International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 2 21 - 26

# Detection of Prevention of DDoS Attack Using Gateway Mechanism

Satvir Kaur[a], Gureshpal Singh[b], Baljinder Singh[c]
a Research Scholar, Beant College of Engineering and Technology, Gurdaspur, Punjab, India
b Beant College of Engineering and Technology, Gurdaspur, Punjab, India
c Beant College of Engineering and Technology, Gurdaspur, Punjab, India
[a]*satbirkaur019@gmail.com*

**Abstract:** Denial of service is one of the most terrible attacks is the cloning attack of the node, where the attacker captures the knot and extracts its secret information, create replicas and enter them in the network field other malevolent behavior. To detect and mitigate this attack, several static-based detection schemes have been proposed. The detection algorithm based on the node location speed was proposed, to detect the attack of nodes clones in the wireless network. This algorithm reduces the costs of communication, routing, overloading the entire network and improving network performance.

*****

## I. Introduction

WSN is presently used for unmanned physical surroundings within the world to measure distinct variables. Therefore, the features of the WSN should be thought-about for the economical execution of the network. Further, the various options of WSNs are outlined below:

**1. Inexpensive:** Within the WSN, lots or thousands of sensing element nodes are sometimes enforced to measure any physical atmosphere. To reduce the general value of the whole network, the value of the sensing element node should be unbroken as low as attainable.

**2. Energy effectiveness**: Energy in WSNs is engaged for a variety of functions, such as IT, communication and archiving. The detector element node utilizes ample of power than the other for communication. If they run out of power, they usually become invalid as we've got no recharge possibility. Therefore, protocols and algorithmic program development should contemplate energy consumption within the network.

**3. Restricted power:** Unexceptionally the node has limited computational capabilities, because it is significant to contemplate prices and energy.

**4. Communication skills:** Normally, the WSNs communicate untreated radio waves via wireless channel. The communicating is two-way or unofficial. With the unmanned and hostile in operation atmosphere, it's troublesome to run WSNs. Therefore, communication hardware & computer software should take into consideration security and robustness.

**5. Security and privacy:** Every sensing element node must have sufficient security methods to stop unauthorized admittance, attacks & accidental harm among the sensing element node. More important is extra privacy mechanisms ought to even be enclosed.

**6. Multi-hop communication:** An outsized range of sensing element nodes is enforced in WSN. Therefore, to communicate with the sinker or bas, it is require assisting associate degree intermediate node through the routing path. If it's necessary to speak with the opposite node or base station that's on the far side its oftenness, it should do therefore through the multiple jump path by intermediate node.

**7. Application oriented:** The WSN is totally different from the traditional network because of its nature. It depends plenty on the applying ranges of the military, environmental & health sectors. The nodes are enforced indiscriminately & expand in keeping with the sort of use. Routing is that the method of transferring information from the sender to the destination in a network. However, routers communicate with one another and distribute information that permits them to pick methods between 2 nodes in a network. Most of those kinds of algorithms confirm the selection of the precise path. Every router in topology solely has the information of networks that are directly connected thereto. It conjointly shares information firstly between immediate neighbors & then across the whole network. This means, routers acquire the information of the whole configuration. The technique of deciding the trail is that the routing algorithms confirm and manage the routing tables that enclose the full routing information of the packet. A routing table could be a table of information that hold on a router or network pc that lists the routes of some network destinations

and, in some cases, the distances related to those methods. It conjointly contains information on the configuration right away. Therefore, the development of routing tables is the main objective of routing protocols. The entries within the routing tables are the prefix of the informatics address and also the next hop. There are 2 kinds of routing: static routing and dynamic routing. Static routing is solely the method of manually getting into routes into the routing table of a tool through a configuration file that is loaded once the router starts from the router. These methods may be entered by a network administrator who manually configures the routes.

