Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130517

Mitigation of Distributed Denial of Service Attacks on the Internet of Things

R. Radhika and K. Kulothungan*

Department of Information Science and Technology, College of Engineering Guindy, Anna University, Chennai, Tamilnadu, 600025, India.

Received: 2 Mar 2019, Revised: 10 May 2019, Accepted: 15 May 2019
Published online: 1 Sep 2019

Abstract: The tremendous growth of the pervasive network and its utilization, in the Internet of Things (IoT), is purposefully explored around the world. The Internet of things has an enormous attraction for contender, and is effortlessly attacked due to destitute resource and imperfect distribution of things. The distributed denial of service attacks are fetching an increasingly, continual hassle into the network. Security possess significant insistence in the Internet of Things (IoT). In this paper, an algorithm for malicious user identification named as Flooding Distributed Denial of Service Attack Detection and Prevention Mechanism (FADM) is coined to protect the network, from ruining. The entropy-based approach for detection and bloom filter for prevention is used. A user is classified as malicious when its entropy value is low compared to threshold. The simulation outcome makes evident that the algorithm identifies the malicious user accompanied by elevated detection ratio, reduced false alarm ratio, and exceptional scalability.

Keywords: Internet of Things, Distributed Denial of Service, Flooding DDoS Attack Detection and prevention Mechanism (FADM).

1 Introduction

Internet of things (IoT) is a digital environment, which interconnects the devices. Infrastructure around the environment is having the impact of socio-economy. The device to device communication, needs cooperation and it requires the ALERT of data security. As the number of connected devices expands the issues of security has been mottled. The effects to overcome this is tremendously increased. [1] since the sensitive data present in the IoT device are more vulnerable to simple attacks, this leads to compromised devices in a huge number. The reason behind these is the diverse nature of IoT networks. The new device auto-configure will implicitly leading to security prone. While manufacturing IoT devices, the standardization are not considered as a vital role, by the manufacturer and hence they are in hurry to release their products [3]. Hence they have to consider the impact of data breach and take actions. There are many breaches that are responsible for IoT security like storage, computation, and power. The traditional system differs from IoT device vulnerabilities [4] supporting the cross device communication and dynamic environment which focus on perimeter defense and manual patching. The IP address spoofing [5]is the common strategy to carry random IP source address and act as a reflector host which triggers and mitigate as the source. The challenges faced by the IoT user make them feel that their information is leaked due to storage format, processing methods and data filtering methods. It also credits difficulty in providing privacy, trust, and confidentiality. Among these vulnerabilities Distributed Denial of Service (DDoS) is one. The Distributed Denial of Service (DDoS) acts as a powerful threat since it attacks distributed computers and blocks the server or the communication channel by flooding. By projecting this problem, a meritorious solution called FADM is proposed in this paper to defend against them. Remaining of this paper is arranged as follows. Section II, shows the related works. In Section III, the proposed work is explained with Section IV, the detection and prevention techniques of DDoS attack variants and all are discussed in IV. DDoS attack detection mechanism in V Filtering Mechanism for protection is expalined and the result analysis of DDoS variants are shown in Section VI, ultimately, Section VII. concludes the paper.

* Corresponding author e-mail: rradhikaphd@auist.net

2 Related works

The DDoS attack on IoT network at different layers [2] are detailed as Perception layer, faces desynchronizing attack and bootstrapping attack. Network layer deals with reflection , protocol amplification, flooding attacks and application layer has reprogramming attack and path Dos.

There are different attacks that exist in connected things like voluminous attack, application attacks, and protocol attack. The voluminous attack represents the flooding attack which involves communication with enormous traffic by so it freezes the bandwidth. The network time protocol, domain name server, and user datagram protocol, flooding and transmission control protocol prevent these attacks. The applications layers are exploited by manipulating request over the web server [6]. The ping of death helps to inject the vulnerabilities in the network layer and is focused by the protocol attacks, which exhaust the processing efficiency in this layer for the targeted service.

In [7] the joint entropy security scheme is used to detect DDoS, on statistical calculation this entropy reduces the system burden compared to machine learning algorithms. The attack on the Domain Name Services (DNS) services is flooded by the Hypertext transfer protocol. The bandwidth depletion cause flooding storm and resource exhaustion cause protocol attacks. These two methods support application attacks, by analyzing all these attacks. The DDoS attack are classified and explained with cooperative relationship to handle malwares in bot [3]. The botnet devices [8] are responsible for an extremely huge DDoS attack. Bot injects DDoS attacks, conducting spamming and phishing attacks [9] and helps the attacker to take dominance over the influenced computer, which acts like malware.

