ISSN (Online) 2394-6849

International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE)
Vol 4, Issue 5, May 2017

Review on Path Based DOS Attack Prevention in WSN using Improved PSO techniques with QoS Parameters

[1]A.Praveena, [2] Dr.E.S.Shamila, [3] R.N.Devendra Kumar

[1] Assistant Professor, [2] Associate Professor, [3] Assistant Professor

Abstract - **Wireless sensor networks are more susceptible to various attacks due to the deployment in aggressive environment. These networks offer the promise of exciting new technological developments. They are emerging as one of the most reliable technologies for implementing ubiquitous computing ultimately leading to an all-pervasive paradigm of computing infrastructure. They are increasingly become viable solutions to many challenging problems and will successively be deployed in many areas in the future such as in environmental monitoring, business, and military There have been significant contributions to overcome many weaknesses in sensor networks like coverage problems, lack in power and making best use of limited network bandwidth, however; work in sensor network security is still in its infancy stage. In contrast to resource-rich networks such as the Internet, a WSN is less stable, more resource limited, subject to open wireless communication, and prone to the physical risks of in-situ deployment. Due to their inherent limitations, WSNs are especially sensitive to Denial of service (DoS) attacks and can cause serious damages. This paper addresses an especially damaging form of DoS attack, called PDoS (Path-based Denial of Service). In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets. The main idea of negotiation based routing in WSNs is to suppress duplicate information and prevent redundant data from being sent to the next sensor or the base-station by conducting a series of negotiation messages before the real data transmission begins. Negotiation messages can include optimum value using Particle Swarm Optimization along with data**

Keywords: **Denial of Service, Sensors, Energy Efficient.**

I. INTRODUCTION

Recent advancements in the design and fabrication of low power VLSI circuitry, along with wireless communications, have broadened the applications prospects for wireless sensor networks. These networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real world challenges and are expected to play an essential role in the upcoming age of pervasive computing. Sensor networks are given by a large number of sensor nodes which collect and disseminate environmental data and are densely deployed either inside or close to a phenomenon of interest with computational capabilities connected through wireless links. Each sensor node is an independent, low-power, smart device with sensing, processing and wireless communication capabilities. These networks are an important ingredient of “anywhere and anytime” ubiquitous wireless next generation communication infrastructure. From national defense, medical applications, to the environment, the data delivered from the sensor networks are unstructured, using their own format and protocols. Sensor networks are delivering near-real-time information and have a role of reliable monitoring and control of variety of applications based on environmental sensing. Extracting this information to gain knowledge and understanding is one of the greatest challenges faced today.

In spite of the diverse applications, they pose a number of unique technical challenges due to the following factors: Adhoc deployment, unattended operation, untethered, and dynamic changes. But to perform any task in sensor network, it is necessary to ensure the best possible utilization of sensor resources so that the network could be kept functional as long as possible. In contrast to this crucial objective of sensor network management, a Denial of Service (DoS) attack targets to degrade the efficient use of network resources and disrupts the essential services in the network. DoS attack could be considered as one of the major threats against WSN security.

As a result, it makes the system or service unavailable for the other legitimate sensor nodes. In this paper, the Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to wireless sensor networks.

A. Contributions of the Paper

This paper is intended to be an introduction to Wireless Sensor Networks—with an emphasis on structural and environmental monitoring applications. A thorough but general survey of the area and referring to several papers in the computer science and engineering literature detailed information were given. In this paper for achieving security the authors have proposed to suppress duplicate information and prevent redundant data from being sent to the next sensor or the base-station by conducting a series of negotiation messages including optimum value before the real data transmission begins. The rest of the paper is described as follows. Section 2 discusses the background information for architecture of WSN and components of a sensor node. The motivation for the proposed scheme presented is discussed in Section 3. Section 4 discusses related work. Section 5 discusses the proposed scheme. Conclusions and future work conclude the paper.

II. SENSOR NETWORKS ARCHITECTURE

The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and perform partial or no processing on the data. Each sensor node has the required infrastructure to communicate with the other nodes. Data are routed back to the sink/base station by a multihop infrastructure less architecture through the sink. A distinguished special type of node is called as gateway node. Gateway nodes are connected to components outside of the sensor network through long range communication (such as cables or satellite links), and all communication with users of the sensor network goes through the gateway node.

