# Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

[1] N.SRINIVASA RAO, Assistant Professor, DEPT OF MCA, SKBR PG COLLEGE, AMALAPURAM, Andhra Pradesh
Email:- Email:- naagaasrinu@gmail.com
[2] PG Students of MCA, SKBR PG COLLEGE, AMALAPURAM, Andhra Pradesh,
Email:- dorarupa2010@gmail.com

**Abstract** : Internet of Things (IoT) networks are made up of sensors, actuators, mobile, and wearable devices that can connect to the Internet. The fact that there are already billions of such devices on the market, many of which have significant vulnerabilities, poses a serious danger to Internet services as well as to cyber-physical systems that are connected to the Internet. IoT devices in particular are susceptible to hacking and usage as part of a new type of covert DDoS attack called as Mongolian DDoS, which is defined by its worldwide spread nature and small attack size from each source. This study provides an innovative anomaly-based intrusion detection system (IDS) that can quickly recognise and counteract this new type of DDoS attack. The suggested IDS can identify and mitigate covert DDoS attacks with even extremely modest attack sizes per source, according to numerical and test bed investigations.

**Index Terms: -** Intrusion Detection System (IDS), DDoS attack Internet of Things (IoT).

## I Introduction

The development of the Internet of Things (IOT) ranks among the most important technological advances of the preceding ten years [1]. Thanks to the development of multiple micro embedded systems, numerous online services, cloud computing, it is now practically possible to make any isolated system link with another computer. Additionally, the number of devices that connect to the Internet has exponentially increased as a result of the increased functionality and severe size reduction of new System on Chip (SOC) devices. The amount of data collected and shared is increasing in lockstep with the billions of IoT devices currently in use and growing at an exponential rate. As a result, a variety of attackers, hackers, cybercriminals, and even governments have turned their attention to the IOT paradigm. Unfortunately, IoT device security cannot keep up with hardware improvements, and new security flaws are constantly being found, posing a risk to users' privacy and compromising their security. Distributed Denial of Service (DDOS) attacks can be launched using compromised devices, for instance. DDOS is a type of cyber attack in which the attacker bombards an online service with traffic from numerous sources. Volumetric attacks are the most common and straightforward type of DDOS attack because, as their name suggests, they generate enormous amounts of traffic and often do not require the hackers to generate much of that traffic.This study examines stealthy DDOS attacks, which are challenging to detect and defend against due to their global distribution and low-rate anomalous traffic from individual sources, which can easily get by standard filters (i.e., stealth attacks). Although covert DDOS attacks, like the recent Mongolian DDOS strikes, only slightly increase traffic from each source, they are nonetheless possible to stop the targeted service because of their widespread distribution.

## DDOS via IOT

- ✓ Minimal Intrusive Mitigation
- ✓ High Dimensionality
- ✓ Unknown Attack Patterns
- ✓ Early Detection And Mitigation

## .2 Literature survey

**R. Christopher, “Port scanning techniques and the defense against them,” SANS Institute, 2001.**

Port scanning is one of the most often employed strategies by attackers to identify services that they can exploit to access systems. All systems that connect to a LAN or the Internet through a modem run services that scan for popular and uncommon ports. Using port scanning, the attacker can learn what services are running on the targeted computers, who is responsible for them, whether anonymous logins are supported, and whether certain network services require authentication. Port scanning is carried out by sequentially sending a message to each port. If the port is being used, it can be investigated for additional faults based on the type of response. Port scanners are used by network security specialists to identify potential security flaws in the targeted system. Port scans can be discovered and the quantity of data about open services can be regulated with the correct tools, just as they can be done against your systems. Every system that is accessible to the general public has ports that are open and available for use. The objective is to allow only authorised users access to open ports while forbidding access to closed ports.

**S. Staniford, J. A. Hoagland, and J. M. McAlerney, “Practical automated detection of stealthy portscans,” Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.**

A common and crucial procedure is port scanning. Computer attackers typically use it to describe websites or networks that they believe to be hostile. System administrators and other network defence personnel can therefore use portscan detection to spot potential warning signs of a more serious attack. It is also used by network defenders to comprehend and find weaknesses in their own networks. As a result, attackers are curious to know whether or not a network's defences frequently conduct port scanning. Defenders, on the other hand, are less likely than attackers to seek to conceal their portscanning. The remainder of this paper will be referred to as for the sake of clarity as While the defenders struggle to stop the search, the attackers will scan the network. Daily legal and ethical debates over portscanning take place on mailing lists and newsgroups on the Internet. One concern is whether it is morally and legally acceptable to port scan faraway networks without the owners' consent. At the moment, this is a grey area in most nations.

