Distributed protection for distributed devices – an exploration into the published results, technological themes, and opportunities within the realm of protecting IoT devices from DDoS attacks.

Joseph Tsai
Department of Computer Science and Software Engineering
University of Washington
Bothell, USA
josephkt@uw.edu

***Abstract*—With the increasing use of Internet of Things (IoT) devices, security professionals and malicious actors have been at odds at securing, or exploiting, IoT devices. The challenges that surround IoT devices are numerous, as IoT devices are typically released to the public audience quickly and in large quantities, many times with little consideration for robust security controls. Distributed Denial of Service (DDoS) attacks on IoT devices have indicated a need for research and further development in the realm of protecting IoT devices. This paper surveys the current solutions available for securing IoT devices from DDoS attacks, defines qualitative metrics and performs a comparison analysis amongst the available solutions, identifies the common challenges these solutions face, as well as indicates future opportunities for researching security mechanisms that protect IoT devices from DDoS attacks. The results of the paper demonstrate that while there are a great variety of IoT protection mechanisms available, it seems that a combination of protection mechanisms would be best suited to properly address the DDoS attack security concerns surrounding IoT devices.**

Keywords—IoT, DDoS, Network Agents, Blockchain, DOTS, PKI, Policy Engines, Peer-to-Peer Networks

I. Introduction

Given the prevalence of increasing usage of Internet of Things (IoT) devices and corresponding security exploits of IoT devices [1], one can observe what seems to be a prevailing tension between the users of IoT devices, and the security professionals that seek to secure them. In what seems to be a dichotomy between innovation and security, malicious actors have found ways to attack vulnerable IoT devices, disrupting the use of such devices to render them useless or ineffective [2]. One such attack that has surfaced against IoT devices in recent years is the usage of Distributed Denial of Service (DDoS) attacks [3], which is performed through flooding a host with network traffic from a variety of sources until it is unable to provide its given service or communicate with legitimate users.

With the growing relevance of such attacks, this paper seeks to explore the existing solutions for protecting IoT devices from DDoS attacks, and present potential qualitative metrics for evaluating such solutions. In doing so, this paper can serve as a beneficial reference for those seeking to understand what solutions are currently available for protecting IoT devices from DDoS attacks, how to potentially compare currently available solutions, as well as better understand opportunities for future research in this field of study.

The structure of this paper is as follows: Section II summarizes and aggregates previous relevant work for potential protection mechanisms. Section III describes how the qualitative metrics were derived and used for comparison analysis of the different protection mechanisms. Section IV evaluates the results of the conducted comparison analysis. Section V concludes the paper.

II. Related Work

While protection from DDoS attacks has been explored and researched in depth, it is at the large number of devices and distributed nature of IoT devices that seems to present new challenges for researchers. With the new distributed topology of devices, several techniques have risen which leverage the distributed nature of IoT devices in order to protect them. Such techniques, when combined with existing DDoS protection mechanisms, culminates in the collective related previous works. These techniques and mechanisms have been aggregated from multiple sources and are summarized in Section II A.

A. Previous Related Work

1) Installation of agents to detect and alert on malicious network traffic [4] – [7]: Agents can be installed on network gateways to detect traffic to and from each IoT device. This solution allows the network traffic analysis to be distributed amongst the IoT network to perform detections and trigger alerts when abnormalities in network traffic are detected between the different agents.

2) Adding sensors which push network data to a central repository that indicates abnormalities [8] – [10]: Although not only specific to DDoS protection mechanisms, prior research has shown that the data collected by additional sensors on an IoT network can assist in detecting network traffic abnormalities. With such a solution, additional sensors push network traffic to a central location where network traffic is analyzed and generates alerts when there are abnormalities.

3) Usage of DDoS Open Threat Signaling (DOTS) [11]: A relatively recent advancement in the protection of IoT devices from DDoS attacks, DOTS architecture allows for specific DOT

packets to be sent between hosts on the network. These packets contain information regarding the previous node, and can ultimately be used to determine if a sensor is acting like an abnormality, when compared to the other DOT packets.

4) Establishment of Public Key Infrastructure (PKI) to confirm device communications on IoT device networks [12] – [15]: Although the implications of this protection mechanism also touch on data encryption and security aspects, this protection mechanism relates to DDoS attacks by verifying communications from a trusted source. Especially in networks where the IoT devices are only expected to communicate with a central control point, all other traffic attempting to connect to the IoT device can be dropped.

5) Policy engines for quarantining IoT devices with abnormal behavior [16], [17]: In certain scenarios, attackers may obtain control of IoT devices on a secured network. Hence, attackers can use the compromised devices to perform an internal DDoS attack on devices within the IoT device network. This protection mechanism relies on the usage of policy engines to detect abnormal network behavior of interactions on the network and quarantine such devices on the network.

