IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S08): 164-167, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0828
Available online at: https://www.ijmtst.com/vol8si08.html

Preventing DDos Attacks for IoT Based Networks using Odit

Dr. D J Samatha Naidu[1] | P.Vasundhara [2]

Principal, Annamacharya PG college of computer studies, Rajampet.
Annamacharya PG college of computer studies, Rajampet.

To Cite this Article
Dr. D J Samatha Naidu and P.Vasundhara. Preventing DDos Attacks for IoT Based Networks using Odit. International Journal for Modern Trends in Science and Technology 2022, 8(S08), pp. 164-167. https://doi.org/10.46501/IJMTST08S0828

Article Info
Received: 26 May 2022; Accepted: 24 June 2022; Published: 28 June 2022.

ABSTRACT

The emergence of things(iot) has been one of the most significant technological advances of the last decade.Internet of Things(IOT) networks consists of sensors,actuators,mobile and wearable devices that can connect to the Internet.With billions of such devices already in the market which have significant vulnerabilities,there is a dangerous threat to the Internet services and also some cyber-physical systems that are also connected to the Internet.With the proliferation of IOT devices, and the ease of triggering DoS attacks even by unsophisticated malicious parties,there is an increasing need for developing solutions to DDoS via IOT, especially the recent stealthy DDoS attacks.In this context,A general and emerging threat model for hierarchical IOT networks.The proposed novel intrusion detection and Mitigation frame work that employs an online,scalable and nonparametric anomaly detection algorithm.Through real and stimulated data,as well as an IOT tested to evaluate the performance of proposed detection and Mitigation scheme under challenging stealthy DDoS attack scenarios.Applications of the proposed scheme to large and dynamic networks with varying number of devices were also considered.

KEYWORDS: introduction, related work, proposed algorithm, modules and discription,screens

1. INTRODUCTION

This project investigates the denial of service problem, in the context of services provided over a network, and contributes to improved techniques for modelling, detecting, and preventing denial of service attacks against these services. While the majority of currently employed denial of service attacks aim to pre-emptively consume the network bandwidth of victims, a significant amount of research effort is already being directed at this problem. This research is instead concerned with addressing the inevitable migration of denial of service attacks up the protocol stack to the application layer. Of particular interest is the denial of service resistance of key establishment protocols Along with the base technologies of PIDs and dynamic path identifiers, the thesis highlights and discusses the importance of supporting technologies like integration, Big Data analytics and Develops that enhance the business value of convergence. the conclusion, summarizes the whole work and points out its benefits and deficits. It also discusses the next steps that could be taken to improve the outcome. It sets questions for further work in this topic. Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Botnets). Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community

2.EXISTING WORK

DDoS attacks via IoT networks are relatively less addressed compared to other security issues in the IoT enviornment. However, it is recently attracting considerable interest, e.g., [4], [7], [8]. In [10]–[13], a wide range of vulnerabilities because of which conventional signature-based detection techniques fail, are discussed. In [14], authors propose a solution to UDP flood attack in an IoT environment using 6LoWPAN and IEEE 802.15.4. However, it has high overheads and complex architectures and components which do not suit an IoT environment [15]. An agent-based DDoS mitigation approach is proposed in [16]. The authors propose a two-part algorithm in which the attack detection part has been performed in the border router. A similar entropy-based solution is proposed in [17], but with the requirement that the packet contents should be detectable. They also do not consider scenarios in which the entropy does not change but the number of packets do. Xiang et al. [18] proposes an information metric approach to quantify the differences between legitimate and attack network traffic by assuming that the legitimate traffic follows a Gaussian distribution, whereas the attack traffic follows a Poisson distribution. Machine learning algorithms are also gaining attention as recent anomaly detection research shows promise [19].

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.

1.3.2. PROPOSED WORK WITH ADVANTAGES

In the proposed system, the system proposes a practical anomaly-based detection and mitigation technique for IoT-based DDoS attacks, especially the challenging stealthy DDoS attacks with data rate increase per device as low as 10%, which is significantly lower than the considered rates in the literature, and can easily bypass most of the existing approaches. Specifically, the proposed technique is based on a statistical anomaly detection algorithm called Online Discrepancy Test (ODIT) that mitigates the attack with minimal interruption 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.

ADVANTAGES

A novel detection and mitigation technique for stealthy DDoS attacks is proposed, and its time and space complexity is analyzed;

Asymptotic optimality of the proposed detector is proven in the mini max sense as the training data size grows;Solution to a dynamic scenario in which the number of devices in the network changes is provided;

A comprehensive performance evaluation is provided using a test bed implementation, the N-BaIoT dataset, and simulations.