**M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.**

Networked system security has evolved from a minor concern to one that now has a significant worldwide impact on people, corporations, and governments. Attacks on networked systems have drastically increased, and attackers' methods are always changing. To mention a few, these include the availability of knowledge, the security of data storage platforms, and the confidentiality of sensitive information. Depending on these difficulties, cyber terrorism is one of the most important problems in today's society. Cyber activists, criminal organisations, and professionals are now posing a threat to public and national security as a result of the cyber terror that has devastated people and institutions. . Intrusion detection is one of the defences against these assaults. Making Intrusion Detection Systems using Machine Learning is cheap and efficient (IDS). Deep learning and support vector machine (SVM) techniques were used in this study to detect port scan attempts using the fresh CICIDS2017 dataset. Introduction The Network Intrusion Detection System (IDS) is a hardware or software application that monitors networks for malicious activities [1,2]. Depending on the detection method, intrusion detection can be classified as anomaly-based or signature-based. IDS developers employ a range of tactics for intrusion detection. Information security is the process of defending data against unauthorised access, use, disclosure, destruction, alteration, or injury.

## 3 Implementation Study

DDoS assaults employing IoT networks receive much less attention than other security flaws in the IoT context. However, as shown by [4], [7], and [8], it has recently drawn a lot of interest. In [10]–[13], a wide variety of vulnerabilities for which conventional signature-based detection algorithms fall short are described. A 6LoWPAN and IEEE 802.15.4-based defense against a UDP flood attack in an IoT environment is proposed by the authors of [14]. On the other hand, it has high overhead costs, complex architecture, and components that are inappropriate for an IoT environment suggests a technique for agent-based DDoS mitigation. To present their findings, they also make use of the N-BaIoT dataset. Meidan et al suggest using deep auto encoders to detect DDoS assaults at the network level. By training a deep autoencoder for each device in the network, they are able to achieve low false positive rates, but this approach might not scale well to large networks with numerous devices. They also use a window-based majority voting method, which isn't the best for quick detection, to find attacks.

**Disadvantages**

➢ There is less security on outsourced data due to lack of Timely detection and mitigation.

➢ The heterogeneous nature of an IoT network makes parametric anomaly detection approaches for DDoS detection less effective since they assume probabilistic models for nominal and anomalous conditions.

### 3.1 proposed methodology

The proposed system proposes a practical anomaly-based detection and mitigation technique for IoT-based DDoS attacks, particularly the difficult stealthy DDoS attacks with data rate increases per device as low as 10%, which is significantly lower than the rates considered in the literature, and can easily bypass most of the existing approaches. The proposed technique is based on the Online Discrepancy Test (ODIT), a statistical anomaly detection algorithm that mitigates the attack with minimal disruption of regular service, scales well to large systems, does not rely on presumed baseline and attack patterns, and achieves quick and accurate detection and mitigation thanks to its sequential nature. In detecting malicious traffic, Doshi et al compares the performance of prominent machine learning methods such as SVM, knearest-neighbors, neural networks, and others. They do, however, need training data for malicious traffic (supervised anomaly detection), and they extract attributes that are particular to certain IoT devices without taking into account other devices in the network, such as laptops or smart phones. In [21], Nomm et al. suggests detecting IoT botnet assaults by combining feature selection with popular anomaly detection approaches such as one-class SVM.

**Advantages:**

1. A novel detection and mitigation technique for stealthy DDoS attacks is proposed, and its time and space complexity is analyzed;
2. Asymptotic optimality of the proposed detector is proven in the mini max sense as the training data size grows;
3. Solution to a dynamic scenario in which the number of devices in the network changes is provided;
4. A comprehensive performance evaluation is provided using a test bed implementation, the N-BaIoT dataset, and simulations.

## 4. Methodology

**MODULES:**

✓ Monitoring and analyzing both user and system activity2.

✓ Analyzing system configurations and vulnerabilities3.

✓ Assessing system and file integrity4.

