AN APPROACH TO IMPROVE DETECTION and PREVENTION of DDoS IN WIRELESS SENSOR NETWORK (WSN)

[1]Shabnum Khan,[2]Vandana Pushe,[3]Manmeen
[1]Research Scholar, [2] Assistant Professor, [3]Assistant Professor
[1]Department of Computer Science,
[1]Swami Vivekanand Institute of Engineering and Technology, Banur, India

Abstract : Wireless sensor network is a self-configuring network in which the sensor nodes are deployed in such a manner so that they can join or leave the network whenever they want. To transmit the date within the specified network the nodes communicate with each other. Due to decentralized nature of the network it is prone to numerous malicious nodes entering the network. With the progression of this innovation, one of the significant concerns these days is security. The attacks are set off inside the network because of the presence of such sort of malicious nodes in the network. There are two types of attacks namely active and passive attack. Distributed Denial of Service (DDoS) is a active type of attack in which raw packets are flooded to the victim node. The malicious nodes in the attack can adapt different kinds of attack like flooding attack, black hole attack and warm home attack to cease the normal functioning of the network. Whenever a DDoS attack happen, it will minimize the lifetime of the network and also the energy consumption increases. This is very risky in applications like military and industry. In order to detect the malicious nodes from the network which cause the DDoS attack, a novel approach is proposed in this research work. In this approach, monitor mode technique is used. This results in increase of throughput from 14 to 19.25.

IndexTerms **- DoS, DDoS, WSN, IP, QoS, MAC.**

1. INTRODUCTION

There are different sensor hubs passed on inside a wireless sensor network (WSN) close by one base station in it. The sensor hubs are minimal estimated contraptions which have very less power and cost close by constrained memory, computational power and correspondence resources. There are different spatially appropriated self-overseeing sensors present inside the association what amass the information from their natural factors and pass it to the base station.

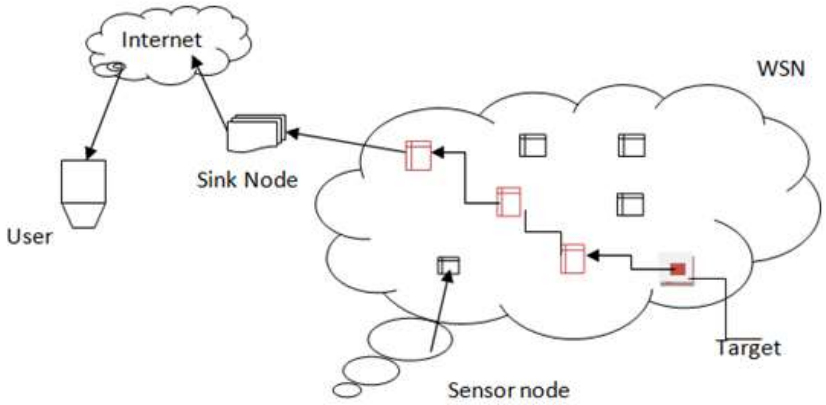

Fig 1 Wireless sensor Network

The hubs sent inside these organizations assemble the information from including. All the amassed information is shipped off the base station present in the organization which goes probably as a section among the sensor organization and the external climate. The limit furthest reaches of base stations is high and it furthermore involves different data taking care of capacities which is useful in the association of organization. The critical task of the base station is to get the information which is conveyed by the sensor center points. This information can be gotten to by the end customer and can be utilized by its need as exhibited in Fig. 1. The sensor center points are sent inside the space of base station which can shape packs as indicated by the essential of the application. Due to the more unobtrusive sizes of the sensor centers, the ranges of their batteries are close to nothing. The batteries of the sensors channel successfully and can't be re-empowered viably as they are passed on once in gigantic zones. In this manner, the lifetime of the association diminishes which is a critical concern [13].

The information that is cultivated through the steady seeing of the hubs is shipped off the base station in light of which these organizations are known as bi-bearing remote sensor organization. Inside the circumstances which require consistent noticing, and it isn't serviceable for individuals to screen the ecological elements, which can be possible by passing on these organizations. There are various phenomenal properties of these organizations, for instance, the batteries have confined life time; the sensor centers are heterogeneous in nature, the center points are compact, and so forth From the outset, the military application utilized the WSNs inside them to screen the wellbeing and military applications. Further, as per the improvement in these advancements, various applications were moreover intricate like modified creating, home computerization, robot control, and so forth In view of

the information of temperature gathered from the natural components by sensor center points, the forest flames were similarly recognized inside various applications.

