A Novel lightweight DDOS Attack Detection Algorithm for Internet of Medical Things (IoMT)

Somasundaram R[1†] and Mythili Thirugnanam[2††]

SCOPE, Vellore Institute of Technology, Vellore, 632014 India

Summary
Internet of Things (IoT) and its applications are getting very popular nowadays. Internet of Medical Things (IoMT) is a major application under IoT that stores and transmits sensitive data over the network. The increasing number of security attacks such as DDoS attacks and Sybil attack is the major concern while using IoMT devices in the healthcare organization. In this paper, a novel lightweight DDoS attack prevention algorithm using device-level packet filtering is proposed and implemented in Contiki OS and Cooja simulator. Results obtained from the simulations show that the proposed filtering algorithm delivers less genuine packet drop ratio and less DDoS attack packet delivery ratio comparatively with the other existing algorithms in the IoMT environment.

Key words:
DDoS attack, Internet of Things (IoT,) Internet of Medical Things (IoMT), Lightweight security.

1. Introduction

Internet of Medical Things (IoMTs) is one of the major application under the Internet of Things (IoT) which gives various emerging services to the healthcare industry. IoMTs are sensor-enabled embedded electronic devices that are connected with internet. The important services in IoMT such as remote patient monitoring, analysing personalized health data, and monitoring patient drug consumption is reducing the delay in the treatment and also improve the accuracy in healthcare. Security issues such as unauthorized device access, DDoS attack, and device hijacking are the major security concern when all the devices transmitting sensitive data over the internet. In particular, DDoS attack is the critical security attack to identify which deliberately targeted on IoMTs by attackers. The purpose of such attacks is to create damage in the patient's life, to beat in the business completion, or to financial loss to particular healthcare organization. DDoS is a type of network attack featuring disrupting service for legitimate requests, which is often done by flooding the targeted host server with bad requests to temporarily reduce legitimate users' bandwidth [1]. During the year 2016, a massive DDoS attack was identified in Europe based webhosting company called OVH. In that, several IoT devices are attacked by DDoS including routers, IP cameras, webcams, and routers.

Manuscript received November 5, 2019
Manuscript revised November 20, 2019

One of the huge threats for IoT device is the Mirai malware. Which scans the default device passwords and send that into botes to conduct a DoS attack in the IoMT network. In the year 2016, this method was used to target an Oracle DYN which recorded one of the massive DDoS attack all time. In this attack, attackers used more 4000,000 Mirai botnets which are basically an IoT device. a This attack slow downed the functioning of Twitter, Reddit, Airbnb, PayPal, and Netflix for more than five hours [2][3]. In order to safeguard patient life, identifying and preventing DDoS attack is very essential. Therefore, a strong lightweight security mechanism is needed to be introduced to ensure the data security of IoMTs.

2. Related works

Several researchers worked in the area of detecting DDoS attack in the IoT environment. Many attack defence strategies were proposed, implemented, and tested to be effective against DDoS attack over the Internet. Yin D et al. (2018) [5] proposed a DDoS attack detection algorithm called the Software Defined IoT framework. Which uses threshold value to identify the DDoS attacks and mitigating the attack by blocking the attacker. The proposed algorithm is following a reactive security strategy. But a proactive security mitigation technique is required for IoMT devices since it transfers more sensitive data. In order to reduce the computation power, da Silva Cardoso et al. (2018) [7] proposed a DDoS attack detection system. The experimental results of the proposed system show that the presented Complex Event Processing (CEP) mechanism helps to process huge data and intrusion detection in IoT network. Kajwadkar, S et al. (2018)[11] proposed DDoS detection algorithm for IoT network. Which differentiate the attacking packet and genuine packet into the network by checking the payload size. But, identifying attacker's packet is difficult when receiving same size payloads. In order to identify the abnormal traffic in the IoT network Gurulakshmi, K et a. (2018) [8] used Support Vector Machine Algorithm (SVM). Which classifies DDoS attack packet traffic into the network.
Zheng, J et al. (2018) [9] introduced a Markov Decision Process (MDP) based DDoS attack prevention system. The

proposed work is a manual data monitoring process. Therefore, the implementation of MDP in non SDN based IoT environment is difficult.