✓ Ability to recognize typical attacks patterns

✓ Analysis of abnormal activity patterns

✓ Tracking user policy violations

✓ Signature based Intrusion Detection

✓ Anomaly based Intrusion Detection

✓ Artificial Neural Network based Detection

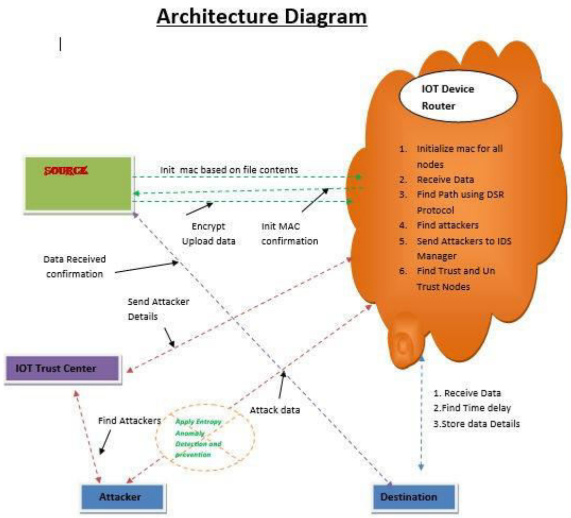


Fig 1:- System Architecture

## 5 Results and Evolution Metrics

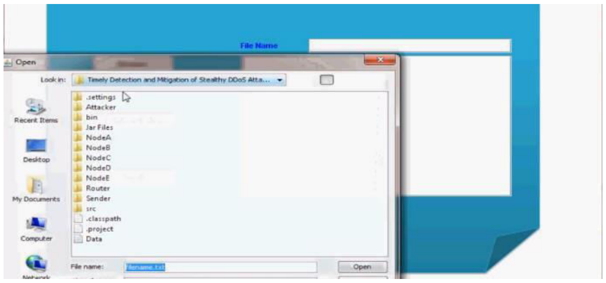
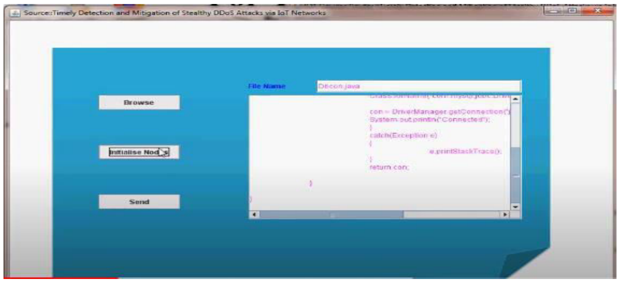


**Figure 1:** Here sender selects the file to send to destination


Source::Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

File Name: Dbcon.java

```
con = DriverManager.getConnection("
System.out.println("Connected");
}
catch(Exception e)
{
        e.printStackTrace();
}
return con;

}
```

**Figure 2:** Contents of the file

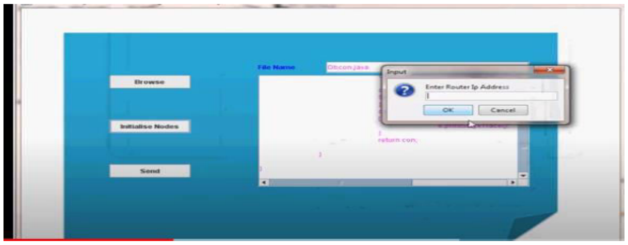
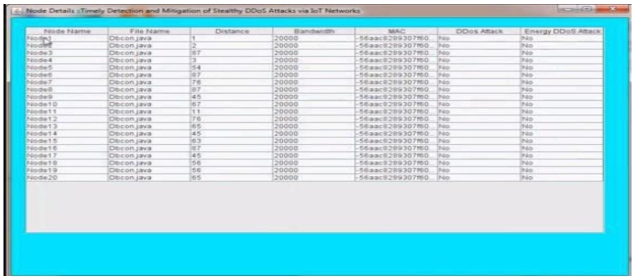


