**Imperial Journal of Interdisciplinary Research (IJIR)**
**Vol-3, Issue-2, 2017**
**ISSN: 2454-1362,** http://www.onlinejournal.in

# Probing and Removal of Denial of Service Attack in Wireless Sensor Networks

Pallvi Sharma[1] & Amarvir Singh[2]
[1]Dept. of Computer Science, Punjabi University, Patiala, Punjab, India
[2]Assistant professor, Dept. of computer science, Punjabi university, Patiala Punjab, India

***Abstract***- *The number of security breaches is on a sharp increase and so is the damage and losses. Although the actual amount of damage from malicious codes has not been fully revealed, it is enormous, and such damage occurs from common services such as in cases of game hacking, defense services messenger phishing, voice phishing, and so on. Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications. Denial of Service (DoS) attack is one of them. Each layer has different type of DoS attack. Tackling this attack requires knowledge of types of DoS as well as various defense mechanisms applied to overcome them. In this project, an introduction to DoS attack along with various countermeasures has been discussed. For simulation, network simulator NS2 is used under Ubuntu 12.0.4 OS.*

***Keywords****—defense, Security attacks, revealed, NS2, Ubuntu.*

## I. INTRODUCTION

Wireless sensor networks are required as:

- Sensing + CPU + Radio = Thousands of potential applications
- Provide a bridge between the real physical and virtual worlds

Wireless communications have provided low cost and small size sensor nodes. A wireless sensor network consists of thousands of limited resource sensor nodes, used to collect information from the surrounding environment. The aim of Denial of service attack is to make services unavailable to legitimate users, and current network architectures allow easy-to-launch and hard-to-stop DoS attacks.Particularly challenging are the service-level DoS attacks, whereby the victim links are destroyed and flooded with legitimate-like requests attack, in which wireless communication is blocked by malicious radio interference. These sensor nodes are able to communicate with each other and also with base station (BS).

### (1) Security issues related to WSN

Security objectives in sensor systems rely on upon the need to realize what we are going to ensure. We decide four security objectives in sensor systems which are Confidentiality, Integrity, Authentication and Availability **(CIAA).** Security also distinguish the active attacks and passive attacks. Security is quite challenging issue as WSN is not only being deployed in battlefield Applications but also for surveillance, building monitoring, and burglar alarms and in critical systems such as airports and hospitals. Confidentiality is required in sensor networks to protect information traveling between the sensor nodes of the network or between the sensors and the base station; otherwise it may result in eavesdropping on the communication. In sensor networks, it is essential for each sensor node and the base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. The OSI model are required below various attacks and threats are discussed.

**TABLE 1 OPEN SYSTEM INTERCONNECTION LAYER ATTACKS [3].**

| Layer | Threat |
|---|---|
| Physical | Jamming |
| | Tampering |
| Data Link | Exhaustion |
| | Collision |
| Network | Route information manipulating |
| | Selective forwarding |
| | Sybil attack |
| | Sinkhole attack |
| | Wormhole attack |
| | Hello Flood attack |
| Transport | Flooding |
| Application | Clone attack |

(2) **Denial of service Attack**

**DoS** are one of the most serious attacks on the Internet. Payload-based approaches are effective to known denial of service attacks but are unable to be deployed on high-speed networks. To address this issue, flow-based DOS detection schemes have been proposed for high-speed networks as an effective supplement of payload-based solutions. However, existing flow-based solutions have serious limitations in detecting unknown attacks and efficiently identifying real attack flows buried in the background traffic. In addition, existing solutions also have difficulty to adapt to attack dynamics. To address these issues, here we proposes a flow-based DOS detection scheme based on Artificial Immune systems. We adopt a tree structure to store flow information such that we can effectively extract useful features from flow information for better detecting DoS attacks. We employ Neighborhood Negative Selection (NNS) as the detection algorithm to detect unknown DoS attacks, and identify attack flows from massive traffic. Because the strong tolerance of NNS, the proposed solution is able to quickly adapt attack dynamics. The experimental results show that this solution is able to effectively detect unknown DoS attack flows and identify attack flows from background traffic. Meanwhile, the theoretical analysis demonstrates that this system can extract flow features more effectively.