## II. Related Work

[1] Said that DDoS assaults could be powerful to the point that they could without much of a stretch come up short on processing assets or transmission capacity of potential targets. DDoS assaults can be performed on two dimensions: application level and system level. The feeble purpose of the system based application is that the correspondence port is typically open. This enables aggressors to likely dispatch disavowal of administration (Dos) assaults. Answers for this issue; authors utilize the port hop procedure to help numerous customers without the requirement for gathering synchronization within presence of clock drift. Likewise, we utilize the HOPERAA program and the BIGWHEEL program to defeat circulated refusal of administration assaults.

[2] Said that the assortment of digital assaults makes the accessibility of administrations a noteworthy security concern. A typical kind of malware is refusal of DDoS. A DDoS assault is intended to keep authentic clients from getting to administrations. It is simple for an inmate who has real access to the framework to mislead any security check which results in an interior assault. This report proposes an arrangement of ID and early seclusion (EDIP) to relieve DDoS assaults helped by inside staff. EDIP identifies the advantaged data among every single genuine customer in the framework at the intermediary level and disconnects it from blameless customers amid movement to the assault intermediary. Besides, a productive calculation is created for the identification and confinement of special data so as to expand the seclusion of the assault and limit the interruption of considerate customers. Likewise, the heap adjusting idea is utilized to counteract intermediary invades.

[3] Proposed that when DDOS assaults interfere with Internet administrations, DDOS devices affirm the viability of the present assault. The DDOS assault and countermeasures keep on expanding in number and intricacy. In this paper, we investigate the extent of the DdoS flood assault issue and endeavor to battle it. A developing heightening of refusal of-administration assaults dispersed over the application layer in Web benefits rapidly drew the consideration of the forswearing of-administration look into network onto the customary system. Thus, new sorts of assaults have been investigated, for example, HTTP GET Flood, HTTP POST Flood, Slowloris, RU-Dead-Yet (RUDY), DNS, and so on. Furthermore, after a short prologue to DDOS assaults, we talk about the usefulness of the new application proposed Denial of Service assaults conveyed on the dimension and decorate the effect on current Web administrations.

[4] Said that the widespread use of Wi-Fi (Wireless Fidelity) allowed us to easily access the Internet and also paved the way for many hacking attacks. The identification of anomalies applied to the identification of gaps in active data is possible in several things, as the end user and the administration repeatedly discover trying to understand the DDoS attack (distributed denial of service). A new approach to anomaly detection using the Decision Tree procedure to protect wireless nodes within the network and destination nodes from DDoS attacks and to determine attack patterns and provide appropriate countermeasures using the KDDCup data set 99 for determination and classification intent indicate that it classifies the respective instances of attack type with detection rate of the week. This exploit integrates recognized classification skills such as Random Forest and J48

[5] Said that, to understand well the characteristics of DDoS problems and investigate the corresponding defence mechanisms, there are significant contributions not only for the academic sector and industry, but also for social security and agencies. management They can use this knowledge to improve their risk assessment capabilities and help stakeholders to make appropriate decisions in the face of DDoS threats. In the existing research work the different types of problems, this perspective in terms of detection of DoS attacks is seeing the problem as a problem of classification in the network state (and not in individual packages or other units) by modeling the normal and attacking the traffic and classifies the current status of the network as good or bad, detecting attacks when they occur. Another is that transmission failures or failures in the expiration can cause alterations in the process, the degradation of the performance of the general check. In the future, all this will be solved with the help of detection of DDoS attacks and the DSR algorithm with encryption in the WSNs and WSN with BS, CHMs.