1.1 DISTRIBUTED DENIAL OF SERVICE ATTACKS

Denial of Service (DOS) attack: The DOS attack can be set off at various layers however the essential intention of these assaults is to briefly make the organization assets inaccessible. The total programming of the sensors can be controlled by the aggressors. The aggressors can be powerful to such an extent that they can even place a bogus sensor instead of an authentic sensor coming about the adjustment of entire hardware.

Distributed Denial of Service (DOS) attack: The motivation behind this attack is to keep credible clients from utilizing site, web administration or PC framework like indicated network asset. It is a planned assault of given objective organization or framework accessibility. This assault is in a roundabout way dispatched through many bargained registering frameworks. The auxiliary casualties are those that are utilized to dispatch the undermined frameworks and essential casualties are those that attack the administrations.

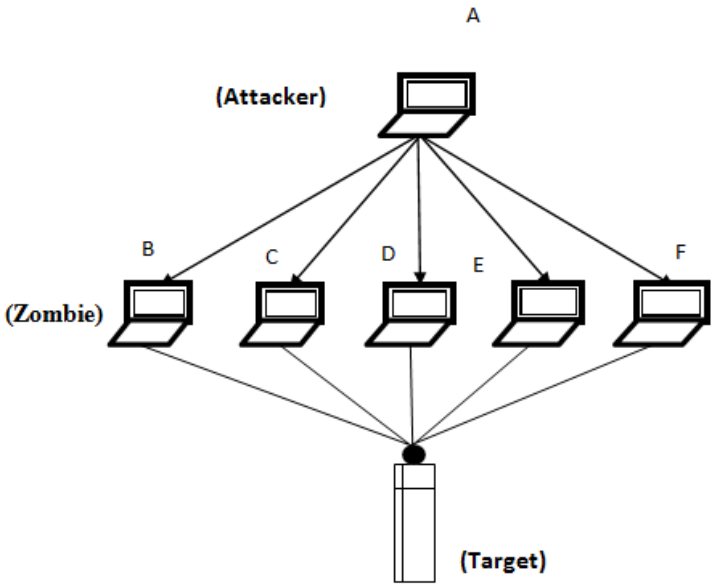

Fig 2 DDoS Attack in WSN

In this attack unnecessary measure of bundles are shipped off a worker to hinder its speed or to make the shortage of assets to the clients so a client can't get to the office. The Fig.2 shows the chart of Distributed Denial of Service assault. It comprises of six hubs or PCs name as A, B, C, D and E. In this sort of destructive assault, a solicitation or bundles are sent by the PC A for example an aggressor to influenced PCs, for example, B, C, D, E, F and make them slaves then the assailant sends the control parcels as opposed to information bundles to the genuine hubs which are currently captives of the assailant after this, assailant overwhelmed the worker with many pointless or undesirable solicitation because of which client incapable to get to assets

2. RELATED WORK

Manhee Lee, Eun Jung Kim, et.al (2004) proposed the two existing stepping computations, for instance, Probabilistic Packet Marking and Deterministic Packet Marking couldn't show practical results, in after the source on account of the directing adaptively in the prompt associations. DDoS attacks inside the gathering are considered as the critical issue in the association as it crashes the whole structure [1]. The DDoS attack incapacitates the laborer, association or organization by flooding external data traffic as correspondence requests. Another group stepping plan, for instance, Deterministic Distance Packet Marking is presents in this paper in which the distance between the individual being referred to and the source is recorded that is valuable in choosing source. In light of the obtained results, it is seen that the proposed coordinating computations are incredible and pertinent to work, torus, and hypercube. With the help of this procedure, overhead on the tremendous associations are restricted and extended its adaptability.

S. Kumar, R. Valdez, et.al (2006) presented that a singular direct frustration for the end-toward end sensor network establishment is created by the WSN section that causes data arrangement and the leading group of WSNs. This is a critical issue to manage considering the way that the absolute perception action can be cut down as a result of this mistake. To include the way where the preparing resource of section can be exhausted is repeated by DDoS attack inside the WSN-entrance of WSN as indicated by this paper. The data variety practices are clearly impacted by this consumption of handling resource of the section [3]. Inside the Ping-based DDoS attack traffic, the level of exhaustion of figuring resources of the WSN doorway processors is enrolled. The party, recording similarly as specifying of the log sensor data is stopped by the WSN-entrance on account of this strategy. The transformation to inner disappointment ought to be improved in this work with the ultimate objective that the shortcomings relevant to WSN-section can be discarded.