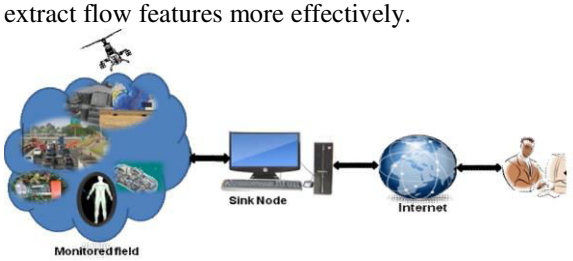



**Fig 1 Occurrence of denial of service attack in WSN**

The experimental results show that this solution is able to effectively detect unknown DoS attack flows and identify attack flows from background traffic. Meanwhile, the theoretical analysis demonstrates that this system can extract flow features more effectively. The first kind of differentiation among various kinds of attack is based on the efficiency of the transmitter and battery power with which the attack takes place. Mote class attacks are having limited power supply, while laptop class devices attack with greater power, capable CPU and sensitive antenna as they are supposed to attack on the powerful devices. Another way to differentiate the adversary is insider and outsider attacks. Insider attack takes place when some authorized participant of the network is turned into a malicious node. Outsider refers to the third party who is not the part of the network. Insider attacks are more difficult to manage. A Denial of Service attack is an attempt to make a computer system (server or client) or some other resource unavailable to legitimate users. Normally, this attack is considered to be a problem of computer network, but for a single CPU also it can be present among various resources. The motive or target of a DoS may vary from person to person but in general, it aims to prevent some services from functioning efficiently either temporarily or indefinitely. Commonly, a DoS attack saturates the victim by excessive communication requests and due to this the targeted system cannot respond the legitimate users at all or responds very slowly, vanishing its effectiveness. It may reset the victim or occupies almost all of its resources obstructing its communication path. Data is collected and managed at application layer therefore it is important to ensure the reliability of data. The system has presented a resilient aggregation scheme which is applicable to a cluster based network where a cluster leader acts as an aggregator in sensor networks. However this technique is applicable if the aggregating node is in the range with all the source nodes and there is no intervening aggregator between the aggregator and source nodes. In hierarchical clustering approach, communication channel between the aggregator and base station has potentially limited bandwidth because the cluster leader as an aggregator itself is a sensor node. To prove the validity of the aggregation, cluster leaders use the cryptographic techniques to ensure the data reliability. Remote correspondences are likewise defenseless against refusal of-administration (DoS) assaults. Associations can find a way to decrease the danger of such accidental DoS assaults. Watchful site overviews can recognize areas where signals from different gadgets exist; the consequences of such studies ought to be utilized when choosing where to find remote access focuses.

**Identification and Mitigation approach**

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.

- A public key, which may be known by anybody, and can be used to encrypt messages.

- A private key, known only by the recipient, and used to decrypt messages.

## Algorithm

- Choose p = 3 and q = 11
- Compute n = p * q = 3 * 11 = 33
- Compute φ(n) = (p – 1) * (q – 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and n are coprime. Let e = 5
- Compute a value for d such that (d ^ e) % φ (n) = 1. One solution is d = 3 [(3 ^ 5) % 20 = 3]
- Public key is (e, n) => (5, 33)
- Private key is (d, n) => (3, 33)
- The encryption of $m = 2^5 \% 33 = 32$
- The decryption of $c = 32^3 \% 33$...

### Simulation and results

The various parameters used for simulation are mentioned below in the respective table.

**Table 2: Parameters used for the experimentation**

| Parameters | Values |
|---|---|
| **Simulator** | NS2 |
| **Terrain Area** | 800 m x 800 m |
| **Simulation Time** | 50 s |
| **MAC Type** | 802.11 |
| **Application Traffic** | **CBR** |
| **Routing Protocol** | **AODV** |
| **Data Payload** | **512 Bytes/Packet** |
| **Pause Time** | **2.0 s** |
| **Number of Nodes** | 15 |
| **Number of Sources** | 1 |
| **No. of Adversaries** | 1 to 3 |

In figure 1, the graph perform the comparison of packet loss parameter where the red line represent existing packet loss and green line shows new packet loss parameter. Here the horizontal axis indicates the time in terms of seconds and vertical axis indicates packet loss in terms of average. It is clear from the graph that proposed technique consumes less amount of packet loss while compared existing technique.

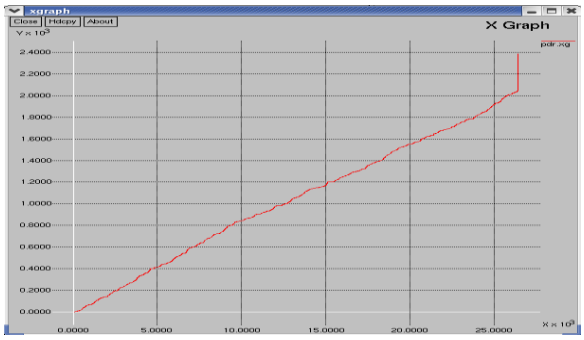



**Figure 1 Performance parameter of packet loss**

In figure 2, the graph represent the comparison of delay parameter where the red line represent existing delay and green line shows new delay parameter. Here the horizontal axis indicates the time in terms of seconds and vertical axis indicates delay in terms of average. Here also the proposed approach is performing better as compare to existing one.