The sink node communicates with the task manager via core network which can be Internet or Satellite. Since Sensors are low cost, low power, and small in size, the transmission power of a sensor is limited. The data transmitted by a node in the field may pass through multiple hops before reaching the sink. Many route discovery protocols (mostly inherited from Ad hoc networks) have been suggested for maintaining routes from field sensors to the sink(s). Due to low memory, scarcity of available bandwidth and low power of the sensors, many researchers considered these separate route discovery mechanisms undesirable.

Once sensors are deployed they remain unattended, hence all operations e.g. topology management, data management etc. should be automatic and should not require external assistance. In order to increase the network life time, the communication protocols need to be optimized for energy consumption. It means a node must be presented lowest possible data traffic to process.

The sensor node is made up of four basic components: a sensing unit, a processing unit, a transceiver unit and a power unit. They may also have additional application-dependent components such as a location finding system, power generator and mobilizer. Sensing units are usually composed of two subunits: sensors and analog to digital converter. The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed to the processing unit. The processing unit is generally associated with a small range a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. A transceiver unit connects the node to network. One of the most important components is the power unit. Power unit may be supported by power scavenging units such as solar cells. There are also other subunits that are application dependent.

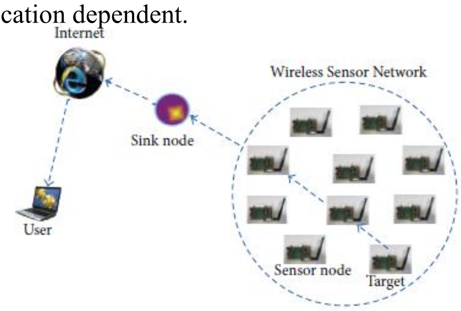


Fig 1: WSN Architecture

The emergence of sensor networks as one of the dominant technology trends in the coming decades has posed numerous unique challenges to researchers. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Cost constraints and the need for ubiquitous, invisible deployments will result in small sized, resource-constrained sensor nodes. While the set of challenges in sensor networks are diverse, we focus on fundamental security challenges in this paper.

A. Security Requirements in WSN

The aim of security mechanism is to protect the information from attacks. In wireless sensor networks security requirements make sure that network services are available even in presence of DoS and also in presence on any vulnerability. Only authorized WSN node can be involved in information passing. It also ensures that a malicious node cannot masquerade as trusted node. There has to be confidentiality and integrity in message, what sent from authorized sender to receiver. Data freshness and non-repudiation is also to be taken into account with the security measures, applied or to be. Since the tiny sensor nodes are randomly deployed and operated in unattended environment so the security requirements include self-organization of node which further includes self-configuration, self-management (autonomous) and self-healing (fault tolerant).

III. DENIAL OF SERVICE ATTACKS IN WSN

Denial-of-Service (DoS) attacks are recognized as one of the most serious threats due to the resources constrained property in WSN. Because the sensor nodes are battery powered, increasing the autonomous lifetime of a WSN is a challenging optimization problem. Most of the WSN's routing protocols are easy and straightforward because of this reason they are vulnerable to attacks. The Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to WSN and it is an explicit attempt to prevent the legitimate user of a service or data. By preventing a single device from sending traffic or by preventing the communication between the network, DoS attacks target availability of services to the users [1].

The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: consumption of bandwidth or consumption of processor time, obstructing the communication between two machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming.

A. Path Based DOS Attack

The DoS attacks are certainly not a new phenomenon. There are standard techniques used to cope up from common DoS techniques. Some of the major types of DoS attacks are Jamming, node destruction, denial of sleep, spoofing, replaying, hello flood attack, homing, SYN flood, de-synchronization, path based attacks, reprogramming attacks etc. This paper focuses on path based DoS attacks. In a path based DoS attack, an attacker overwhelms the sensor nodes a long distance away by injecting spurious packets or replayed packets that floods a multi hop end to end communication path. This attack consumes network bandwidth and also drains the energy of node. Combining packet authentication and anti replay can prevent from path based DoS attack. In this a adversary injects replayed packets to flood the end to end communication between two nodes every node in the path towards the base station forwards the packet, but if large number of fake packets are sent all of these will become busy. So, this attack consumes network bandwidth and energy of the nodes [11].