Mahdi Zamani, Mahnush Movahedi, et.al (2009) proposed an interference disclosure structure to recognize the DDoS in a Wireless Sensor Network. The security issue is the critical test these days in the far off sensor network subsequently, fitting security show is required.With the area of the Distributed Denial of Service (DDoS) attacks, various researchers plan distinctive

compositional approaches as far as possible the effects of this assault [6]. Maker proposed various musings that are isolated from the direct of natural safe structures dependent on obtained results like Danger Theory. Hereafter a model is made that hinder the DDoS attack from the association this model is for vaccination of passed on interference recognizable proof structures.

Jiawei Chen, (2011) proposed system dependent on DBP-MSP and safe steering to accomplish better execution against DDoS assaults for the remote sensor network in the transmission validation. The base station in DBP-MSP, choose and present the riddle trouble level k that limit the computational utilization of the sender to tackle the riddle. At the point when the transmission responsibility in WSN isn't weighty this strategy is used because of which energy utilization pace of the sender is handily controlled [13]. A key chain conveyance plot additionally proposed in which one way key chains is passed by the base station to the sender with the assistance of which stockpiling and calculation trouble on the sender is diminished to more prominent degree. Ideal security execution for the single direction key chain is additionally given by this technique.

Omer Demir and Bilal Khan (2011) proposed a SLANT calculation that has been used to impact gotten data over groupings of source caricature Botnet-drove DDoS assaults. Different difficulties are looked by the Internet Service Providers to give the internet providers among those difficulties DoS/DDoS assaults are major. This assault can upset correspondences association at public level also as can cause foundation issue at country level [11]. To complete source-parodied DDoS assaults, Botnets are broadly utilized. Hence, distinguishing such issues by the assaults is considered as the major concern.This proposed calculation acquired the valuable outcomes and give better execution regarding its adaptability to enormous organizations and quantities of assaulting hubs.

ZHANG Yi-ying, Li Ziang-zhen et.al (2012) presented for the revelation and removal of the DoS attack they proposed a novel technique known as message insight framework (MoM). The usage of sensor networks are extended with the coming in the advancement as it is used in by far most of the applications, yet there are a couple of cutoff points from which these associations are persevered. These requirements are more energy use, estimation and confined storing for sensors and some more. It is the critical test in the security of the associations from this time forward it is expected to have a security show that prevents all of the attacks for WSN, similar to repudiation of organization attack. Present foes to a great extent deal with the sensors and using dreary messages or fake messages it dispatch the DoS attack inside the association [12].

Varsha Nigam, Saurabh Jain, et.al, (2014), has presumed that for working in basic conditions, WSN has demonstrated out to be a decent and solid innovation. The sensor organizations can be conveyed at different places, for example, disaster areas, structures or traffic observation. In the event that we talk around one significant test in the utilization of remote sensor networks then it tends to be the security issues. In this paper, they introduced a profile based insurance plot to forestall the impacts of the DDoS assault. The significant reason for this sort of the assaults is causing of huge measure of information known as flooding of information. Because of this, it totally devoured the transfer speed of the organization by conveying information that prompts influence entire execution of the organization [23]. The primary goal of this paper is to discover the impact of DDoS assault in network and deciding the exhibition influencing hubs.

Raksha Upadhyay, Salman Khan, et.al, (2015), introduced the wireless sensor network which has the ability of detecting and handling got data. There are various segments in wsn like battery, chip, stockpiling media and transducer utilized by sensor hubs. For various applications, it is considered as the straightforward and viable technique. Because of open nature of the wsn it is viable to limit different security dangers. Because of the presence of the diverse security dangers like dark opening, wormhole assault, DDOS assault and a lot more they defame the current data or sensor hub information. The organization is prompts irresistible because of the seepage of asset ability which is the fundamental target of DDOS assault. The organization blockage is expanded and lifetime of the organization and hub is debased because of preparing of unimportant messages in immense amount. The battery life of the battery is straightforwardly debased the existence of hub as organization lifetime is straightforwardly reliant upon the limit of battery.