[6] Said that WSNs is a tremendous space that is utilized to distinguish data in different applications. The recognized data is likewise taken to the base station for preparing. While this data is being prepared, the security of the tended to information is critical and can be tested in WSN. This happened in light of the fact that WSN is actualized in unmanned conditions. Specialists chipped away at different

issues, for example, heartiness, energy utilization, security, and so on from a bygone era period. Be that as it may, the present record concentrates more on the directing that is guaranteed, just as on the solid model. Here they utilized the idea of dynamic trust directing plan to protect different kinds of assaults amid information parcel steering. These assaults comprise fundamentally of a dark gap assault, a refusal of administration assault, and a specific sending assault. The framework likewise ensures data by hiding it while routing utilizing the ECC calculation, which gives security. The test results demonstrate that the proposed framework enhances wellbeing, just as broadening the helpful existence of the system and low energy utilization and more prominent proficiency all through the valuable existence of the system.

[7] Said that WSNs (WSN) are increasingly used in safety-critical applications. Because of their inherent characteristics of limited resources, they are subject to various security attacks and a black hole attack is a type of attack that seriously affects data collection. To overcome this challenge, we propose a safety and reliability routing scheme based on active detection called Active Trust for WSN. The most important innovation of Active Trust is to avoid black holes by actively creating different detection paths to quickly detect and gain nodal trust and, therefore, improve data path security. More importantly, the generation and distribution of detection routes are provided in the active Trust scheme, which can use energy in non-active points to create the number of detection paths necessary to achieve the desired energy security and efficiency. . Both the complete theoretical analysis and the experimental results indicate that the performance of the active Trust scheme is better than that of previous studies. Active Trust can significantly improve the probability of success of the data path and the ability against black hole attacks and can optimize the life of the network

[8] Proposed a large-scale, position-sensitive clone detection protocol in WSN that can effectively detect clone attacks and maintain a satisfactory network life. Specifically, they take advantage of sensor location information and randomly select tokens positioned in a ring area to verify the legitimacy of the sensors and to report on the detected clone attacks. The ring structure facilitates the forwarding of energy efficiency data along the path to the towers and the sink. In theory, they show that the proposed protocol can achieve a 100% probability of detection of clones with reliable controls. They extend the work further by studying the performance of clone detection with unreliable controls and show that the probability of detection of clones is still close to 98% when 10% of controls are compromised. Moreover, in most of the existing clone detection protocols with a randomized control selection scheme, the required sensor buffering usually depends on the density of the node, whereas in the proposed protocol, the required buffering of the sensor is independent of n, but depends on the length of the jump of the network radius h. In-depth simulations show that the proposed protocol can achieve a long network life by effectively distributing the traffic load across the network.

[9] Said that limited resources, the ad hoc nature of deployment and the vulnerability of wireless media are some of the most demanding features of the WSNsthat raise the need for unique security solutions. WSNs are susceptible to various attacks, in which a wrong address, a type of Denial of Service (DoS) attack is very difficult to detect and defend. Network performance (ie performance) is also reduced. Therefore, detection and prevention of this attack becomes very crucial. In this paper, we proposed a new technique for preventing and identifying intrusions based on clustering for incorrect attack. The network parameters calculated using this technique show a significant amount of performance improvement while introducing a small amount of delay.

[10] Said that the WSNs is quite vulnerable to many attacks that compromise security such as worm attacks, repetition or manipulation of messages, identity theft, black hole attacks, illegal interceptions, etc. One of the impacts of the selected forwarding attack is that it can be used to delete certain data packets. LEACHES (Low Energy Adaptive Cluster Hierarchy) applies group rotation randomly for power distribution across all sensor nodes. In this document, the creation, detection and elimination of selective forwarding attacks are performed in the LEACH routing in WSNs. It analyzes the way in which the performance of the affected networks is analyzed with the selected forwarding attack and therefore the performance of the detection and deletion algorithm. Furthermore, LEACH performance was evaluated in terms of package delivery speed with the number of attacking nodes of the selected forwarding attack. The proposed analysis is simulated using the NS2 network simulator. The prevention technique has a considerable success in attack management while restoring network performance and reducing the effect of the attack from the network

## III. Simulation Scenario and Results

A detailed simulation model based on NS2 is used. Following table 1 shows the different simulation used for the proposed approach:

 ISSN: 2321-8169
21 - 26

**Table 1 Simulation Parameters**

| SIMULATION PARAMETERS | VALUES |
|---|---|
| Area | 1000 * 1000 m |
| Number of Nodes | 100 |
| Traffic Type | CBR |
| Antenna Type | Omni Directional |
| Number of Mobile Connections | 10, 15, 20, 25 |

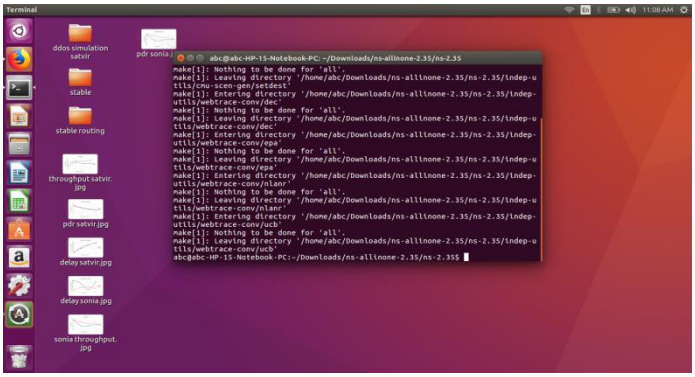

**Fig. 2. Make Command to Refresh NS2**

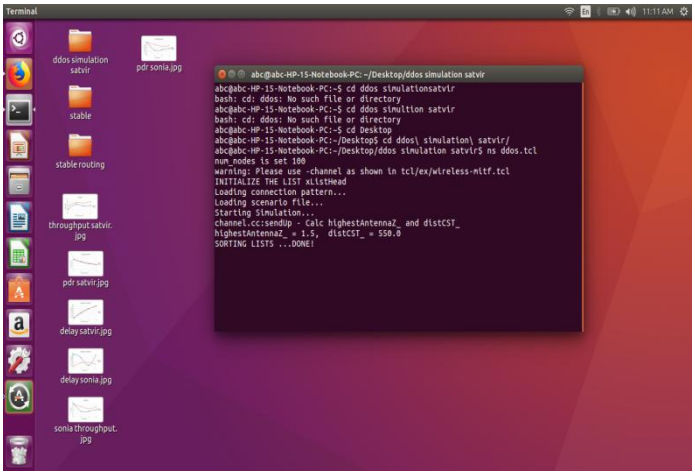

**Fig. 3. Scenario with different wireless nodes in network**

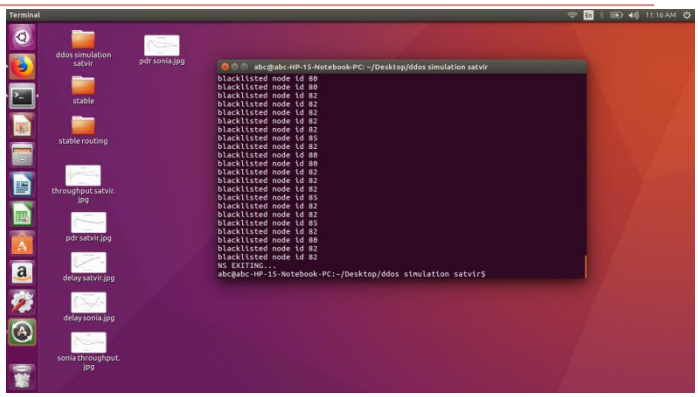

**Fig. 4. Simulation Complete**

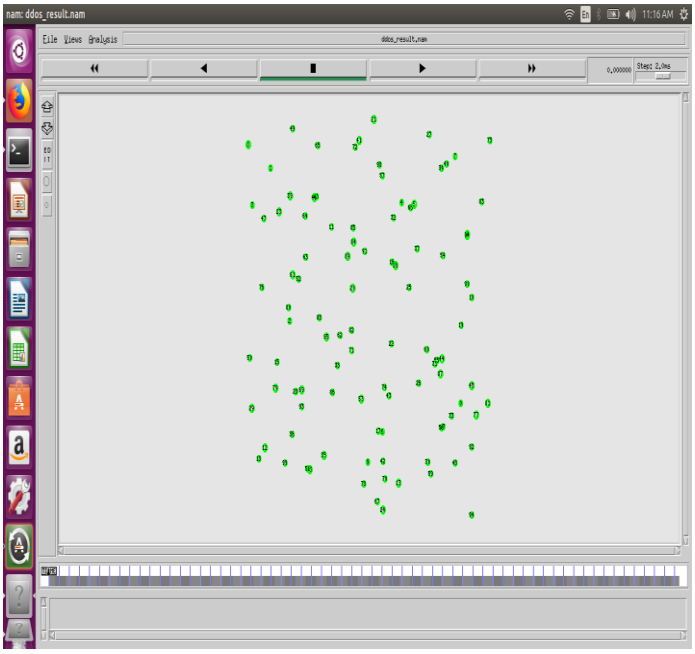

**Fig. 5. Deployment of various nodes in a network**

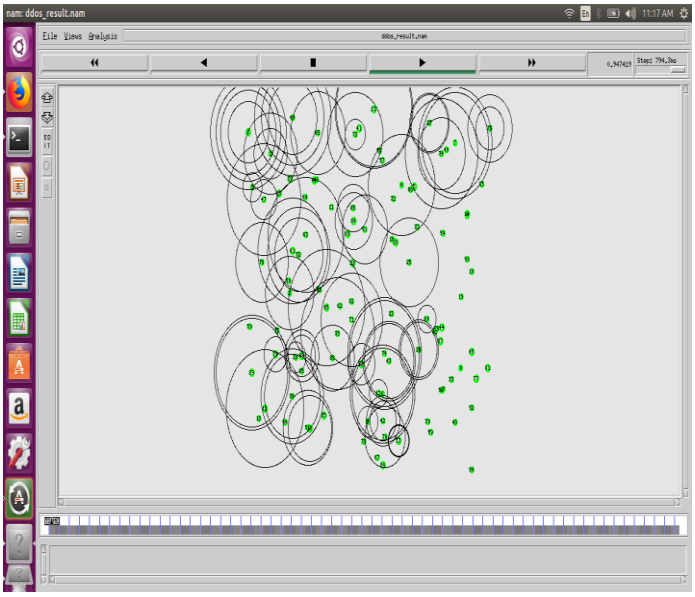