Sambandam, N et al. (2018) [10] implemented an early DDoS detection algorithm by measuring the entropy in the SDN based IoT environment. The experimental results shows that the presented Complex Event Processing (CEP) mechanism helps to process huge data and intrusion detection in IoT network. In order to defend a wide range of DDoS attack on IoT devices, Adat, V et al. (2017) [6] developed a risk transfer security mechanism. Kolias et al. (2017) [4] explained increasing mirai botnet attack in connected devices and how it causes DDoS attack. It is reported that 213,000 to 493,000, variants of Mirai attacks are targeting IoT devices. The study emphasises the importance of identifying and mitigating the Mirai botnet attacks. A general strategy to mitigate these attacks are usage of firewall. Which can filter the incoming packets by verifying the IP address of the sender Somasundaram, R et al [12].

Based on the review on DDoS attack prevention techniques, various research gaps have been identified such as mitigating the Mirai attacks, computational delay in implementing attack prevention algorithms, and some of the works limited to SDN based IoT environments. Conventional DDoS preventive measures and defenses highly rely on power supply, computing resources, and long-time processing. Considering the characteristics of IoT environment, all such preconditions should be avoided in the design of IoT defense system. One needs to keep it in mind that IoT hardware components are highly heterogeneous and very limited in power supply and computing capability when comparing to traditional nodes over the internet such as personal computers, smartphone, and tablets. Also, maintaining real-time communication in IoT network is fairly important, long time processing will cause delay and target miss during the task of identifying malicious traffic. Therefore, there is a need to implement a lightweight DDoS detection algorithm.

3. Proposed Lightweight DDoS Detection Algorithm

There are various DDoS detection strategies are followed in the traditional network security. Some of the general attack detection strategies are discussed in this section. In general, a DDoS causing attack request data in the IoMT network is created from one attacking device to other malicious bot devices. Then all the bot devices will target particular device by sending high frequency of request with similar payloads. One of the easy ways to identify the attacking packets is to filter the packets from identified spoofed IP addresses and dropping them.

Table 1: Various DDoS attack detection strategies

DDoS attack detection strategies	Description
Firewall	A firewall DDoS detection strategy is used to filter the incoming attacker's packet using IP address.
Congestion control	Using congestion control DDoS attacker's packets flow is restricted by increasing the resource production in the host server. But. This method will affect legitimate packet delivery.
Reconstruction attacking route	Using route mapping function, DDoS attacking packet routes are reconstructed. This will limit the flood of UDP packets going into the IoMT network. But This strategy requires huge amount of storage capacity and computation resources.
Deep Packet Inspection (DPI)	DPI is the conventional DDoS attack detection strategies. This method works by inspecting the packet's route, server, and IP. But this time consuming and resource-demanding method is not feasible to work with lightweight IoMT network.

As mentioned in Table 1, a heavy DDoS attack detection and prevention strategy is not suitable for energy-constrained IoMT environment. To design lightweight attack detection system, less energy-consuming with less genuine packet drop ratio and high packet drop ratio technique is required. Keeping all this in mind, to identify and prevent the DDoS attack in the IoMT environment, a new lightweight filtering algorithm is proposed in the device level (Border router) Packet Filtering Embedded Firewall (PFDL) Somasundaram, R et al [12].

4. PFDL Embedded firewall

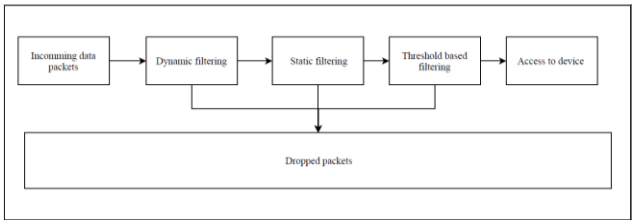

Fig. 1 Various levels of PFDL Embedded firewall

The overall process of the PFDL has shown in Figure 1. It has three level filters to inspect incoming packets into the network namely dynamic filtering, static filtering, and threshold-based filtering. Dynamic filtering is general firewall mechanism that filters packets based on the predefined ruleset. The static and threshold-based filtering are discussed in the following sections.