William Hurst, Nathan Shone, et.al (2015) talked about the impacts made by the DDoS assault that debilitates the worker, organization or administration by flooding information traffic remotely by sending correspondence demand. Significant effects are made by the DDoS assault in the organization like foundation blackout and different effects on the framework of the organization that is yet excessively recognized. The principle objective of this paper is to decide the impacts of previously mentioned assault and proposed approach that decide digital assault impacts inside the organization [25]. Information is addressed in both typical run-time and an assault situation because of the reproduction of a basic foundation organization. It likewise exhibited a procedure that gets to the disturbances on incorporated basic framework network with the assistance of got dataset. In expanding digital danger issues can be limited for which it is needed to decide the event of disappointments in an interconnected organization. at the point when the falling disappointment happens in the organization it is needed to have proper recuperation plan to expand the degree of adaptability that plays as fundamental job.

Monika Malik and Dr. Yudhvir Singh (2015) proposed one of the sort of impromptu organization that are more inclined to purposeful or unexpected assaults when contrasted with wired based organizations known as WSN. The significant impact brought about by Denial of Service (DoS) assault inside the organization and is considered as the significant danger. Huge number of hosts has been used by the DoS assault to send bundles to the focused on helpful parcels by sending invalid access that devour enormous measure of assets and cause worker harm [19]. Different sorts of assaults on WSN are talked about and DoS assault accentuation. Creator in this paper examine the smurf assault which is one of the DoS assault type. Every one of these assaults harm the usefulness of the organization and breakdown the whole frameworks. The assets data transmission, worker, and circle space or processor time are influenced because of DOS and DDOS assaults. The Smurf assault is the ICMP convention based DDOS assault in which assailant take the entrance utilizing IP Spoofing strategy.

Taranpreet Kaur, Dr. Krishan Kumar Saluji, et.al, (2016), have examined that enormous number of sensor hubs are available in the remote sensor networks which has low capacities of gathering all the necessary touchy information. In this organization, security is the significant worry because of approach in the innovation. Different kinds of assaults are dwelled in this organization like dispersed forswearing of administration assaults. Present noxious hub in the organization is embraced by numerous assaults like flooding assault, dark opening assault and wormhole assault so they can lead aggravation in the usefulness of the organization. The danger expanded more, when it is used in the field of military and modern applications. Restricted battery power, low abilities of hubs is the significant imperatives in wsn. In this manner, it turns into a test for the specialists to build up a security model that moderate every one of these requirements and give ideal security to the organization. To distinguish and forestall DDOS assaults, number of scientists has proposed new instruments. In this paper [29], creators did a study on various existing strategies by utilizing different boundaries. This review will assist specialists with improving the current procedures that can't alleviate low energy utilization and bogus alert issue.

Shital Patila and Sangita Chaudhari et.al, (2016), have broke down wide scope of utilization of remote sensor networks in this paper that has been used for the information social event and information transmission measure. There are a few shortcomings in WSN that shows that current sensor hubs more influenced by the security dangers. The most famous assault that impact sensor hub is Denial-of-Service (DoS) assault. Along these lines, there is need to forestall Dos assault utilizing various strategies. There are number of strategies that have been utilized by various scientists for forestalling DDoS assault. In this paper [30], creators have proposed an improved Co-FAIS insusceptible framework for DoS assault in WSN. Co-FAIS invulnerable framework is the interruption recognition model first ongoing framework that contrasts current framework and typical framework to perceive the assault by utilizing fluffy rationale. Be that as it may, it has a few disservices like needs capacity of simple learning and based model for example single which don't changes with change on schedule during the cycle of recognition.

Raksha Upadhyaya, Uma Rathore Bhatta, et.al, (2016), have investigated that open nature of remote sensor organizations (WSN) brings about greater weakness to outside assaults. Various assaults like forswearing of administration, dark opening and sink opening exceptionally influence the general yield of the organization. DDOS assaults the most perilous assaults which enormously mischief and hamper the total working of the organization. The assaults in the organization are dispatched by the arrangement of vindictive hubs among the first hubs and cause DDOS assault. In this paper [24], creators have proposed an ideal answer for the counteraction of DDOS assault from sensor organizations. In proposed arrangement they have utilized powerful source steering. For the location and counteraction of assaults, the upset hubs energy was used. The change in DSR alongside some security component for DDOS assault has been proposed in this paper. For this reason, they completed four stages. The assessment of battery charge of every hub forestalls the previously mentioned assault by recognizing malevolent hubs. Since a sensor network doesn't have any boycott to recognize malignant hubs subsequently a closure technique can be applied to limit these irresistible hubs. With the assistance of this irresistible hubs are taken out from the correspondence and begin utilizing elective approaches to move information or bundles. Qualnet 5.2 test system was used in this paper for the execution of the proposed conspire.