6) Peer-to-peer networks with blockchain ledgers to verify device communications [13], [18], [19]: Although there are variations between different blockchain solutions, the core of this protection mechanism is to use a ledger that verifies the IP addresses allowed for communication with a given host. Hosts which cannot authenticate themselves are flagged and quarantined. As blockchain technology also emphasizes peer-to-peer communication, there are also capabilities for the devices to determine amongst themselves what is considered normal traffic on the network through seeing the recorded network traffic of its peers on the ledger.

7) Integrating overall best security practices on IoT devices themselves [18], [20]: This protection mechanism focuses on strengthening the IoT devices with simple denial of service options, such as whitelisting and blacklisting algorithms, to detect and block spam-like activity sent to IoT devices. The rationale for such a solution is that even with a minor improvement, many more IoT devices will be secured from larger scale attacks, such as DDoS attacks. With such protection, should a single IoT device be targeted, the additional securities provided establish a greater barrier of effort against attackers for the attack to be successful.

B. Building On Previous Works

With these current solutions in mind, this paper builds on previous related works through analyzing the current and cutting-edge solutions in qualitative regards. Rather than treating these solutions as completely separate, this paper presents a framework by which IoT device administrators could compare the different solutions available today. This is explored in greater detail within Section III.

III. Methodology

A. Establishment of Qualitative Metrics

To obtain the qualitative metrics by which the different IoT device DDoS protection mechanisms were compared, each solution was assessed for the challenges it presents in its implementation. This rationale was chosen on the basis that, at the challenges of implementation for any given protection mechanism, therein lies the potential weaknesses of the protection for the IoT devices. By comparing the challenges of different mechanisms, this paper is able to show how different mechanisms may possibly be combined to create an overall stronger defense for IoT devices from DDoS attacks.

The qualitative metrics which were extracted from the different DDoS protection methods are described and defined in Section III B. The performed comparison analysis is seen in Section III C.

B. Definition of Qualitative Measures, Derived From Presented Challenges

1) *Determination of baseline network traffic:* Detecting abnormalities in network traffic requires a baseline configuration for standard and expected network traffic. This is a fundamental challenge which is similarly faced by Intrusion Detection Systems (IDS's) as well. Questions which may arise in attempting to solve this challenge are: What is considered normal network traffic? What model should be used to determine abnormalities? How sensitive should the detection mechanisms be?

2) *Requiring modification of the original IoT devices or changing the functionality of the IoT devices:* Attempting to modify IoT devices can become resource intensive, depending on the number of IoT devices which must be monitored. This challenge is further complicated in the case that a given organization utilizes multiple types of IoT devices, from different manufacturers. Hence, solutions which resolve this challenge should account for a wide variety of IoT devices.

3) *Cost of storing of historical data:* To detect abnormalities, more storage space is required to look and analyze historical trends. Having a large or growing amount of managed IoT devices could add to the amount of network traffic to store for analysis purposes.

4) *Cost of network bandwidth to detect abnormal traffic:* Some protection mechanisms utilize additional network packets and agents to report on the state of the network. Such a mechanism can utilize additional network bandwidth, and at scale, cause greater costs on network bandwidth. Such network traffic would be generated in addition to the IoT network which is required for the devices to operate properly.

5) *User privacy concerns:* Rather than comparing to historical data, some solutions utilize network agents and centralized data analysis servers to compare user data to each other in order to see if abnormal activity is detected. It could be the case that some users do not want the details of their network traffic being analyzed in great depth.

6) Handling authentication of devices: Authenticating communications between devices and potential command points is key to preventing attackers from spoofing traffic on the network, or commands to the IoT devices. Strong authentication mechanisms can also provide an opportunity for devices to drop traffic which is not first authenticated.

7) Creation of additional computing costs: With a larger network of IoT devices, deployment of agents to monitor the network can incur additional computational costs, as the agents will need to operate, push data, and flag relevant findings on the network.

8) *Protecting a central aggregate:* Some of the mentioned protection mechanisms require the usage of a central aggregate, whether that be in the form of centralized computing of network traffic abnormalities, or centralized storage of PKI keys. Hence, attackers may divert DDoS traffic to such central aggregates instead of the IoT devices themselves.

9) Additional security protections needed for new infrastructure: Solutions which require adding more devices, sensors, agents, or any type of infrastructure to the established topology run the risk of creating additional points of attack for attackers. Essentially, adding such devices could increase the scope of the initial problem of protecting the IoT devices.

C. Comparison Analysis

Using the methodology described in Section III A and the derived qualitative measures explained in Section III C, Table I displays the outcome of the comparison analysis for each presented IoT device DDoS protection mechanism stated in Section II A. The results of the comparison analysis are articulated in Section IV.