**Fig. 6. Animation to Show Flooding Attack**

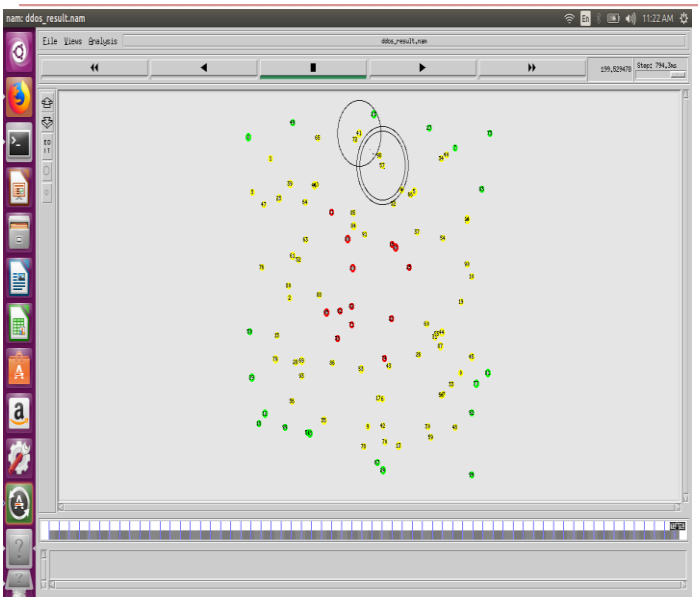

**Fig. 7. Blacklisted Nodes with Red Colored to prevent Flooding**

Traffic sources with bit rates (CBR) are used. Originating destination pairs are randomly distributed across the network. Data packets of 512 bytes are used. The mobility model used is a random reference point in a rectangular area of 1000 X 1000 with 100 knots. The node moves with a mobility of dispositions towards a destination in which it stops for a period of time (pause time) and then moves to the next destination. The simulation is performed for a few seconds. The detailed description of the simulation scenario is shown in Table 1. **Performance Metrics**