MODULES AND ITS DESCRIPTION

1. D-PID Design Modules

New D-PID of the path is still known only by the two domains. However, it is possible that a communication lasts longer than two update periods. Thus, when the PID of the path changes to PID3, ongoing communications may be interrupted. Based on this period, the content consumer then re-sends a GET message to the network in order to renew the PIDs along the path. Note also that in D-PID, all domains should dynamically change the PIDs of its inter-domain paths. Depending on its local policy, a domain may simultaneously (or asynchronously) change these PIDs. In the former case, the cost for updating the PIDs is fixed since a domain only needs to distribute the new PIDs to its border routers once every PID update period. In the latter case, every time the PID of an inter-domain path is updated, the domain needs to distribute the new PID to its border routers. However, the cost for updating PIDs in the latter case is significantly less than the update cost of IP-prefixes in the Internet today.

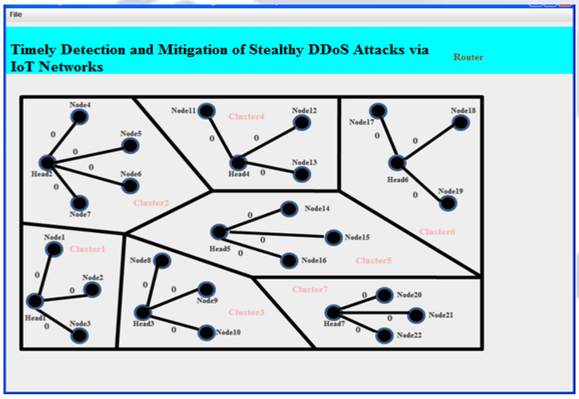
3.DISTRIBUTING PID TO ROUTERS MODULE

Having negotiated the new PID of a path connecting a neighboring domain, the RM in a domain A needs to distribute the new PID to the routers in that domain so that the new PID can be used to forward data packets. To achieve this, the RM simply sends a PID update message to every border router in the domain. The PID update message contains the path and its corresponding new PID. When a border router receives the PID update message, it updates its inter-domain routing table. After that, it sends an acknowledgement message to the RM. When the RM receives the acknowledgement messages from all border routers, it then updates its PID table. After that, the RM appends the new PID instead of the old one onto the GET messages when it forwards them. Accordingly, the corresponding data packets will be forwarded from the neighboring domain to domain A by using the new PID.

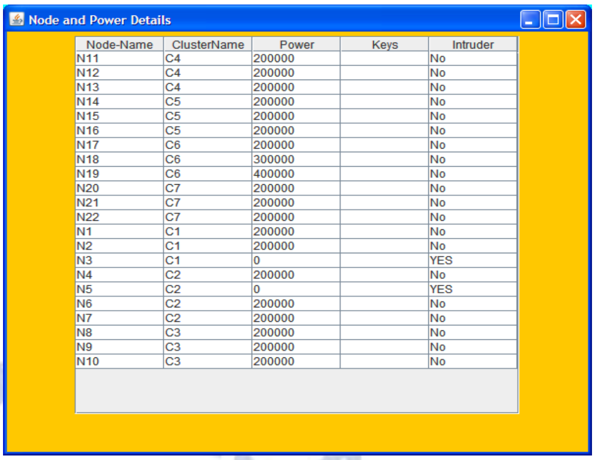
3.IDS MANAGER MODULE

In this module, the IDS Manager detects intruder and stores the attacker details. In a router any type of attacker (All Spoofers like source, destination, Flooding Attacks) is found then details will send to IDS manager. And IDS Manager will detect the attacker type (Source or destination,malicious data), and response will send to the router. And also inside the IDS Manager I can view the attacker details with their tags such as attacker type, attacked node name, time and date.