**Figure 3:** Entering into IP address


Node Details ::Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

| Node Name | File Name | Distance | Bandwidth | MAC | DDos Attack | Energy DDoS Attack |
|---|---|---|---|---|---|---|
| Node1 | Dbcon.java | 1 | 20000 | -56aac8289307f60... | No | No |
| Node2 | Dbcon.java | 2 | 20000 | -56aac8289307f60... | No | No |
| Node3 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node4 | Dbcon.java | 3 | 20000 | -56aac8289307f60... | No | No |
| Node5 | Dbcon.java | 54 | 20000 | -56aac8289307f60... | No | No |
| Node6 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node7 | Dbcon.java | 76 | 20000 | -56aac8289307f60... | No | No |
| Node8 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node9 | Dbcon.java | 45 | 20000 | -56aac8289307f60... | No | No |
| Node10 | Dbcon.java | 67 | 20000 | -56aac8289307f60... | No | No |
| Node11 | Dbcon.java | 11 | 20000 | -56aac8289307f60... | No | No |
| Node12 | Dbcon.java | 76 | 20000 | -56aac8289307f60... | No | No |
| Node13 | Dbcon.java | 65 | 20000 | -56aac8289307f60... | No | No |
| Node14 | Dbcon.java | 45 | 20000 | -56aac8289307f60... | No | No |
| Node15 | Dbcon.java | 63 | 20000 | -56aac8289307f60... | No | No |
| Node16 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node17 | Dbcon.java | 45 | 20000 | -56aac8289307f60... | No | No |
| Node18 | Dbcon.java | 56 | 20000 | -56aac8289307f60... | No | No |
| Node19 | Dbcon.java | 56 | 20000 | -56aac8289307f60... | No | No |
| Node20 | Dbcon.java | 65 | 20000 | -56aac8289307f60... | No | No |

