cannot move join other groups since neighbors or fingerprints vary. Some WSN application requires mobile nodes. The entire access become complex when considering for mobile nodes which dealt with location claims (only) and Deployment knowledge are not suitable for mobile WSN, since location changes time to time in mobile wireless sensor network.

Najma Farooq, Irwa Zahoor, Sandip Mandal and Taabish Gulzar et.al propose schemes for detecting such attacks and also provide solution for its mitigation. DDoS attacks can be detected by analyzing affected or degraded services as DDoS attacks are transmitted across the internet and directed towards the victim, but to launch a defense measurement against a DDoS attack near the victim is not a smart idea because the resources are already under heavy load and the victim cannot properly respond those measures. Therefore it is recommended to stop the attacks near the attack sources which are also helpful to save network resources and can reduce the congestion. However, DDoS attacks can’t be fully detected and filtered near the source.

There are two main stages in the proposed detection scheme. During first stage, each local node identifies the traffic anomalies using profile of normal traffic which is constructed using stream sampling algorithm. The next phase, we can improve the accuracy of detection of media by using gossip based multicast based on sharing information among different nodes. To improve the safety and reliability, our system is based on an overlay network which consists of local nodes such as routers with a DDoS attack detection and packet filtering function. New detection scheme at the intermediate result shows much promise as well.

Lifu Zhang and Heng Zhang et.al made a survey on the Security and privacy in CPS from the viewpoint of the closed-loop. The present and the latest achievements in CPS security, including security analysis of general Cyber-Physical Systems, security issues in smart grid and power systems, secure algorithms, secure state estimation and control, game-theoretic analysis. The corresponding literatures are classified. Then the recent researches on CPS privacy have been discussed from the aspects of communication, computation, and control, respectively.

4. RELATED WORK

Several researchers have worked with different techniques to detect DoS attack and to identify the malicious nodes that source Denial of Service attack in wireless sensor networks. Those techniques are classified and depicted.

4.1 Monitor Nodes Technique

Monitor nodes manage whether there emerge any jamming or misrouting of information through other remaining nodes. Based on remaining energy of nodes a few of the existing nodes are marked as monitor nodes. These nodes collect the packet delivery ratio and Receiver Signal Strength Indicator from all the other nodes. Based on it has compute a weight significance of each node. The computed weight significance is compared beside the threshold value. When the expected weight value goes away from the threshold value, the corresponding node is marked as jammer and it is lonely from data transmission. This technique significantly improves system performance.

4.2 Gateway MAC Technique

G-MAC is an energy efficient sensor intermediate contact control technique planned to direct transmission within a cluster. G-MAC has numerous energy-saving features. It shows pledge in extending the network reality and also the centralized architecture crafts the network more resistant to denial of sleep attacks.

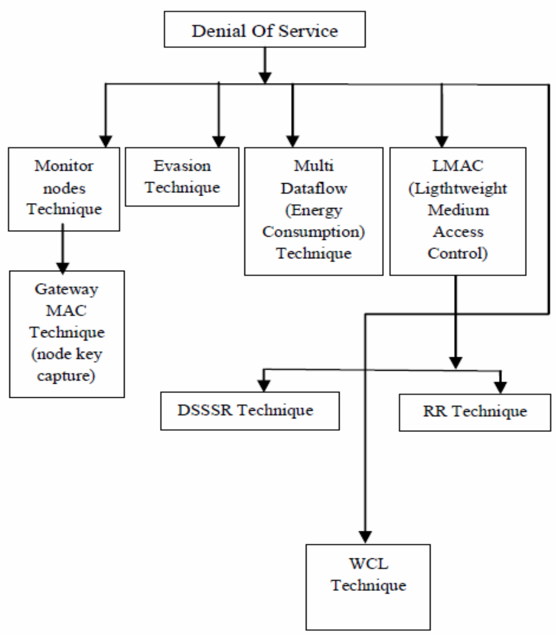
Denial Of Service
Monitor nodes Technique
Evasion Technique
Multi Dataflow (Energy Consumption) Technique
LMAC (Ligthtweight Medium Access Control)
Gateway MAC Technique (node key capture)
DSSSR Technique
RR Technique
WCL Technique

Figure 3. Classification of Denial of Service attacks

4.3 Evasion Technique

It has 2 totally different however complementary approaches. initial approach is to easily retreat from the interferer, which can be accomplished by either spectral evasion (channel surfing) or abstraction evasion (spatial retreats). The second approach aims to contend a lot of actively with the interferer by adjusting resources, like power levels and communication secret writing, for win communication within the presence of the sender. These techniques area unit necessary areas for finding out and classifying the situations wherever one defense strategy is advantageous over another. It's derived solutions to the improvement issues, optimum attack and network defense methods. it's conjointly found alternatives for modeling lack of information for the assaulter and also the network.