**1. Packet Delivery ratio**

The package distribution ratio in this simulation is defined as the ratio between the number of packets sent by the constant bit rate sources (CBR, application level) and the number of receiver packets per CBR receiver in the destination Table

**Table 2: Packet delivery ratio**

| No of mobile connections | Base work | New work |
|---|---|---|
| 5 | 0.9163 | 0.9832 |
| 10 | 0.7144 | 0.7374 |
| 15 | 0.5669 | 0.5979 |
| 20 | 0.4732 | 0.5024 |

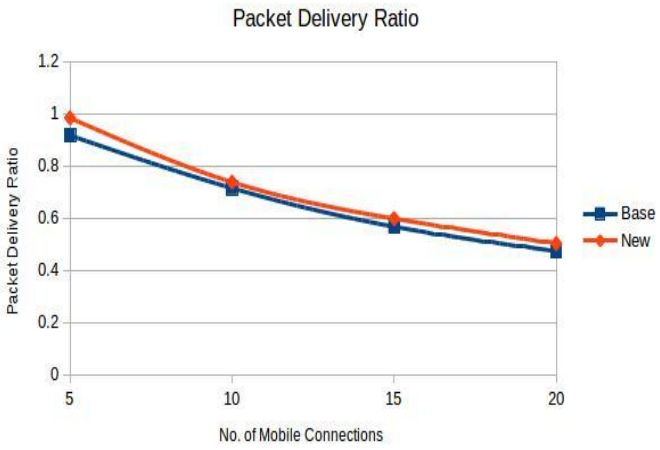


**Fig. 8. Packet Delivery Ratio**

**2. End-to-end delay:** This metric represents an average end-to-end delay and indicates how long it takes for a packet to travel from the source to the target application level. It includes all the possible delays caused by buffering during the latency of the route detection, transmission delays in the MAC, the queue in the interface queue and the propagation and transfer time. It is measured in seconds

**Table 3: Average End-to-End Delay**

| No. of mobile Connections | Base work | New work |
|---|---|---|
| 5 | 139.123 | 80.0112 |
| 10 | 666.374 | 790.251 |
| 15 | 1145.69 | 1183.51 |
| 20 | 1505.46 | 1454.07 |

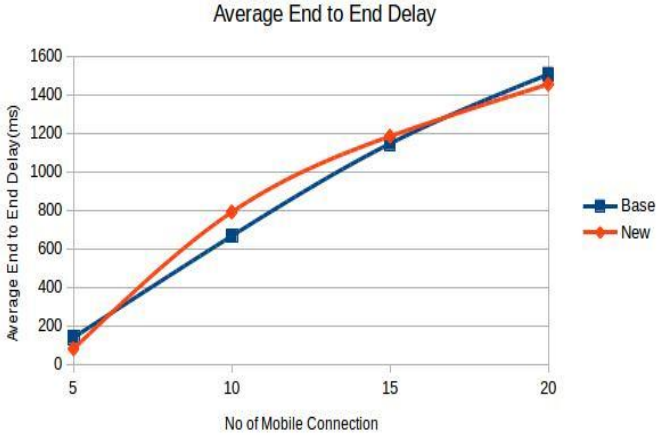


**Fig. 9. Average End to End Delay**

**3. Throughput**: Throughput is total packets success fully delivered to individual destinations in excess of total time.