4.1 Algorithm for static filtering

```
Input: Incoming Packet(P_i):[SrcIP,DestIP,Data]
begin
    Read: (P_i Header)
    if SrcIP ∈ BlackIP(Rec) then
        Drop Packet;
    else
        if DataSize > DataThreshold then
            Drop Packet
            Add the IP to BlackIPList;
        end
        else if Src IP ∈ GrayIPList then
            filter the packet as suspected and forward it to Threshold based
            filter;
        Start Time Period Ti = 0
        Data Ti = DataSize
        while Ti < Tp do
            for Incoming Packet Pj do
                Data Ti = Data Ti + DataSize(Pj)
                if Data Ti >= DataThreshold then
                    Forward packets P_i to P_j to the Threshold based filter
            end
            Proceed;
        end
    end
end
```

Fig. 2 Static filtering algorithm

Static filtering is the second level packet filtering in the 6LoWPAN PFDL (Border Router). All the incoming data traffic from the external world to IoMT network will be passed through the PFDL Static filtering. In this filtering process, all the data packets (Pi) are filtered based on the source IP index which has already listed in the firewall ruleset as shown in Figure 2.

While verifying the SrcIP, if the incoming packet is presented in the Backlisted IP then it will be dropped into honeypot. Otherwise, it will be verified for the packet size constraint. If the DataSize is greater than the DataThereshold that is 120 bytes per second then the packet will be dropped into honeypot. Finally, the packet will be verified frog GreyList IP verification and forwarded to threshold-based filtering.

4.2 Algorithm 2: Threshold based filtering

```
Input: A set of packets P_i; i = 1 to n or a suspected packet P_j
begin
    if SourceIP of all the incoming packets is same then
        if Data packets are same then
            Drop Packet;
            Denial of Service attack detected;
            Add the SrcIP to BlackIPlist;
        else
            Proceed;
        end
    else
        if The incoming Data packets are same then
            Drop packets;
            Distributed Denial of Service attack detected;
            Add the SrcIP to GrayIPList;
        else
            Proceed;
        end
    end
    if packet P_j marked as suspected is coming then
        if PLoad(Data) is same as the malicious packet then
            Drop Packet;
            Add the SrcIP to the BlackIPList;
        else
            Proceed;
        end
    end
end
```

Fig. 3 Threshold-based filtering algorithm

In the threshold-based filtering, all the incoming packets are verifying for the DataSize in a particular interval of time. If the same DataSize packets are coming from the same IP for a particular period of time, then it is considered that the suspected SrcIP sending packets with intention of DoS attack also the IP will be added into the Blacklist as shown in the Figure 3.

Also, the same behavior of data is sent from different SrcIP with particular interval of time, then it is suspected that the multiple sources are targeting a single targeted medical device with the intention of DDoS attack, finally the SrcIP from various sources are blocked and send to the honeypot.

5. Simulation and Experiment Results

The proposed algorithms are implemented and tested in the Contiki operating system and Cooja simulator. Contiki is a real-time operating system widely used for lightweight processing. In order to test the proposed static and dynamic filtering in border router, we have used 100 Tmote sky motes and one border router. In this, 80 motes are legitimate and another 20 motes are attack motes. Both the algorithms are implemented in the Border Router (BR). After the 60 minutes of the execution in the Cooja simulator, the results are obtained and analysed.

Table 2: Device properties of DDoS attack simulation

Devices	Description
Attacking device	Attacking devices which intended to perform DDoS attack are designed to transmit the same request for particular amount time with higher frequency to the targeted device.
Border router	Border Router (BR) connects the nodes into the external network (internet). PFDL algorithm implemented in the BR will verify the incoming data packets into the IoMT network.
Genuine device	Genuine devices will transmit legitimate request to other nodes. These devices usually transmitted from known IP devices with less frequency