4.4 Multi Dataflow Technique

Multi dataflow is a topologies method that can efficiently protect the mobile jamming attack. Mobile jamming attack not only causes the energy expenditure but also breaks the routing on WSN and also shows that the existing protection mechanism is unable to withstand this attack.

4.5 WCL Technique

The fast calculation, the low complexity and the minimal resource requirements counsel WCL as localization algorithm in wireless technique. Weighted Centroid Localization technique to create it rapid and trouble-free for the algorithm to locate devices in WSN.WCL algorithm is derived from centroid determinations which calculate the arrangement of devices through averaging the organizes of identified suggestion points. They summarized the basic theoretical and practical facts relating to the analysis of RSSI measurements.

4.6 LMAC Technique

Lightweight Medium Access Control (LMAC) has confirmed to be the most challenging protocol beside energy efficient attack. LMAC is a excellent delegate of the TDMA category. In LMAC time is separated into frames, which are additional divided into time slots. Initially, it classified denial-of-sleep attacks on WSN medium access control protocols based on an attacker's knowledge of the MAC protocol and capability to break in the network. Next, it discovers probable attacks since every attack categorization. The impacts on sensor networks running for most important WSN MAC protocols and analyzing the competence of implementations of these attacks. Finally, it proposed a structure to protect beside denial of- sleep attacks and offer explicit method that can be used beside each denial-of-sleep susceptibility.

Table 2: Simulation parameters for Case study

Examined Protocol	AODV
Number of nodes	56
Dimensions of simulated area	1000*1000
Simulation time (in seconds)	30
Radio range	250mtrs
Traffic type	Cbr/udp
Packet size (in bytes)	512
Types of attack	DDoS
DDoS attacker nodes	1,2,3,4

The proposed model appraises two amendments to the Lightweight Medium Access Control (LMAC) protocol. The initial step is that DSSSR (Data Packet Separation Slot Size Randomization) and the subsequent step is Round Robin (RR) slot size assignment. Enhancing the attack and pertain it to other types of protocols is also a latent future work because the war among the attacker and defender never ends and it categorize the DoS deluge attacks and categorize existing countermeasures support on where and when they prevent, identify, and respond to the DoS flooding attacks.

5. ALGORITHMS FOR DOS ATTACK DETECTION AND DEFENSE

5.1 Backscatter

Backscatter analysis takes advantage of the fact that for direct DoS attacks, attackers commonly spoof the source IP address at random. Attacks can be detected by monitoring a large enough IP address range and detect unsolicited responses from a victim. The algorithm assumes that the source address is spoofed at random, that attack traffic is delivered reliably to the victim, that backscatter is delivered reliably to the monitor and that unsolicited packets observed by the monitor represent backscatter. The algorithm is not able to detect (D)DoS reflector attacks.

5.2 Kolmogorov Complexity

The algorithm uses Kolmogorov Complexity to correlate traffic flows in the network and detect possible DoS attacks. The underlying assumption is that information, comprising observations of actions with a single root cause, whether they are faults or attacks, is highly correlated and therefore has a high compression ratio.

5.3 DDoS detection on ISP networks

The proposed detection mechanism is distributed: each router detects traffic anomalies using profiles of normal traffic constructed using stream sampling algorithms. Normal traffic profiles are created by sampling traffic over a relatively long time, while current traffic profiles are constructed by using smaller time windows. Whenever the current profile does not corroborate with the normal one, a router becomes suspicious. Routers aggregate the suspicions received from all other routers before deciding whether a certain traffic aggregate belongs to an attack or not.