Different scanning tools can help to find the security holes in different stages of design. Recently, a DDoS attack detection was proposed through stresser, booster. DDoS and flash crowd varies with minimum parameters [10] so it is difficult to differentiate between them, this flash crowd triggers the attack which relies on traffic intensity. In this [11] the packet time series is fixed using Box-Cox transformation, is made used for better prediction based on some properties of attack time. In [12] the server gives a centralized interface which frequently checks the level of infected machine and current attack device. The bot is lodged in the target computer port number, type of attack and time to live parameters is included in the command, and implicitly it will execute the attack in the resources. The patterns are identified in data and inadequate to acquire the identity of attacks by using anomalous traffic[13].

The exponential and chaos theory details the detection rate of the attack to discover malicious and legitimate user, the lyapunvov exponents [14] generates false alarm, doesn't supports the slow legitimate connections. The nearest neighbor classifiers [15], rule-based covering algorithm like decision trees, random forests are hopeful perspectives for the IoT network for anomaly detection. Sending and receiving traffic rates infers consumer consumption behaviors [16]. This bloom filter [17] act as a quality time enhancer and space improving data structure to prevent DDoS attack. The verification filter in antidotes's [18] used to identify the legitimate packets from the malicious nodes , here bloom filters has a major role in listing the recent legitimate user. The attackers leverage different bots to manipulate traffic with real IP, it makes the detection process slow. Some techniques [19], [20], [21] are proposed. Still no such existing productive protection mechanism against the DDoS attacks.

Thus we propose a new flooding DDoS attack detection mechanism, in which the network traffic feature that captures the abnormality to model DDoS attacks in IoT, is used to discover and block DDoS victims more effectively.

3 Proposed Work

3.1 Detection and Prevention Techniques of DDoS Attack Variants

3.1 A) Flooding DDoS Attack Detection and Prevention Mechanism (FADM) The proposed flooding based DDoS attack detection mechanism is used against several DDoS attacks imitating flash crowds. The four types of abnormal traffic are classified as Iterative Request DDoS, Iterative Workload DDoS, Recursive Invocation DDoS, and Flash Crowd. Moreover, this is divided into three different phases. The first phase is abnormal traffic detection. This phase detects the abnormal traffic, an "ALERT" signal is sent to the next phase, which is the DDoS attack identification. When the "ALERT" signal reaches the DDoS attack detection, this phase calculates the frequency of the incoming IP address and its packets. When the frequency is calculated the entropy can be decided.The worth of the entropy classifies this attack as DDoS attack or flash crowd. The last phase is the filtration. This filters and elliminate the non-legitimate IP addresses while legitimate traffic continues to have access.

3.1 B) Anomalous Traffic Detection Anomalous traffic detection is the first phase of FADM. The main cause of this function is to detect sudden changes in REST traffic requests, like anomaly detection is sent to the server. This does not take any action if no anomalies are detected. If abnormal information is detected from the incoming REST traffic, an "ALERT" signal is passed to the next phase DDoS attack detection. This analyses the packet and makes a decision.1.

The traffic received is used to distinguish between different types of application-layer DDoS attacks and flash crowds.The first measurement is to analyze incoming traffic. This can be done in different ways, but it predicts traffic intensity by applying an Auto Regression

Table 1: DEFINITION OF NOTATIONS

Notations	Explanation
ψ_t	Estimation of the total packet received
x_t	Observation of the total packet received
d_t	Difference between ψ_t and x_t
FADM	Flooding DDoS Attack Detection Mechanism
T	0.1 second
$\tau 1$	2
$\tau 2$	4
$\tau 3$	8
j	1
z	3
l	6
m	100
φ	0.5
υ	0.5
POC	probability of collision
H	The entropy of received traffic
k$\rightarrow$ threshold	The threshold in our system is evaluated as 2×10^6 and this threshold works well till now.

model (AR model) [22]. The prediction rate in REST requests is monitored by using the simple AR model and the dynamical Kalman filter to correlate the prediction result.The procedure is narrated below. Initially, the REST and GET are monitored. A time series $\{\psi_1, \psi_2, ...\psi_t\}$ is formed by the traffic intensity which is studied at constant time intervals.The traffic intensity is preconceived by calculating the traffic intensity within the time limit.The intensity of the traffic helps to predict with the help of the Auto Regressive (AR) model. If major changes are detected, it can potentially be an application-layer DDoS attack. At a certain time t, dissimilarity of the observation xt with the prediction ψ_t is shown in equation(1).