TABLE I:
COMPARISON ANALYSIS OF IOT SECURITY SOLUTIONS AND CHALLENGES *

IoT Device DDoS Protection Challenges	**Solution**					
	Additional Network Agents	***Additional Sensors to Push Data to Data Processing Aggregate***	***DDoS Open Threat Signaling (DOTS)***	***PKI for Device Communications***	***Peer-to-Peer Networks with Blockchain Ledgers***	***DoS Protection Installed Directly on IoT Devices***
Need to determine network traffic baseline				**x**		
Not modifying the IoT device	**x**	**x**				
Cost of historical data for analysis				**x**		**x**
Need for additional bandwidth to detect abnormal traffic						**x**
Addressing user privacy concerns				**x**		**x**
Handling device authentication	**x**	**x**		**x**	**x**	
Reducing compute costs via less network agents				**x**	**x**	**x**
Creation of a central aggregate	**x**		**x**		**x**	**x**
Requirement to secure new infrastructure						**x**

* Note that Table I indicates which solutions can resolve, or do not face, the listed challenge

IV. RESULTS

A. Acknowledgement of Unexpected and Surprising Results

Based on the comparison analysis performed, the following points articulate unexpected and surprising results from the performed research:

1) While adding additional sensors and network agents seems to relieve some of the need to modify the IoT device itself, this seems to occur at additional cost. Such solutions seem to be more robust in being able to compensate for cases where attackers try to attack the whole network of IoT devices, as provided through the additional network traffic analysis and monitoring capabilities.

2) PKI, peer to peer, and IoT device implemented DoS protections seem to be most cost-effective for the user or organization that purchases the devices. It could be in such scenarios that this puts the ownership on the manufacturer to make secure devices, which could increase the cost of the devices. It should also be considered that these solutions are also only strong if a user would only want to have the devices

communicate with each other, but not let external users communicate with them. Such solutions are strong in verification of appropriate traffic between or to other devices on the network.

3) While PKI and integration of DoS at the IoT device level seem to have performed well in the comparison analysis when compared to the other solutions, the resource cost of adjusting the IoT devices to be able to perform such mechanisms, especially at a large scale of IoT devices from different manufacturers, should be considered.

B. Interpretation of the Quality of the Results

The quality of the results discovered by this paper were determined in direct correlation to the comparison analysis performed. For the purposes of this paper, the goal of the comparison analysis was to discover where certain IoT device DDoS protection mechanisms can be combined for greater results. Such a result was indeed achieved.

C. Measurement of the Paper's Success and Evaluation of Goals

Success for this research was measured through the identification of common themes amongst current and past literature for protecting IoT devices from DDoS attacks, establishing criteria for comparing the different solutions, and presenting a summary of the findings from the performed comparison analysis. Each of the aforementioned points have been explained and presented in detail in Section II A, Section III B, and Section III C, respectively.

V. Conclusion

A. Key Results and Takeaways

As seen by the performed research, IoT device protection from DDoS attacks spans a wide spectrum of potential solutions. Some solutions focus on altering the IoT devices themselves, while other solutions focused on adding components to network topologies in order to analyze network traffic. Depending on the solution, different challenges are faced, and the benefits must be weighed when determining a viable solution for a given organization.

B. Implication of the Results

This research displays that IoT devices require different solutions depending on their context. It is clear that there is not a single solution which every organization should gravitate towards, since no single solution can meet all the presented challenges. Such an implication seems to indicate that what is needed is a combination, or hybrid approach, toward protecting IoT devices from DDoS attacks.

C. Limitations

As with any cutting-edge field, new literature is continually produced. With such a limitation in mind, this paper acknowledges that the scope of the provided analysis addresses only in part the vast number of solutions available for DDoS protections for IoT devices.

Further reflection on the conducted research indicates that there could be solutions at the manufacturer level which were not considered as part of this research. That is, IoT devices should not only be secured once they have been purchased. However, such situations were not explored in-depth and were considered out of scope for this research project.

D. Areas of Future Work, and Proposed Next Steps

Potential areas for future work include:

- Exploring what solutions have been implemented to build in security into the IoT development lifecycle.
- Understanding how the cost of storage or computation can be made efficient amongst the different proposed solutions.
- Articulating how detection of abnormalities of network traffic may be different for IoT devices when compared to other devices with connect to an organization's network.
- Categorizing IoT devices in order to understand if there are optimum protection mechanisms for different types of IoT devices.
- Adjusting the provided comparison analysis to be score-based, thus taking into account the different effectiveness of the IoT DDoS protection mechanisms instead of treating them all as of equal weight.

This paper's goal was to provide a reference for those who may be intrigued by the possibility of what can be protected, especially in a distributed topology. With new technologies come new security solutions. In such a cutting-edge field, what is needed are cutting-edge solutions, many of which, have yet to be explored.