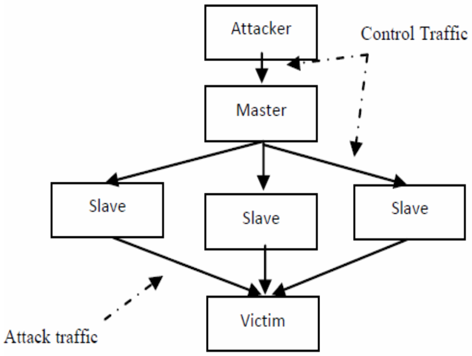

Figure 4. DoS Attack

5.4 Detecting SYN Flooding

Two anomaly detection algorithms for detecting TCP SYN attacks: an adaptive threshold algorithm and a particular application of the cumulative sum algorithm for change point detection. The adaptive threshold algorithm compares the number of SYN packets received over a given interval to the estimated number based on recent measurements. To raise an alarm, the threshold has to be exceeded consecutively. The CUSUM algorithm uses the difference between the number of SYN packets in a time interval and the estimated number for the same interval as a Gaussian random variable. A SYN flooding attack is then detected using the cumulative sum based on the likelihood of the momentary value being caused by a change in the mean traffic rate.

5.5 Detecting SYN Flooding

The SYN flooding attack detection mechanism proposed by Wang, Zhang and Shin is based on the protocol behavior of TCP SYN-FIN (RST) pairs at leaf routers that connect end hosts to the Internet. The difference between the number of observed SYN and FIN (RST) packets is observed and a CUSUM algorithm is applied for change point detection. To reduce the impact of different access patterns of different sites, the difference between the number of SYNs and FINs (RSTs) is normalized by an estimated average number of FINs (RSTs).

5.6 Adaptive change point detection

Adaptive anomaly detection system based on the detection of change-points in the observed traffic pattern. The proposed detection methods employ statistical analysis of data from multiple layers of the network protocol for detection of changes in the statistical models of traffic. The information regarded includes the number of TCP packets categorized by size or type, the numbers of UDP packets and their sizes, the source and destination port for each packet, etc.

5.7 DDoS detection using MIB

The proposed system detects DDoS using information from MIB (Management Information Base) traffic variables for attacker and target. Signatures to match for attack detection were determined from known attacks. On the attacker’s side, a DDoS attack should be detected prior to its launch by identifying MIB-based precursors.

5.8 CATS

The CATS (Cooperative autonomous attack detection) system comprises individual detection systems consisting of a network monitoring part and an attack detection part. Each detection system captures network data and applies both statistical anomaly detection and signature based mechanisms to detect DoS attacks. The anomaly detection engine compares long-time behavior to short-time behavior of statistical parameters not further specified. The signature matching engine is based on tools like Snort and Bro. An enhancement of the detection quality is achieved through coupling multiple autonomous systems, which share their information.

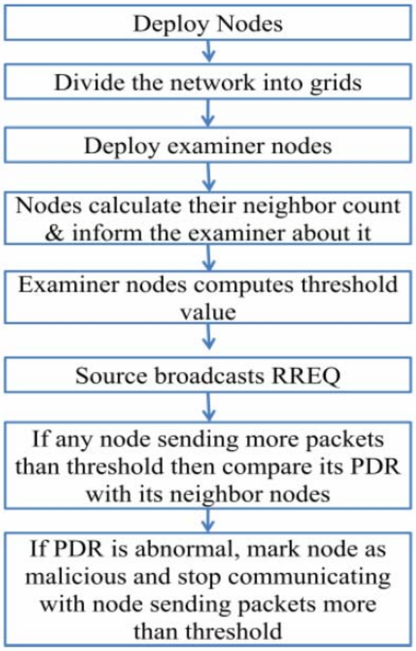
Deploy Nodes
Divide the network into grids
Deploy examiner nodes
Nodes calculate their neighbor count & inform the examiner about it
Examiner nodes computes threshold value
Source broadcasts RREQ
If any node sending more packets than threshold then compare its PDR with its neighbor nodes
If PDR is abnormal, mark node as malicious and stop communicating with node sending packets more than threshold

Figure 5. Steps for attack detection

5.9 Detecting Pulsing DoS attacks

Pulsing DoS (PDoS) attacks are detected at the victim's network using two anomalies caused by PDoS attacks, namely the fluctuation of the incoming data traffic, and the decline of outgoing TCP ACK traffic. To monitor these parameters, the input is sampled using a discrete wavelet transform (DWT). A CUSUM algorithm is then employed to detect abrupt changes in the statistics.