**Figure 4: Node details**

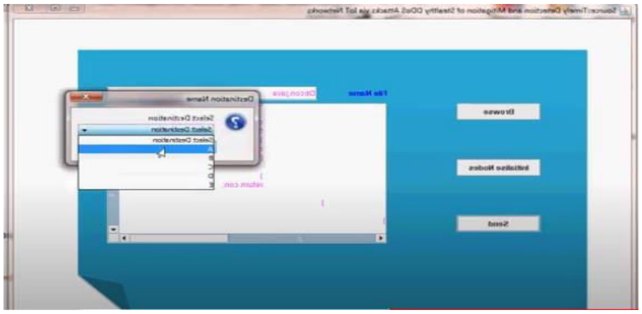


**Figure 5:** selecting destination node

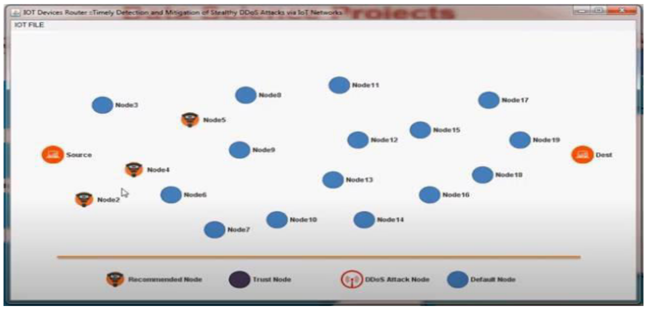


**Figure 6:** Simulation Of Transmission Of Data

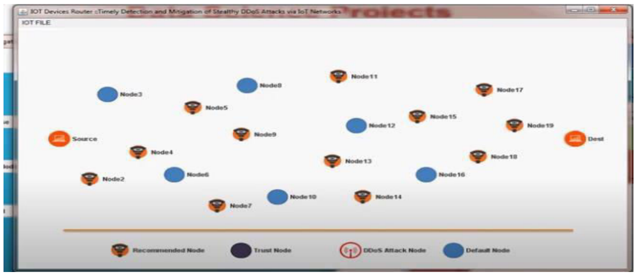


**Figure 7**: Data Transmitted To Destination Node

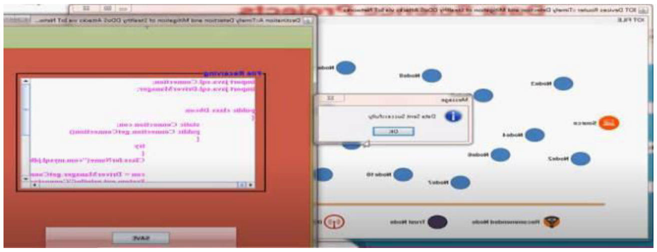


**Figure 8:** Alert Message To Sender And The Data Is Received To The Receiver

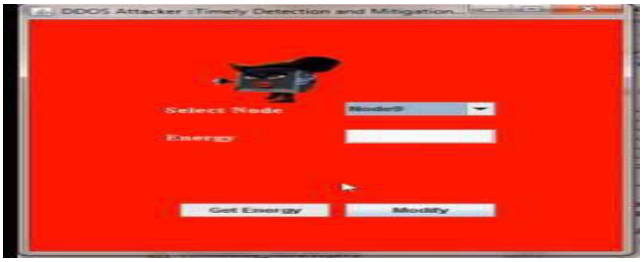


**Figure 9:** Applying The Ddos Attack

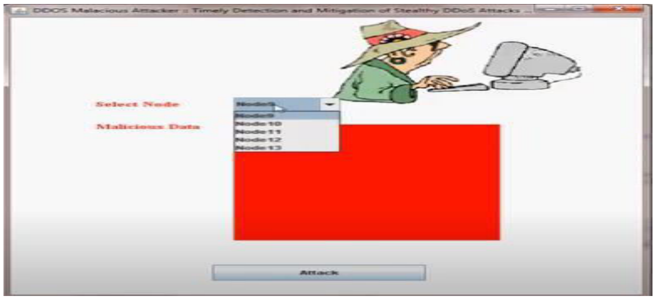
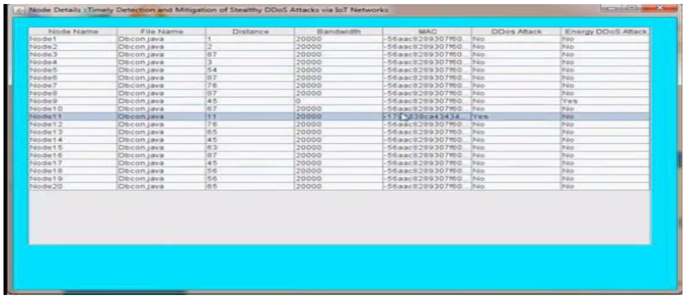

DDOS Malicious Attacker :: Timely Detection and Mitigation of Stealthy DDoS Attacks
Select Node
Malicious Data
Node9
Node9
Node10
Node11
Node12
Node13
Attack

**Figure 10:** Applying Ddos Malicious Attack



Node Details :Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

| Node Name | File Name | Distance | Bandwidth | MAC | DDos Attack | Energy DDoS Attack |
|---|---|---|---|---|---|---|
| Node1 | Dbcon.java | 1 | 20000 | -56aac8289307f60... | No | No |
| Node2 | Dbcon.java | 2 | 20000 | -56aac8289307f60... | No | No |
| Node3 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node4 | Dbcon.java | 3 | 20000 | -56aac8289307f60... | No | No |
| Node5 | Dbcon.java | 54 | 20000 | -56aac8289307f60... | No | No |
| Node6 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node7 | Dbcon.java | 76 | 20000 | -56aac8289307f60... | No | No |
| Node8 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node9 | Dbcon.java | 45 | 0 | -56aac8289307f60... | No | Yes |
| Node10 | Dbcon.java | 67 | 20000 | -56aac8289307f60... | No | No |
| Node11 | Dbcon.java | 11 | 20000 | -17[illegible]838ca43434... | Yes | No |
| Node12 | Dbcon.java | 76 | 20000 | -56aac8289307f60... | No | No |
| Node13 | Dbcon.java | 65 | 20000 | -56aac8289307f60... | No | No |
| Node14 | Dbcon.java | 45 | 20000 | -56aac8289307f60... | No | No |
| Node15 | Dbcon.java | 63 | 20000 | -56aac8289307f60... | No | No |
| Node16 | Dbcon.java | 87 | 20000 | -56aac8289307f60... | No | No |
| Node17 | Dbcon.java | 45 | 20000 | -56aac8289307f60... | No | No |
| Node18 | Dbcon.java | 56 | 20000 | -56aac8289307f60... | No | No |
| Node19 | Dbcon.java | 56 | 20000 | -56aac8289307f60... | No | No |
| Node20 | Dbcon.java | 65 | 20000 | -56aac8289307f60... | No | No |