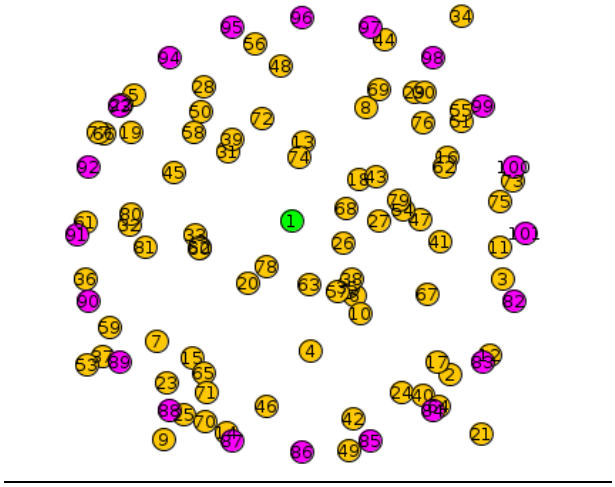

Fig. 4 Device positions of Border Router (BR), Attacker Devices, and Genuine devices

The three-level Packet Filtering Device Level (PFDL) embedded firewall is implemented in the Contiki operating system Cooja simulator. As shown in Figure 4 simulated sky motes are deployed in a random elliptic position. The Pink colour nodes are attack nodes deployed in an elliptic position. These nodes will act as bots and send continuously requested to the targeted legitimate devices. The yellow colour nodes are legitimate devices that transmit sensitive heartbeat data from one device to another as well as to the border router. Finally, the green one is a Border Router which acts as a gateway to IoMT network to the internet. In this, all the external packets are filtered with the implemented PFDL filtering algorithms.

The results are analysed based on the packet drop and packet delivery ratio of the static and dynamic filtering process. In this a less packet drop in genuine incoming packets is considered to be better performance. And low attack packet delivery ratios are considered to be the better performance filter.

5.1 Packet Drop Count

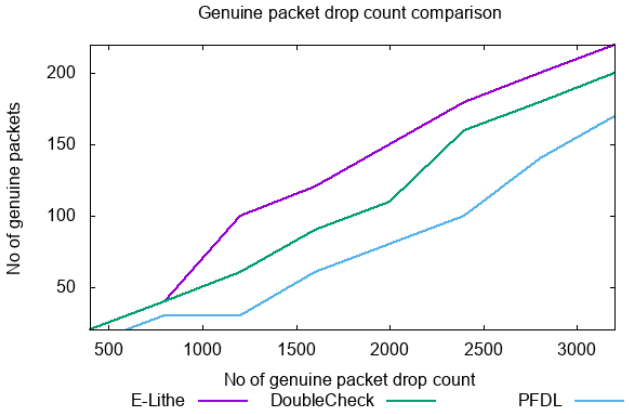

Fig. 5 Genuine packet drop ratio comparison

In order to identify the genuine packets that are not dropped in the PFDL, genuine packet drop count is calculated and compared with other existing DDoS detection algorithms is shown in Figure 5. The results shows that the proposed three-level PFDL filtering algorithms drop less amount of genuine compare to the existing E-Lithe algorithm introduced and by Haroon, A et al. [13] and DoubleCheck proposed by Kajwadkar, S et al. [11].

5.2 Ddos Attack Packet Delivery Count Comparison

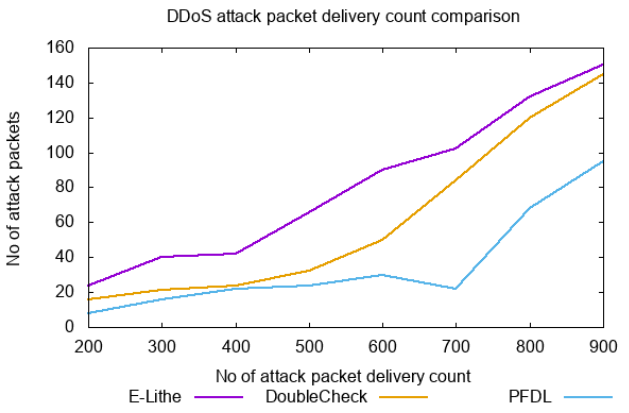

Fig. 6 DDoS Attack Packet Delivery Ratio Comparison

To identify the DDoS attack packets delivery count, all three algorithms' attack packet delivery ratio is calculated and compared. In Figure 6, the results shows that the proposed three level PFDL filtering algorithms delivers less amount of attack packets into the IoMT environment compare to the existing E-Lithe algorithm introduced and

by Haroon, A et al. [13] and Doublecheck proposed by Kajwadkar, S et al. [11]

6. Conclusion and Future work

The proposed lightweight DDoS attack detection packet filtering algorithms, efficiently identify and prevents the incoming DDoS attack prone packets in the device level IoMT environment. The simulated results shows that the static and threshold-based filters performing better in terms of low malicious packet delivery ratio and less legitimate packet drop ratio. In the future, a machine learning-based malicious packet analysis will be included on the dropped packets to reduce the legitimate packet drop ratio as lower as possible.