KatarzynaMazur, Bogdan Ksiezopolski, et.al (2016) introduced the issue of DDoS assault and its staggered examination in the remote sensor network as it corrupts the usefulness of the entire framework. They proposed the two security levels with eight characterized situations and distinctive number of bargained gadgets. Creator in this paper examined the sink's exhibition and energy utilization under the DdoS assault utilizing reproductions. Subsequent to acquiring every one of the outcomes from the reproductions, another sort of (DdoS) assault is recognized

3. METHODOLOGY

In WSN, sensor nodes can relate or dissert the network at whatever point they need in light of property of decentralization. In view of the decentralization property any node can go into the network organization that node can be the genuine node or the malignant node. Presence of malignant node inside the network organization is fit for setting off unique and inert attacks this is a result of dynamic nature of the network organizations. The malicious node can spoil the introduction of the network organization. The network execution in regards to specific limits has been impacted by the unique attacks. There are such incalculable attacks possible on WSN, in Distributed-Denial of Service (DDOS) attacks; toxic nodes changes various assaults like flooding assault, dull opening assault and warm opening assault to end the overall working of organization. The Denial of organization is the unique kind of assault wherein malicious hubs flood the veritable hubs with the unsavory groups to diminish network execution. The dispersed renouncing of organization is the advancement kind of DOS assault in which malicious hub pick its slave and slaves will flood the veritable hub which the unforgiving bundles and it decline network execution. This investigation work, relies upon the ID and imprisonment of malicious hubs from the organization which are fit to trigger DDOS attack in the organization. In the proposed method, the key specialists are molded in the organization and each hub in the organization will enlist itself to the primary hub with their data rate and bandwidth usage. Exactly when all of the hubs start sending data in the organization, and when the DDOS assault is set off in the organization and throughput of the organization get diminished to edge regard then malicious center recognizable proof measure starts. During the time spent harmful hub recognizable proof, the hubs which are sending data over the edge regard are considered as malevolent hub and methodology of gatekeeper canine is applied that whether these hubs are sending data packages or control bundles. Exactly when the hubs are sending the data bundles, by then that center points are considered as the slave hubs. The procedure of screen mode is applied on the slave hubs which would then have the option to separate the organization traffic. Right when the slave hubs gain the power packages from the other hub, by then the hub which send control group is perceived as the poisonous hub in the organization. The proposed strategy is applied under the reproduced climate so presence of malignant hubs can be settled successfully which is reliable of causing DDOS assault in the organization. The edge is depicted using the condition showed up underneath:

set timer = rt(msg*data) node "" - (tt(msg*data) node ""+ size of(msg*data nsnode "") check node_()*address_alloc[];
select timer;

Where,

data = this attribute will represent the rate of data transmitted in given time.
size = this attribute will represent the size of data in bytes
node_()*address_alloc[] = this attribute will represent the address of node which includes node number and their IP address.
timer = this attribute represents amount of data transmitted by particular node in the given amount of time

4. PROPOSED ALGORITHM

Input: The nodes present in network which are genuine i.e Sensor nodes

Output: The nodes which are ingenuine i.e Detected malicious nodes

1. Deploy wireless sensor network with limited number of sensor hubs
2. To serve their respective datarate every node should register with the defined key server.
3. If (the value of Throughput is reduced to threshold value)

   Identify the node which is sending data above threshold value (Node send data with high data rate== true)

   Check traffic type of nodeif (traffic == data traffic) Define node= slave node

4. Else

   By applying the monitor mode technique identify with node is sending controlpackets

   The node which will be sending control packets to slave node is detected as malicious nodes i.e in-genuine node

   Communication continues in the network.

5. RESULTS

The technique as proposed was compared with existing technique, it proved to be more reliable and efficient. The comparisons are based on parameters as throughput, energy and packet drop.

The packet drop of proposed and existing procedure is looked at changed occasions. In the proposed method, the packet drop is less because of disengagement of DDOS assault in the organization. In existing framework the normal bundle drop was 1.6 yet in proposed framework the normal bundle drop is 0.6.