5.10 Space-time network patterns

Method to detect DDoS attacks in the Internet backbone by a set of nodes. The idea is that for a DDoS attack, a direction of the attack is observable, since the data tends to aggregate from the distributed sources towards the target. For monitoring nodes, the number of packets sent by a node is tracked using a vector with one element for each neighbor. To detect a change in the direction of the node's flow, a generalized likelihood ratio algorithm is applied. Statistics of different nodes are then correlated to decrease the detection delay given a fixed false alarm rate probability.

5.11 Sharing beliefs

Approach to detect distributed reflector attacks. Potential reflectors broadcast a warning message to other potential reflectors if abnormal traffic is observed. The detection decision is then made based on the information from multiple potential reflectors. A reflector detects an abnormal network behavior using a CUSUM algorithm on the number of RST packets that have a SYN/ACK state in the outgoing connection. To detect other attacks than TCP, ICMP port unreachable packets are considered. The agents cooperate by sharing their beliefs about potentially Suspicious traffic, leading to a general decision.

5.12 Statistical approaches to DDoS attack detection

Algorithms are proposed that detect DDoS attacks on the basis of statistical properties of specific fields in the packet headers measured at various points in the Internet backbone. To detect changes in the statistics of a parameter, its entropy is calculated consecutively for a sliding window of packets. For the comparison of distributions where the number of possible values is small, Pearson's chi-square test can be applied as well. Examples of parameters are source and destination IP address, TCP/UDP ports, datagram length and TCP window size.

5.13 Hop-count filtering

Hop-count filtering is a method to filter spoofed IP packets by examining the Time-to-Live (TTL) value in the IP header. Since most operating systems use only a few selected initial TTL values, the initial TTL value can be guessed from the observed TTL value, and therefore the hop-count of an IP packet can be obtained. Using a table that maps IP addresses and hop-count values, it can be checked if the packet's hop-count value matches the hop-count of the source address in case of a mismatch the source address is likely spoofed.

5.14 COSSACK

COSSACK is a distributed DDoS detection and response system. An instance of its watchdog program monitors a network and detects attacks using any intrusion detection mechanism. When a watchdog detects an ongoing attack, it broadcasts information about it to other watchdogs indicating the attacking source networks. Each source network watchdog then tries to find out if there exist zombies within its infrastructure and deploy countermeasures if necessary.

5.15 D-WARD

D-WARD is a DDoS defense system that is deployed at the source-end network to prevent the machines from participating in DDoS attacks. Network flows not complying to predefined models are rate-limited dynamically. The monitored data is aggregated traffic from and to each local host for each of its active connections. Considered statistics are TCP packets sent/received ratio, ICMP echo, time stamp, and information request and reply packets sent/received ratio and number of UDP "connections", packets and sending rate per destination.

5.16 Pushback

Pushback is a mechanism employing aggregate-based congestion control. It is implemented on routers to prevent bad traffic from congesting links in a recursive way. The idea is that traffic belonging to an attack is most easily recognized near the victim, and therefore the router closest to the victim can identify the links which deliver the traffic causing the congestion. It then drops traffic from these links and tells the routers forwarding the bad traffic to rate-limit traffic. These routers propagate the request along the attack path towards the attack source(s) requiring that each router on the attack path supports pushback.

5.17 Ingress filtering

Ingress filtering applied by routers, is a method to mitigate attacks involving IP address spoofing. The concept is that routers connecting hosts to Internet service providers check if the source address of every packet to be forwarded is from within the network it is coming from. Packets with source addresses from outside the source's prefix range are dropped. With ingress filtering applied, it is still possible to use spoofed source addresses for an attack, but since the spoofed addresses have to be from within the attacker's prefix range it is easier to track the attacker down, or at least the victim can block a range of source addresses until the problem is solved.

5.18 Traffic control system using traffic ownership

The proposed a distributed Internet traffic control system that controls network traffic close to routers and that is deployed by various network operators. The used fundamental concept of traffic ownership guarantees that deployed traffic control and filter rules have no negative impact on the network and that collateral damage is prevented. For the case of DDoS, a server operator preventively or reactively can inject rules into the traffic control system to block others from using his registered IP addresses as source addresses, which immediately blocks source spoofed packets that are required for e.g. a DDoS reflector attack. Route-based filtering, rate-limiting and other mechanism can be deployed to mitigate more traditional DDoS attacks. Due to the distributed nature of the system, malicious traffic can be stopped close to the attack source.