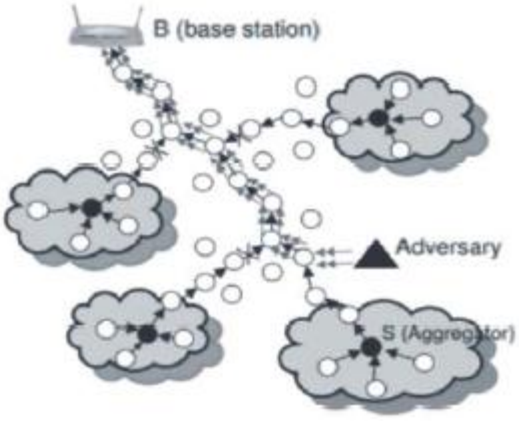


Fig 2: Path Based DoS Attack

The path based DOS attack is another category of physical attaches and typically, combination of jamming attack. In this attack, the attacker sends a large number of packets to the base station. The effects of this physical attack are disturbing the network availability and node batteries exhaustion. The path based DOS attack is belonged to modification and fabrication class and availability and authenticity are main threats for WSN network. In below Figure 2 shows the nodes affected by path based DOS attack. Initially the nodes along the path will rapidly become exhausted and after this, the second nodes downstream from nodes along the main path and unable to communicate with base station. This is because of tree-structured topology the path based DOS attacks can disable a much wider region than simply a single path.

IV. PREVIOUS WORK

Because of the problems mentioned in previous section security is commonly considered as a delicate problem. One security aspect that receives a great deal of attention in WSN is path based DoS attack. WSNs are vulnerable to the DoS attacks since they are energy-constrained devices without a central powerful monitoring point [1]. Meanwhile, there are deferent types of DoS attack in the layers protocol of sensor network. In [6], the authors designed a one-way hash chain (OHC) to protect end-to-end communications in WSNs from path-based DoS attacks. The OHC deploys an OHC in each intermediate node of path to detect a PDoS attack. OHC put a new OHC number for every message from source. Therefore, the messages, which can be authenticated correctly in the chain, can only be transferred. The proposed solution is lightweight, tolerates burst packet losses, and can easily be implemented in modern WSNs. However, OHC did not provide any protection for the data transmission between the member nodes and the CH, which is threatened by the attacks. Therefore, it not provide any protection for the head of the network, the attacker node may attack head and disrupt overall functions of the network.

In [2]; two types of attacks on WSN that are jamming and flooding has been discussed and this paper provides an efficient technique for detection of flooding and jamming attacks. The method discussed in this paper provides improved performance over the existing methods. Article [3] examines how attacks happen in WSNs and differentiate these attacks by conducting a survey. However, the main aim of this analysis is to examine how to prevent such attack in the WSNs by creating a sound understanding about various kinds of attacks in WSNs.

[10] Shows that the absence of central monitoring unit makes it vulnerable to several attacks. Denial of service attack (Dos) is an active internal attack which results in performance degradation of the wireless sensor network. This attack can be localized or distributed in nature based on intent of attack. In this paper, authors using modified variant of Ad-hoc On Demand Distance Vector (AODV) protocol to analyze the effect of Dos attack on system performance and later apply the prevention scheme to analyze the change in network performance.

In paper [16] authors proposed a scheme using game theoretic approach for preventing DoS attacks in WSN. This scheme uses two concepts: utility based source routing which computes the total utility of each source route in data packets.

This routing is a dynamic routing mechanism. The other concept is based on a reputation list where each node earns rating from its neighbouring nodes. The disadvantages in this scheme are the node that has less reputation does not get selected in source routing results complexity in routing and difficult to detect compromised nodes if the nodes are large in number.

The scheme proposed in paper [17] is a flexible novel framework for detection of denial of service attacks. This is a hierarchal framework consists of two important stages: attacks detection stage and the other is defending stage where various defensive methods are utilised to overcome detected attacks. By this scheme only flooding, jamming, and exhaustion attacks can be detected.