References

[1] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-capable IoT malwares: Comparative analysis and Mirai investigation," Security and Communication Networks, vol. 2018, 2018.

[2] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Feb. 2017, pp. 32–37, doi: 10.1109/I-SMAC.2017.8058363.

[3] M. D. Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "Analysis of DDoS-capable IoT malwares," in 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Sep. 2017, pp. 807–816, doi: 10.15439/2017F288.

[4] F. Leu and C. Pai, "Detecting DoS and DDoS Attacks Using Chi-Square," in 2009 Fifth International Conference on Information Assurance and Security, Aug. 2009, vol. 2, pp. 255–258, doi: 10.1109/IAS.2009.292.

[5] N. Giachoudis, G. Damiris, G. Theodoridis, and G. Spathoulas, "Collaborative Agent-based Detection of DDoS IoT Botnets," in 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), May 2019, pp. 205–211, doi: 10.1109/DCOSS.2019.00055.

[6] S. Armoogum and N. Mohamudally, "Efficiency of using mobile agents to trace multiple sources of attack," in 2009 First International

Conference on Networked Digital Technologies, Jul. 2009, pp. 464–468, doi: 10.1109/NDT.2009.5272204.

[7] I. Kotenko and A. Ulanov, "The Software Environment for Multi-agent Simulation of Defense Mechanisms against DDoS Attacks," in International Conference on Computational Intelligence for Modelling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC'06), Nov. 2005, vol. 1, pp. 283–289, doi: 10.1109/CIMCA.2005.1631280.

[8] S. Naik and V. Maral, "Cyber security — IoT," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), May 2017, pp. 764–767, doi: 10.1109/RTEICT.2017.8256700.

[9] S. K. Y.R and H. N. Champa, "IoT Streaming Data Outlier Detection and Sensor Data Aggregation," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Oct. 2020, pp. 150–155, doi: 10.1109/I-SMAC49090.2020.9243509.

[10] T. Munasinghe, E. W. Patton, and O. Seneviratne, "IoT Application Development Using MIT App Inventor to Collect and Analyze Sensor Data," in 2019 IEEE International Conference on Big Data (Big Data), Dec. 2019, pp. 6157–6159, doi: 10.1109/BigData47090.2019.9006203.

[11] S. Badruddoja, R. Dantu, L. Widick, Z. Zaccagni, and K. Upadhyay, "Integrating DOTS With Blockchain Can Secure Massive IoT Sensors," in 2020 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), 2020, pp. 937–946, doi: 10.1109/IPDPSW50202.2020.00156.

[12] S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," in 2017 International Conference on Inventive Systems and Control (ICISC), Jan. 2017, pp. 1–5, doi: 10.1109/ICISC.2017.8068718.

[13] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," in 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), Oct. 2018, pp. 9–15, doi: 10.1109/CIC.2018.00-45.

[14] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "Ethereum for Secure Authentication of IoT using Pre-Shared Keys (PSKs)," in 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM), Oct. 2019, pp. 1–7, doi: 10.1109/WINCOM47513.2019.8942487.

[15] B. Oniga, S. H. Farr, A. Munteanu, and V. Dadarlat, "IoT Infrastructure Secured by TLS Level Authentication and PKI Identity System," in 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), Oct. 2018, pp. 78–83, doi: 10.1109/WorldS4.2018.8611563.

[16] S. M. Sajjad and M. Yousaf, "UCAM: Usage, Communication and Access Monitoring Based Detection System for IoT Botnets," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Aug. 2018, pp. 1547–1550, doi: 10.1109/TrustCom/BigDataSE.2018.00221.

[17] B. K. Bal, W. L. Shi, S. S. Huang, and O. Gnawali, "Towards a Content-based Defense against Text DDoS in 9–1-1 Emergency Systems," in 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Oct. 2018, pp. 1–6, doi: 10.1109/THS.2018.8574125.

[18] M. H. Rohit, S. M. Fahim, and A. H. A. Khan, "Mitigating and Detecting DDoS attack on IoT Environment," in 2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON), Nov. 2019, pp. 5–8, doi: 10.1109/RAAICON48939.2019.5.

[19] N. Giri, R. Jaisinghani, R. Kriplani, T. Ramrakhyani, and V. Bhatia, "Distributed Denial Of Service(DDoS) Mitigation in Software Defined Network using Blockchain," in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dec. 2019, pp. 673–678, doi: 10.1109/I-SMAC47947.2019.9032690.

[20] N. Vlajic, D. Zhou, and J. Tung, "IoT Cameras and DVRs as DDoS Reflectors: Pros and Cons from Hacker's Perspective," in 2018 IEEE International Conference on Industrial Internet (ICII), 2018, pp. 181–187, doi: 10.1109/ICII.2018.00035.