**Figure 11**: Attack Information At Nodes

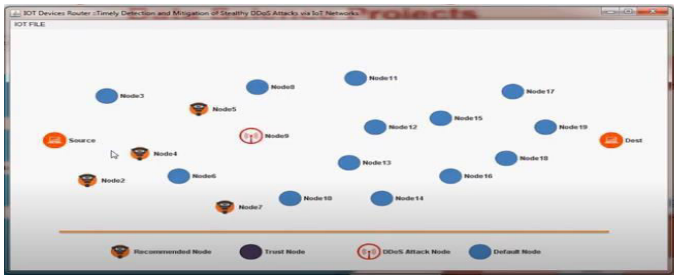


**Figure 12**: Attack Identified At Node 9

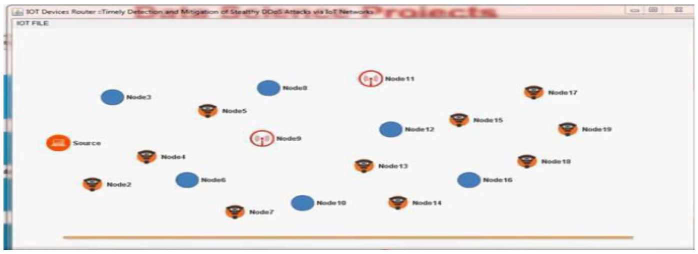
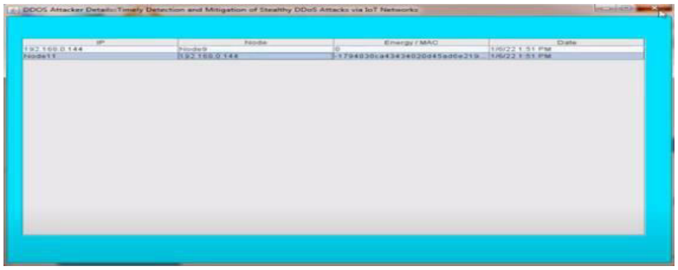


**Figure 12:** Attack identified at node 9 and node 11 and by pass the route and sends the data to the destination



DDOS Attacker Details::Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

| IP | Node | Energy / MAC | Date |
|---|---|---|---|
| 192.168.0.144 | Node9 | 0 | 1/6/22 1:51 PM |
| Node11 | 192.168.0.144 | -1794830ca43434e020d45ad6e219... | 1/6/22 1:51 PM |