The authors in paper [18] proposed a watchdog scheme that detects the misbehaviour nodes and is achieved by using two concepts: watchdog and a pathrater. In the network, every node implements a watchdog which constantly monitors the activities of packet forwarding of their neighbours. The path-rater rates the reliability of transmission of all the alternative routes to a destination node. The disadvantages of this proposed mechanism are that it is not practical for any general routing protocols rather than source routing protocol and the problem of collusion among the compromised or malicious nodes remains unsolved. In paper [19] proposed a novel RSA based framework to prevent the DoS attacks ensures that the malicious nodes prior to the counterparts exhausts the resources. The scheme presented three methodologies to establish an ephemeral key. In [20] for distributed wireless sensor networks (WSN) a scheme is proposed that prevents the possible DoS attacks whenever a packet be intercepted by using a broadcast- key management mechanism. A number of numerical calculations and hashing operations are there to invalidate the first intercepted packet. The Public key cryptography (PKC) technique in [21] prevents only certain DoS attacks which targets on the energy of batteries in WSN. The proposed scheme is a combination of Elliptic curve cryptography (ECC) based key generation and DoS mitigation scheme.

A novel cluster based intrusion detection and prevention technique is proposed in [22] to prevent DoS attacks mainly misdirection attacks. The technique builds the clusters from mobile nodes that are in communication range with each other. Among these a node is elected as cluster head (CH) based on two things: fairness probability of a node as a CH should be equal and efficiency- a node having high efficiency should be selected periodically from the cluster. The authors in paper [23] designed a novel Message Observation Mechanism (MoM) for preventing DoS attacks. This mechanism utilizes similarity function which is based on spatio temporal correlation for identifying the frequency attacks and content attacks. To isolate the compromised or malicious nodes the MoM adopts the reroute and rekeys counter measures. The analysis shows that this solution reduces the energy consumption but detects and defends the DoS attacks.

V. PROPOSED WORK

To detect DOS attack, we normally consider two aspects, the number of messages and the content of messages. After receiving the message it check whether the received message is normal , abnormal or new message and if the message is if the message is normal then compare the counter value with the threshold value if it greater then consider that sender as a attacker node , if the message is a abnormal then consider that sender node as attacker node, if the message is new one then add that message to the normal message list and also check the threshold value if it crosses then consider that node as malicious node.

A. Algorithm for Detecting the DOS Attack

Step 1: Receive the input message.
Step 2: Check whether the message belong to normal or abnormal messages
Step 3: If the message is abnormal then consider the sending node as malicious node.
Step 4: If the message is normal then compare the count and threshold value, if it crosses the threshold value then consider that sending node as a attacker node
Step 5: go to step 1

After determining the attacker node, cluster head send the notification message to the authenticated server node, server add that information in its attacker list , generate and distribute the new keys to all the nodes in that cluster region except the attacker node. Also cluster head broadcast the attacker id to all its sensor nodes and inform that don’t receive the message from that id. Even though attacker node try to communicate with the node it not authenticated so communication get discarded. Suppose if the attacker node try to communicate with other cluster head, there also it not get authenticated.

B.Algorithm for Cluster Head Selection

We use an Enhanced PSO-Based Clustering Energy Optimization (EPSO-CEO) algorithm to form clusters and cluster head selection with a combination of centralized and distributed method using static sink node.

4.1. Particle Swarm Optimization (PSO). Particle Swarm Optimization (PSO) is a population-based optimization scheme. The random solutions of the system are initialized with a population and search optimal solutions in each generation [20]. The potential solutions in each generation are called particles. Each particle in PSO keeps the stored record for all its coordinates which are related to obtaining the better solution by following the current best particles. Fitness function of every particle is executed and the fitness value (best solution) is calculated and stored. The fitness value of the current optimum particle is called"pbest." PSO optimizes the best population value that is obtained so far by any particle in the neighbors and its location is called lbest.

When all the generated populations are considered as topological neighbors by a particular particle, then the best value is chosen among the generated population and that particular best value is the best solution and it is known as gbest.

The PSO always try to change the velocity of every particle towards its pbest and lbest. The velocity is determined by random terminologies, which is having randomly generated numbers for velocity towards pbest and lbest localities. From the large deposit of generated solutions, the best one is selected to resolve the problem. The PSO algorithm always stores and maintains a record of results for three global variables such as target value or condition, gbest, and stopping value. Every obtained particle of PSO contains the following details.

(i) A data which can represent a global solution.
(ii) Value for velocity which will indicate the amount of data to be changed.
(iii) lbest value.