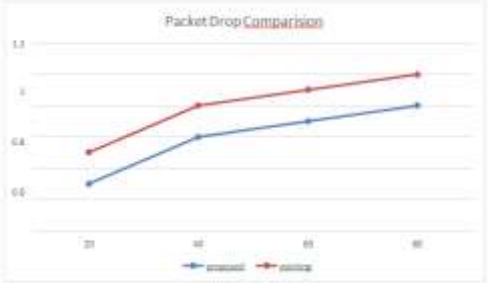

Fig 3 Packet Drop Comparison

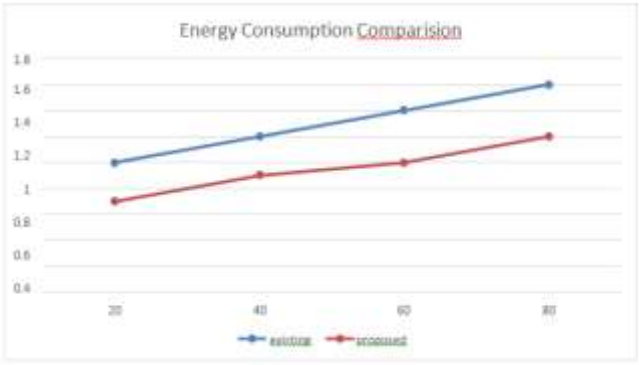

Fig 4 Energy Consumption Comparison

The energy utilization of proposed and existing method is looked at changed spans. It is being dissected that energy utilization of proposed method is diminished due segregation of assault in the organization. In existing framework normal energy utilization was 1.3 however in the proposed framework energy utilization diminishes to 1.15.

The technique that is proposed is much trustworthy and efficient when compared with existing technique. On the parameters of throughput, energy and packet drop the proposed technique is efficient. The statement is evident from the table given below.

Parameters	Existing Technique	Proposed Technique
Throughput	**14**	**19.25**
Energy Consumption	**1.3**	**1.15**
Packet Drop	**1.6**	**0.6**

REFERENCES

[1] Manhee Lee, Eun Jung Kim, Cheol Won Lee, "A Source Identification Scheme against DDoS Attacks in Cluster Interconnects", 2004, Proceedings of the 2004 International Conference on Parallel Processing Workshops (ICPPW'04)

[2] A.K. Pathan, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. 8th International Conf. Advanced Communication Technology, vol. 2, pp. 1043-1048, 2006.

[3] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in wireless sensor networks", WCE, vol.1, pp 5-15, 2008.

[4] Healy M, Newe T, Lewis E, "Security for wireless sensor networks: A review in Sensors Applications Symposium (SAS)", 2009 IEEE, vol. 3, pp. 80-85, 2009.

[5] Kaur, K., & Kumari, N. Evaluation and Analysis of Active RFID Protocol in Wireless Sensor Networks, vol. 3, pp. 121-129, 2010.

[6] P. Mohanty, S. Panigrahi, N. Sarma, and S.S. Satapathy, "Security Issues In Wireless Sensor Network Data Gathering Protocols: A Survey", Journal of Theoretical and Applied Information Technology, vol. 13, pp. 14-27, 2010.

[7] Priyanka Goyal, Sahil Batra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, vol.9, pp.11-15, 2010.

[8] M.H. Anisi, A.H. Abdullah, S.A. Razak, "Energy-Efficient Data Collection in Wireless Sensor Networks", Wireless Sensor Networks, vol. 3, pp. 329-333, 2011.

[9] Jiang, L., Bing Fang, & Li., "Energy optimized approach based on clustering routing Protocol for wireless sensor networks", CCD Conference. IEEE, vol. 5, pp. 181-190, 2011.

[10] M.K. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.

[11] Omer Demir, Bilal Khan, "Finding DDoS Attack Sources: Searchlight Localization Algorithm for Network Tomography", 2011, IEEE.

[12] ZHANG Yi-ying, LI Xiang-zhen, LIU Yuan-an, "The detection and defense of DoS attack for wireless sensor network", 2012, Science Direct, 19(Suppl. 2): 52–56.

[13] Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "Issues and Challenges in Wireless Sensor Networks", IEEE International Conference on Machine Intelligence Research and Advancement, vol 4, pp.58-62, 2013.

[14] Gouvy, N., Hamouda, E., Mitton, N., & Zorbas, D., "Energy efficient multi-flow routing in mobile Sensor Networks", IEEE In Wireless Communications and Networking Conference (WCNC), vol. 3, pp. 1968-1973, 2013.