**Table 4. Throughput**

| No of mobile connection | Base work | New work |
|---|---|---|
| 5 | 114.96 | 122.84 |
| 10 | 126.9 | 131.22 |
| 15 | 122.49 | 130.53 |
| 20 | 124.13 | 133.79 |

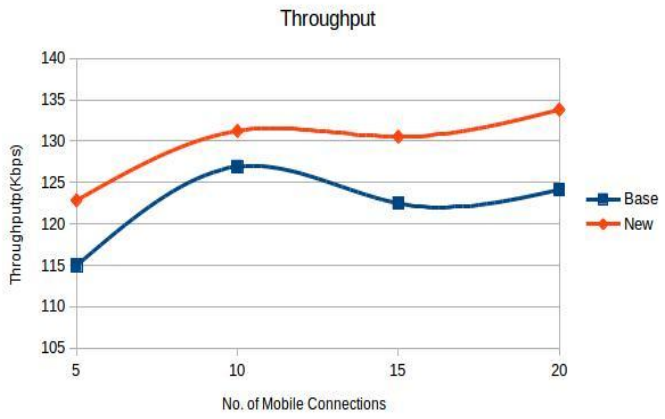


**Fig. 10. Throughput Analysis**

## IV. Conclusion

One of the most alarming attacks in the WSN is the cloning attack of the nodes where the attacker takes the details of the node and collects their personal data, duplicates them and inserts them into the network field for further malicious activities. To detect and eliminate this type of attack, different detection techniques have been designed based on both static and mobile WSNs. Further, in this research work, a novel node's sending speed is noticed based on which a detection alarm is generated if node's speed exceeds the actually speed in wireless network. Then, a blacklist is maintained, in which the malicious node's identity is placed. When, in future the node with same identity tries to enter, it will be blacklisted and hence could not enter in a network communication. The base work is compared with the proposed approach, which further suggests that proposed approach is better in case of Throughput, Packet Delivery ratio and delay.

## References

[1] C.Kavitha, "Complete Study on Distributed Denial of Service Attacks in the Presence of Clock drift," ICICES2014, Chennai, Tamil Nadu, India, 2014.

[2] V. Kansal and M. Dave, "Proactive DDoS Attack Detection and Isolation," International Conference on Computer, Communications and Electronics (Comptelix) Manipal University Jaipur, Malaviya National Institute of Technology Jaipur & IRISWORLD, July 01-02, 2017.

[3] K. S. Bhosale, M. Nenova and G. Iliev, "The Distributed Denial of Service Attacks (DDoS) Prevention Mechanisms on Application Layer," IEEE, 2017.

[4] S. Lakshminarasimman , S.Ruswin and K.Sundarakantham, "Detecting DDoS Attacks using Decision Tree Algorithm," 4th International Conference on Signal Processing, Communications and Networking, Chennai, INDIA,IEEE, 2017.

[5] A. Kaur, D. Kaur and Gagandeep "DDOS Attack Detection on WSNs: A Review" International Journal of Innovative Research in Science, Engineering and Technology (A High Impact Factor & UGC Approved Journal) Vol. 6, Issue 8, August 2017.

[6] M. Shinde and D. Mehetre, "Black Hole and Selective Forwarding Attack Detection and Prevention in WSN," IEEE, 2017.

[7] Y. Liu, M. Dong and A. Liu, "Active trust – secure and trustable routing in WSN," IEEE, 2016.

[8] Z.Zheng, and A. Liu, "Energy and Memory Efficient Clone Detection in WSNs," 32nd Annual IEEE International Conference on Computer Communications, IEEE INFOCOM, 2013.

[9] R. Sachan, M. Wazid and A. katal, "A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN," International conference on Communication and Signal Processing, 2013.

[10] D. Acharya and S.L Agarwal , P. sharma and S.K Gupta "Performance analysis of detection technique for select forwarding attack on WSNs," fourth International conference on parallel, distributed and grid computing, 2016.