C. Cluster Formation

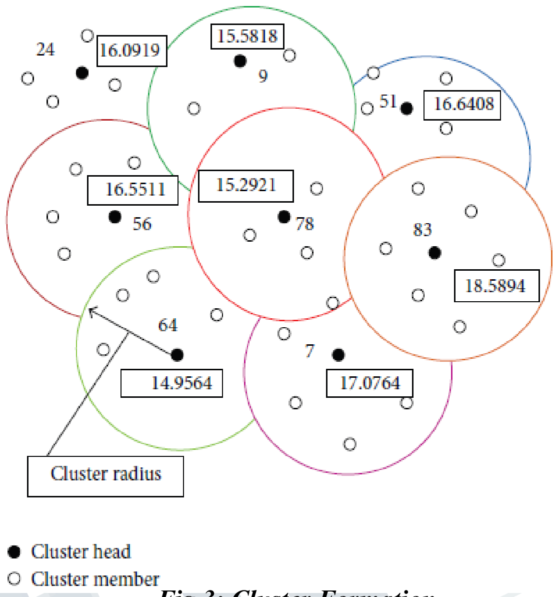


Fig 3: Cluster Formation

The cluster is formed by the base station or sink on the basis of centralized clustering. For clustering base station (sink) broadcasts info collection message to all sensor nodes. Sensor nodes after receiving this message start to send its node information such as node id, location (distance from the base station in X and Y position), energy loss and energy loss ratio (velocity), and current energy to send base station. Then base station initiates the clustering process steps as follows.

Step 1 : Conversion of problem into the PSO space in which the PSO particle has two dimensions such as particle position
and velocity.
Step 2 : Estimation of fitness value using fitness function.

The fitness function for PSO based clustering is to optimize the average distance and average energy of the member nodes and from the current cluster head and headcount. Figure 3 shows the cluster formation using PSO.

D.Cluster Head Selection

After clustering, each sensor node maintains "my cluster list." It includes current cluster id, velocity, location, and energy. Then the round procedure is initiated to perform cluster head selection. Cluster head selection by implementing PSO algorithm is shown in Fig 4.

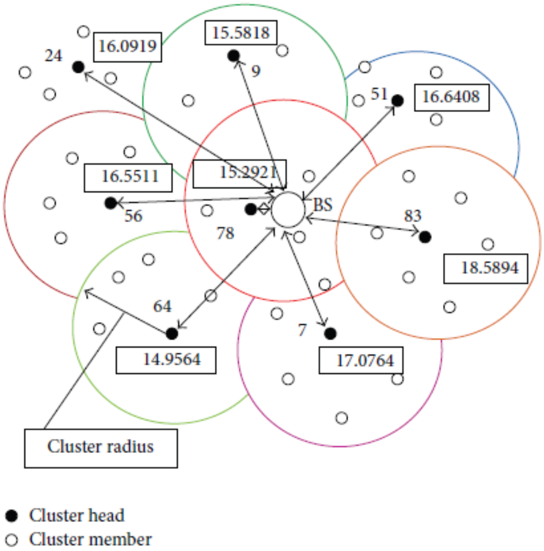
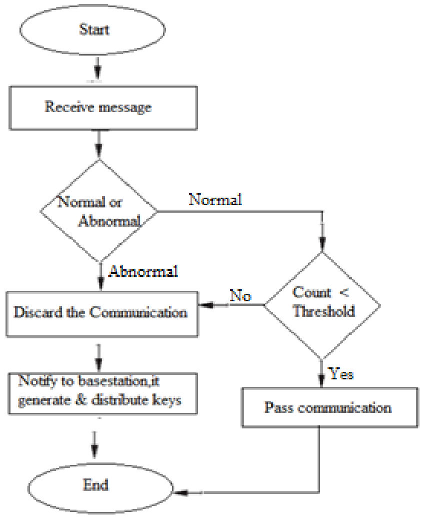


Fig 4: Cluster Head Selection

E. Algorithm for Avoiding the DOS Attack



Step 1: Cluster head send notification message, consist attacker details to the server.

Step 2: Server store that info in its history record ,generate and distribute the new keys to all the nodes in the cluster region except the attacker node.

The overall process flow is shown in following diagram4. First start the server node and setting the attacker node. The cluster head receive the message from the sensor node and it verify whether its normal or abnormal, if it abnormal or , if the message is normal then compare count with the threshold value , if it crosses then consider that node as attacker node and discard the communication with that node. Cluster head notify to the base station , the base station generate and distribute the new key to all other nodes in cluster region then consider that node as attacker node and inform to the base station else pass the communication with that node.