Reference

[1] F. Lau, S.H. Rubin, M.H. Smith and L. Trajkovic. “Distributed Denial of Service Attacks.,” In 2000 IEEE International Conference on Systems, Man, and Cybernetics, 3:2275–80 vol.3, 2000.

[2] "IoT and DDoS: Cyberattacks on the Rise | A10 Networks", A10 Networks, 2019. [Online]. Available: https://www.a10networks.com/blog/iot-and-ddos-cyberattacks-rise/. [Accessed: 26- Oct- 2019].

[3] F. Team, "IoT DoS Attacks | Hacked IoT Devices Can Lead To Massive DoS Attacks", Finjan Blog, 2019. [Online]. Available: https://blog.finjan.com/iot-dos-attacks/. [Accessed: 26- Oct- 2019].

[4] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets", Computer, vol. 50, no. 7, pp. 80-84, 2017.

[5] D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework", IEEE Access, vol. 6, pp. 24694-24705, 2018.

[6] V. Adat, B.B. Gupta and S. Yamaguchi, “Risk transfer mechanism to defend DDoS attacks in IoT scenario,” In 2017 IEEE International Symposium on Consumer Electronics (ISCE), pp. 37-40, 2017.

[7] A.M. da Silva Cardoso, R.F. Lopes, A.S. Teles and F.B.V. Magalhães, “Real-time DDoS detection based on complex event processing for IoT,” In 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 273-274, 2018.

[8] K. Gurulakshmi and A. Nesarani, “Analysis of IoT Bots against DDOS attack using Machine learning algorithm,” In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1052-1057, 2018.

[9] J. Zheng and A.S. Namin, “December. Defending SDN-based IoT Networks Against DDoS Attacks Using Markov Decision Process,” In 2018 IEEE International Conference on Big Data (Big Data), pp. 4589-4592, 2018.

[10] N. Sambandam, M. Hussein, N. Siddiqi and C.H. Lung, C.H., “Network Security for IoT Using SDN: Timely DDoS Detection. In 2018 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-2, 2018.

[11] S. Kajwadkar and V.K. Jain, "A Novel Algorithm for DoS and DDoS attack detection in Internet of Things", in Conference on Information and Communication Technology (CICT), pp. 1-4, 2018.

[12] R. Somasundaram and M. Thirugnanam, "Preventing Unauthorized Access to Internet-of-Things Medical Devices Using Packet Filtering Device Level Embedded Firewall", Journal of Computational and Theoretical Nanoscience, vol. 15, no. 6, pp. 2174-2178, 2018.

[13] Haroon. S. Akram. M.A Shah. and A. Wahid. “E-lithe: A lightweight secure dtls for iot,” in conference IEEE 86th Vehicular Technology Conference (VTC-Fall), pp. 1-5, 2017.

Somasundaram R received the B.Tech and M.E. degrees, from Anna University. In 2010 and 2012, respectively. He has worked as a Assistant Professor in the department of Computer Science and Engineering at Arulmigu Meenakshi Amman College of Engineering, Anna University Chennai. He has teaching experience of around Six years. His research interest includes Internet of Things, Network Security, Blockchain and Cyber forensics.

Mythili Thirugnanam received Master’s in Software Engineering from VIT University and awarded doctorate in Computer Science and Engineering at VIT University in 2014. She has been working as a Associate Professor in the School of Computer Science and Engineering at VIT University, Vellore, India. She has teaching experience of around 12 years. She has a research experience of 3 years in handling sponsored projects funded by Govt. of India. Her area of specialization includes Image Processing, Software Engineering and Knowledge Engineering. She has published more than 30 papers in international journals and presented around seven papers in various national and international conferences.