5.19 Aguri

Aguri is a software package that uses a traffic profiling technique in which records are maintained in an address prefix-based tree. To generate an entry, flows are aggregated until the aggregation has a certain volume, then four summary profiles are produced for source addresses, destination addresses, source protocols and destination protocols. A summary output is produced by traversing the tree and aggregating entries. Hostile activities are identified in the aggregated profiles.

5.20 Packet funneling

Packet funneling is a load balancing approach to mitigate the impact of DDoS attacks at the victim's side by privileging regular incoming traffic. The concept's underlying assumption is that DDoS attacks use IP spoofing resulting in a stream of packets with different, non-recurring IP source addresses, opposed to IP addresses recurring at small intervals in legitimate traffic. To distinguish regular traffic from attack traffic, packet funneling keeps track of the arrival times of incoming packets using an Active IP (AIP) table. If the number of active IP addresses exceeds

the size of the table, new addresses are added to the Waiting Matrix. While arriving packets of addresses in the AIP are forwarded, packets of addresses in the Waiting Matrix are delayed. When the timeout value set on every packet's arrival expires for an address in the AIP, the entry gets dropped, and one of the address in the Waiting Matrix will become active instead.

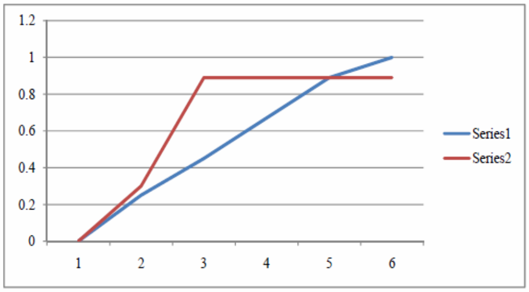

Figure 6: Comparing performance of proposed technique with traditional ones.

6. Simulation results

In this section the analysis of simulation results are mentioned with different number of attackers. Table 1 shows the values of parameters Remaining Energy, packet delivery Ratio, Throughput and Flood count with respect to the different no of attackers.

Table 3 :Parameters Vs No of attackers

↳	Remaining energy	PDR	Throughput	Flood count
1 Attacker	84.9701	0.560	63	1150
2 Attacker	84.85	0.555	65	1344
3 Attacker	84.7946	0.565	65	1538
4 Attacker	84.2156	0.5807	65	1926

6.1 Throughput Analysis:

Number of packets sends in per unit of time. This graph represents throughput analysis in case when there is single attacker and then at two, three and four number of attackers. Throughput is measured in kbps.

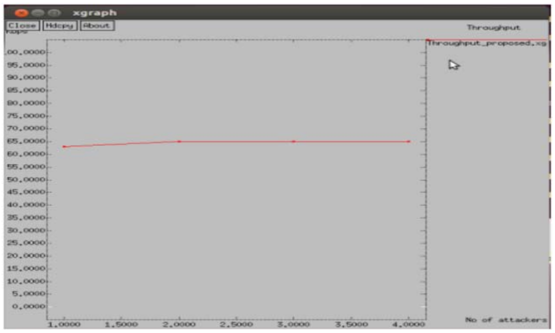

Figure 7: Throughput

6.2 Flood Count:

Flood count is number of packets flooded into the network by different number of attackers. This graph shows the number of packets flooded by one attackers and then by two, three and four attackers.

6.3 Remaining Energy:

Remaining energy is the energy remained in the network after the attack has been launched and prevented in the network. This graph shows the energy remained after the single attacker attacks to the network and then after two, three and four attackers respectively.

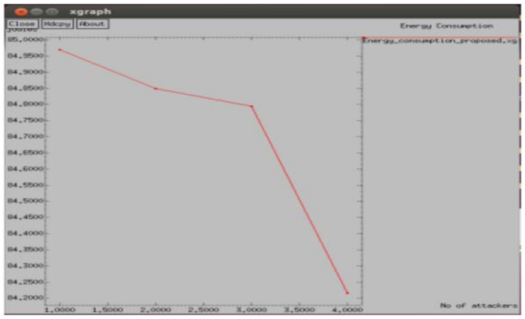

Figure 8: Remaining Energy

6.4 Packet Delivery Ratio:

The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes. This graph represents PDR analysis in case when there is single attacker and then at two, three and four number of attackers.