**Figure 2 Performance Parameter of delay**

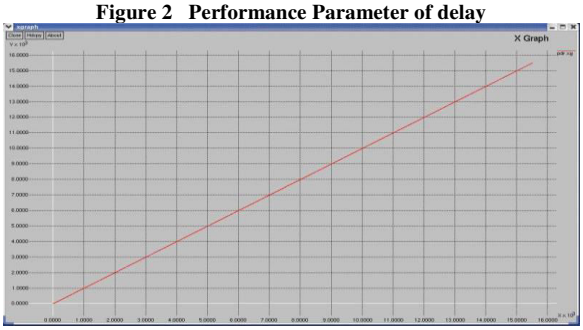
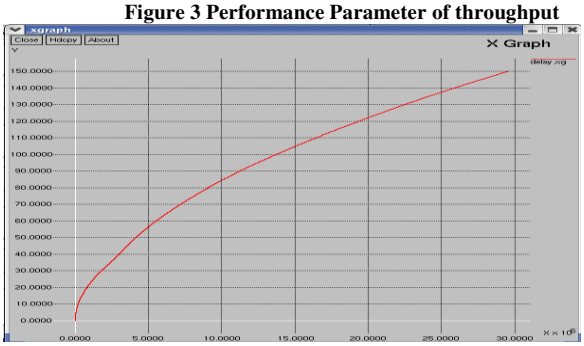



**Figure 3 Performance Parameter of throughput**




In figure 3, the graph represents the comparison of network throughput where the red line represent existing throughput and green line shows new throughput obtained. Here the horizontal axis indicates the time in terms of seconds and vertical axis indicates delay in terms of average. It is clear from the the graph that proposed technique produced better throughput as compared to existing technique.

### Conclusion

A wireless sensor network can be deficient of infrastructure and it can be deployed with some efforts in lieu of existing network framework with suitable environment. The wireless sensor networks no doubt have great potential but still within lies few issues which are needed to conquer indeed. In previous research, most of the solutions which were introduced mostly lack in terms of performance and efficiency of the network. It is not necessary that any proposed algorithm will work absolutely well in presence of a black hole node but there are chances that it might not perform better under collective or numerous black hole attacks. The proposed algorithm in this research will work significantly well in both the single scenario and also in collective or numerous

black hole scenarios. As discussed in the graphs above in existing scenario the value of throughput calculated is around 38% and in new technique throughput calculated approximately is 98 % that is better than previous work done.

Similar, in case of delay output the value of existing technique is approximately 96,000 but in proposed technique the value is 52,000 respectively. Also in term of packet loss the proposed technique drops very less packet as compared to existing technique.

## *References*

[1] Riecker, Michael, Daniel Thies, and Matthias Hillock. "Measuring the impact of denial-of-service attacks on wireless sensor networks". In Local Computer Network (LCN), 2014 IEEE 39th conference on IEEE, 2014,296-304.

[2] Gaurav Kumar Gupt, Mr. Jitendra Singh, "Truth of D-DOS Attacks in MANET", vol.10, issue 15, GJCST 2010.

[3] Sahu, Sonali Swetapadma, and Manjusha Pandey. "Distributed Denial of Service Attacks: A Review".International Journal of Modern Education and Computer Science (IJMECS) 6, no. 1 (2014), 65.

[4] Zargar, Saman Taghavi, James Joshi, and David Tipper. "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks". Communication surveys and Tutorials, IEEE 15, no. 4 (2013), 2046-2069.

[5] Hemanta Kumar Kalita and Avijit Kar. "Wireless Sensor Network Security Analysis". International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009,1-9.

[6] Sukhwinder Sharma and Rakesh Kumar Bansal and Savina Bansal. " Issues and Challenges in Wireless Sensor Networks". International Conference on Machine Intelligence Research and Advancement, December 2013,58-61.

[7] Amr M. Kishk, Nagy W. Messiha, Nawal A. El-Fishawy, Abdelrahman A. Alkafs and Ahmed H. Madian. " Proposed Jamming Removal Technique for Wireless Sensor Network". ISROSET-Int. J. Sci. Res. in Network Security & Communication, Vol-**3**(**2**), Apr 2015, PP (**1-14**).

[8] Priyanka Goyal, Sahil Batra and Ajit Singh. " A Literature Review of Security Attack in Mobile Ad-hoc Networks". International Journal of Computer Applications , Volume 9– No. 12, November 2010,11-14.