**Figure 13:** Attacker Details

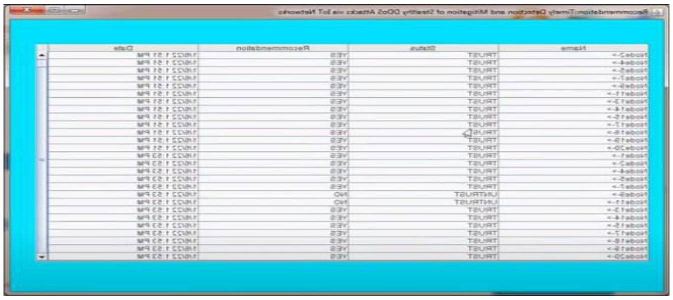


**Figure 14**: trust and non-trust nodes information

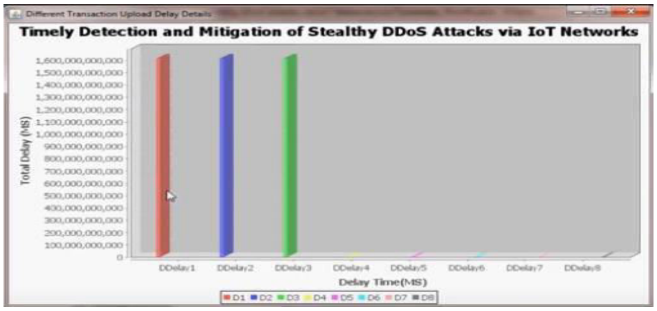


**Figure 15:** Time Delay Graphs

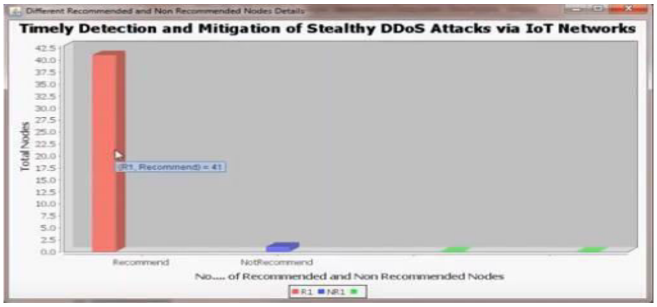


**Figure 16**: Recommendation Nodes

## 6 Conclusion

The demand for developing DDOS via IOT solutions is growing, especially in light of the recent stealthy DDOS attacks, given the prevalence of IOT devices and how simple it is for even novice malevolent parties to launch DOS attacks. We provided a broad and evolving threat model for hierarchical IOT networks in this setting. Then, using an online, scalable, nonparametric anomaly detection algorithm, we presented a novel intrusion detection and mitigation system. We assessed the effectiveness of the proposed detection and mitigation strategy in demanding covert DDOS attack scenarios using actual and simulated data as well as an IOT test bed. Applications of the suggested technique to expansive, dynamic networks with a range of device counts were also taken into consideration.

## 7 References

[1] Arsalan Mosenia and Niraj K Jha. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4):586–602, 2017.

[2] Imperva. Types of ddos attacks. https://www.imperva.com/learn/ application-security/ddos-attacks/.

[3] Nexusguard. Q3 2018 threat report: Distributed denial of service (ddos). https://www.nexusguard.com/hubfs/2019%20PTC/Nexusguard Q3%202018%20Threat%20Report.pdf, 2019.

[4] Elisa Bertino and Nayeem Islam. Botnets and internet of things security. Computer, (2):76–79, 2017.

[5] Yasin Yilmaz and Suleyman Uludag. Mitigating iot-based cyberattacks on the smart grid. In Machine Learning and Applications (ICMLA), 2017 16th IEEE International Conference on, pages 517–522. IEEE, 2017.

[6] Laurence Goasduff. Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020. https://www.gartner.com/en/newsroom/press-releases/ 2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io, 2019.

[7] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. Computer, 50(7):80–84, 2017.

[8] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In USENIX Security Symposium, pages 1092–1110, 2017.

[9] Mirai source code. https://github.com/jgamblin/Mirai-Source-Code.

[10] Alma D Lopez, Asha P Mohan, and Sukumaran Nair. Network traffic behavioral analytics for detection of ddos attacks. SMU Data Science Review, 2(1):14, 2019.

[11] Ahmad Riza'ain Yusof, Nur Izura Udzir, and Ali Selamat. Systematic literature review and taxonomy for ddos attack detection and prediction. International Journal of Digital Enterprise Technology, 1(3):292–315, 2019.

[12] Mark Shtern, Roni Sandel, Marin Litoiu, Chris Bachalo, and Vasileios Theodorou. Towards mitigation of low and slow application ddos attacks. In 2014 IEEE International Conference on Cloud Engineering, pages 604–609. IEEE, 2014.

[13] Enrico Cambiaso, Gianluca Papaleo, and Maurizio Aiello. Taxonomy of slow dos attacks to web applications. In International Conference on Security in Computer Networks and Distributed Systems, pages 195– 204. Springer, 2012.

[14] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits. Denial-of-service detection in 6lowpan based internet of things. In 2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob), pages 600–607. IEEE, 2013.

[15] Vipindev Adat and BB Gupta. A ddos attack mitigation framework for internet of things. In Communication and Signal Processing (ICCSP), 2017 International Conference on, pages 2036–2041. IEEE, 2017.

[16] Krushang Sonar and Hardik Upadhyay. An approach to secure internet of things against ddos. In Proceedings of International Conference on ICT for Sustainable Development, pages 367–376. Springer, 2016.

[17] Ping Du and Shunji Abe. Ip packet size entropy-based scheme for detection of dos/ddos attacks. IEICE transactions on information and systems, 91(5):1274–1281, 2008.

[18] Yang Xiang, Ke Li, and Wanlei Zhou. Low-rate ddos

attacks detection and traceback by using new information metrics. IEEE transactions on information forensics and security, 6(2):426–437, 2011.

[19] Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3):15, 2009.

[20] Rohan Doshi, Noah Apthorpe, and Nick Feamster. Machine learning ddos detection for consumer internet of things devices. arXiv preprint arXiv:1804.04159, 2018.