CONCLUSION

The wireless sensor networks continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital for its proper functioning. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation, etc. In WSNs, an adversary can launch with little effort a path-based denial of service (PDoS) attack that will have a severe widespread effect and reduces the performance of the systems, disabling nodes on all branches downstream of the path, due to the tree-structured topology of WSNs. Special prevention techniques are required to deal with the DoS attacks in WSNs. In this paper, we have proposed a lightweight and efficient mechanism using that allows intermediate nodes to defend against PDoS attacks by detecting replayed and spurious packets. We have proposed a novel and robust set of mechanisms to form clusters and to select the cluster head in WSN. At last, DoS attacks are effective at all the layers, so a special attention is required for their detection as well as prevention.

REFERENCES

[1] S. Chen, B. Mulgrew, and P. M. Grant, “A clustering technique for digital communications channel equalization using radial basis function networks,” IEEE Trans. on Neural Networks, vol. 4, pp. 570-578, July 1993.

[2] Chan, Haowen, and Adrian Perrig. "Security and privacy in sensor networks." Computer 36.10 (2003): 103-105.

[3] Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.

[4] Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." Computer 35.10 (2002): 54-62.

[5] Li, Bai, and Lynn Batten. "Using mobile agents to detect node compromise in path-based DoS attacks on wireless sensor networks." Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on. IEEE, 2007.

[6] Xu, Wenyuan, et al. "Jamming sensor networks: attack and defensestrategies." Network, iEEE 20.3 (2006): 41-47.

[7] Jain, Sushil Kumar, and Kumkum Garg. "A hybrid model of defense techniques against base station jamming attack in wireless sensor networks." Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on. IEEE, 2009.

[8] Badal, Tapas, and Dipti Verma. "A Modular Approach for Intrusion Detection System in Wireless Networks." (2011): 57-61.

[9] Xie, Miao, et al. "Anomaly detection in wireless sensor networks: A survey." Journal of Network and Computer Applications 34.4 (2011): 1302-1325.

[10] M. Kaur, A. Jain and A. K. Goel, "Energy Efficient Two Level Distributed Clustering Scheme to Prolong Stability Period of Wireless Sensor Network", International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 68-73

[11] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[12] Deng, J., Han, R., and Mishra, S. (2005), Defending against Path-based DoS Attacks in Wireless Sensor Networks. ACM SASN’05, November 7, 2005, Alexandria, Virginia, USA, pp 89-96.

[13] Doddapaneni.krishna chaitanya “Analysis of Denial-of-Service attacks on WSN using simulation” Middlesex University.

[14] Al-sakib Khan Pathan “Denial of Service in Wireless sensor networks: issues and challenges.”Advances in communications and Media Research ISBN 978-1-60876-576-8.

[15] A. Agah, S. K. Das, and K. Basu, “Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling, ” Proceedings of 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), Washington, D.C., Nov. 2005.

[16] Afrand Agah, Mehran Asadi and Sajal K, “Preventing of

DoS Attacks using Repeated Game Theory”, May 2007.

[17] Ouyang Xi, Tian Bin, Li Qi, Zhang Jian-yi, Hu Zheng-Ming, Xin Yang,“A Novel Framework of Defense System Agaist DoS attacks in WSN”, IEEE 2011.

[18] S. Marti, T. Giuli, K. Lai, M. Baker,“Mitigating routing misbehaviour in mobile ad hoc networks”, In Proceedings of ACM International Conference on

Mobile Computing and Networking (MOBICOM) 2000.

[19] O. Arazi, H. Qi, D. Rose,“A Public Key Cryptographic Method for DoS mitigation in WSN”, IEEE 2007.

[20] “A new broadcast key management scheme for distributed WSN”, 2009

[21] “A public key cryptography method for DoS mitigation in WSN”, 2007.

[22] “A cluster based intrusion detection and prevention technique in misdirection attack inside WSN”, 2013

[23]"Yi-ying ZHANG, Xiang-zhen L, Yuan-an LIU, “The detection and defence of DoS attack for wireless sensor network”, Elsevier Journal of China Universities of Posts and Telecommunications, Vol. 19, Supplement 2, October 2012, pp. 52-56.

[24] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.