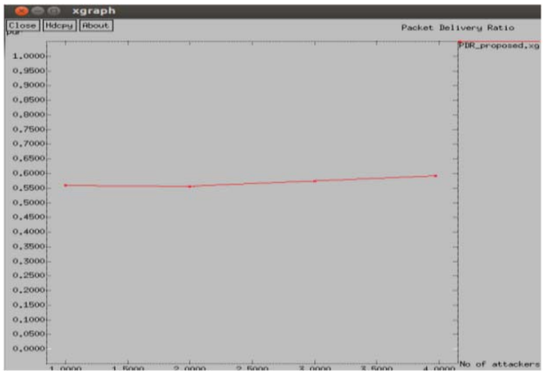

Figure 9: Packet Delivery Ratio

7. CONCLUSION

The paper have provides a detailed and comprehensive study on DoS attacks in Wireless Sensor Networks and classifying them according to their underlying techniques. Protected transaction is very tricky in wireless sensor Network. This paper researched many efficient detection techniques for denial of service attacks in wireless sensor Network proposed by various researchers around the universe. There are many other techniques for detecting DoS attack. By using the above techniques we can make secure communication in wireless sensor network.

8. REFERENCES

[1] R.Ragupathy and Rajendra Sharma, "Detecting Denial of Service Attacks by Analysing Network Traffic in Wireless Networks", International Journal of Grid Distribution Computing Vol.7, no.3 (2014), pp.103-112.

[2] Aruna Rantore, Kapil Vyas, "A Review on Various Routing Attacks on Wireless Sensor Network", International Journal of Science and Research (IJSR), Volume 5 Issue 4, April 2016.

[3] Annie Jenniefer1, John Raybin Jose, "Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2014.

[4] Najma Farooq, Irwa Zahoor, Sandip Mandal and Taabish Gulzar, "Systematic Analysis of DoS Attacks in Wireless Sensor Networks with Wormhole Injection", International Journal of

Information and Computation Technology, Volume 4, Number 2 (2014), pp. 173-182.

[5] Kanchan Kaushal, Varsha Sahni, “Early Detection of DDoS Attack in WSN”, International Journal of Computer Applications, Volume 134 – No.13, January 2016.

[6] Lifu Zhang and Heng Zhang, “A Survey on Security and Privacy in Emerging Sensor Networks: From Viewpoint of Close-Loop”, Sensors 2016, 16, 443; doi:10.3390/s16040443.

[7] Munish Dhar, Rajeshwar Singh, “A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks”, International Journal of Computer Science and Information Technology Research, Vol. 3, Issue 1, pp: (27-33), January - March 2015.

[8] Ankur Rajput, 2 Sachin Goyal, 3Ratish Agrawal, “Detecting Malicious Traffic in Wireless Mesh Network”, International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015.

[9] Manjunatha R C , Dr. Rekha K R , Dr. Nataraj K R, “A Review -Detection & alleviation of Clone Attacks in Wireless Sensor Networks”, INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING. Vol. 2, Issue 12, December 2014.

9. AUTHORS

A.Saraswathi is presently doing Ph.D in P.G. and Research Department of Computer Science, at Government Arts College (Autonomous), Karur, Tamilnadu, India. She has received her B.Sc(Computer Science) degree from Vellalar College for Women, Erode, Tamilnadu, India. She has received her M.Sc degree from Navarasam Arts & Science College for Women, Tamilnadu, India. She has published number of papers in esteemed national/international conferences and journals. Her interests are in Network security and Ad hoc networks.

Dr.K.Thangadurai is presently working as Assistant professor in research and PG Department of Computer science, Government Arts College (Autonomous), Karur. He has Fourteen years of rich teaching experience with 10 years of Research experience in the field of Computer Science. He has worked as the HoD of PG Department of Computer Science at Government Arts College (Autonomous), karur. He has published technical papers in many National and International Conferences and Journals. His areas of interests are Software Engineering, Network Security, Data Mining, etc.,