4. SIMULATION RESULTS:

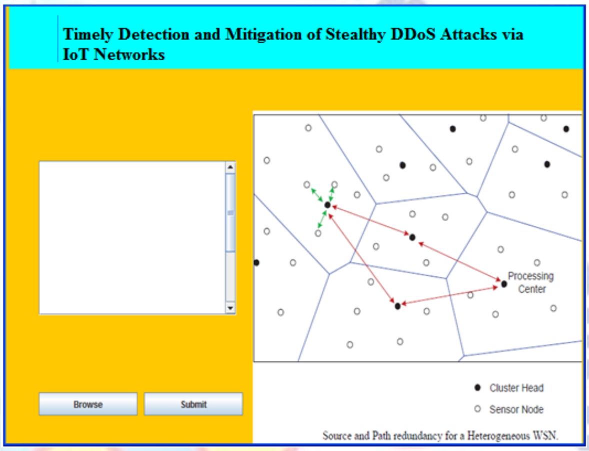


Screen 4.1. Router Window

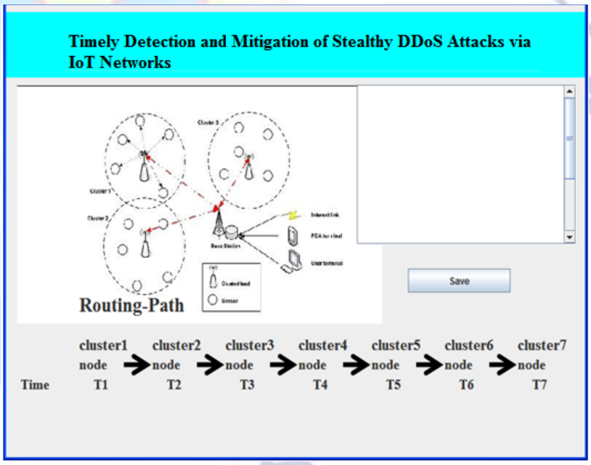


Node-Name	ClusterName	Power	Keys	Intruder
N11	C4	200000		No
N12	C4	200000		No
N13	C4	200000		No
N14	C5	200000		No
N15	C5	200000		No
N16	C5	200000		No
N17	C6	200000		No
N18	C6	300000		No
N19	C6	400000		No
N20	C7	200000		No
N21	C7	200000		No
N22	C7	200000		No
N1	C1	200000		No
N2	C1	200000		No
N3	C1	0		YES
N4	C2	200000		No
N5	C2	0		YES
N6	C2	200000		No
N7	C2	200000		No
N8	C3	200000		No
N9	C3	200000		No
N10	C3	200000		No

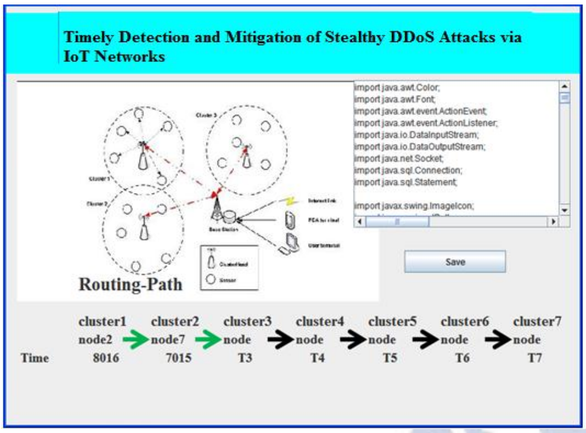
Screen 4.2. Window showing Node and Power Details


Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks
Processing Center
Browse
Submit
● Cluster Head
○ Sensor Node
Source and Path redundancy for a Heterogeneous WSN.

Screen 4.3. Source Provider Window



Screen 4.4. Destination Window



Timely Detection and Mitigation of Stealthy DDoS Attacks via IoT Networks

```
import java.awt.Color;
import java.awt.Font;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.net.Socket;
import java.sql.Connection;
import java.sql.Statement;

import javax.swing.ImageIcon;
```

```
        cluster1    cluster2    cluster3    cluster4    cluster5    cluster6    cluster7
        node2   →   node7   →   node    →   node    →   node    →   node    →   node
Time     8016        7015        T3          T4          T5          T6          T7
```

Screen 4.5. Destination Window Showing Received Fil

5. CONCLUSION

With the proliferation of IoT devices, and the ease of triggering DoS attacks even by unsophisticated malicious parties, there is an increasing need for developing solutions to DDoS via IoT, especially the recent stealthy DDoS attacks. In this context, we presented a general and emerging threat model for hierarchical IoT networks. We then introduced a novel intrusion detection and mitigation framework that employs an online, scalable and nonparametric anomaly detection algorithm. Through real and simulated data, as well as an IoT testbed we evaluated the performance of proposed detection and mitigation scheme under challenging stealthy DDoS attack scenarios. Applications of the proposed scheme to large and dynamic networks with varying number of devices were also consider.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

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] mperva. 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.