$$d_t = \mid \psi_t - x_t \mid \tag{1}$$

The proposed AR model predicts the traffic of current traffic, identified by using equation (2)

$$\psi_t = \sum_{k=1}^{p} a_t^k x_{t-k} + e_t \tag{2}$$

The variable ψ_t is the prediction of instant time t, the variable a_t^kvarying time model parameter and e_t is the observation error. The weighted volume of p values to calculate the contemporary value of observation. This weight is dependent on time a_t^k(k=1,..,p).

From that specific residual under time t, a standard deviation ω_d^2can be calculated, as follows (3).

$$\omega_d^2 = \frac{\sum_{i=(t-p)}^{t} (d_t - AVG(_{d-t}))^2}{p} \tag{3}$$

Now, a threshold [23] shown in equation (4) is used for determining if the traffic is abnormal or not. If $d_t$is higher than kω_d^2, where k is the threshold value, abnormal traffic is detected, next the attack detection phase receives the "ALERT" signal .

FADM threshold value is examined as

$$d_t > k\omega_d^2 \tag{4}$$

4 DDoS Attack Detection

DDoS attack detection is the second phase. When an "ALERT" signal is received, the DDoS attack detection is activated. The manipulative entropy of the incoming traffic decides the type of DDoS attack occurred, or if there is flash crowd. Accordingly the entropy calculation is manipulated, by considering the value and dissimilarity of DDoS attacks and flash crowds are examined in the subsequent steps.

The entropy value is calculated by considering the packet traffic through monitoring things as follows. let M be the set user in N gateways denoted by g(l, δt)a number of packets at the outgoing queue of a nodes l at time δt for each time δt.The probability density function p_f(l,δt) of packets queuing at a things l of the set M is calculated as follows;

$$p_f(l, \delta t) = \frac{g(l, \delta t)}{\sum_{i=1}^{N} g(l, \delta t)} \tag{5}$$

The entropy is calculated using equation (6)

$$H(M, \delta t) = -\sum_{i=1}^{N} p_f(l, \delta t) * log(p_f(l, \delta t)) \tag{6}$$

To normalize the entropy value between [0,1] equation (7) is applied.

$$H'(M, \delta t) = \frac{H(M, \delta t)}{logN} \tag{7}$$

The Novel Entropy (NEB) scheme proposed is better due to the subsequent three facts:

I. Initially the legal traffic waves are recognized. This is known as the detection of shock wave [24] of legal traffic. The waves formed when an attack is observed, the wave is established when a legal traffic is detected, this gives a view that a very lean threshold decides it as a normal traffic or it tigers an alarm. This state achieves elevated detection rate and quieted false alarm rate.

II. The distinctive DDoS and flash crowds. There is a contrast in the raise and drop in the traffic speed.which is calculated based on data rate between them. The flash crowds [25] are restricted to use the same server when it starts its execution because the messages grab time to escalate among the users. Since the cardinal number hikes

to extreme; similarly, at the termination of the flash crowds, all participants regains their interest towards the server concurrently, to such a great extent, the number of request falls in huge difference from the extreme. Still, the attackers in DDoS initiate an immense quantity of invocation to the server, frequently or in a quick contrast time, to successfully bring the effect of desired attack. Hence the request to the server is enlarged suddenly to outstretch the extreme, subsequently dropped sharply at the termination stage of the attack. NEB calculates entropy to discriminate DDoS with flash crowds.

III. Internet traffic sample differs with time, as a result, H(M,δt) as it may deviate in a field. M is the number of things present inside the gateway , δt time and H is the entropy. Novel Entropy - based (NEB) adjusts H(M,δt) regularly to self-adapt network condition.

Algorithm 1 Novel Entropy Scheme - DDoS Detection Algorithm

Input: Entropy Calculation H(M,δt),τ_1,τ_2,τ_3,j,z,l,m,φ,υ
H(M,δt)= φ*H(M,δt)+(1- φ)*[H(M,δt)-H'(M,δt)]
θ =φ*θ+(1-φ)*(θ-θ')
Whereθ<ϕ<l,θ<υ<l
Output: DDoS Detection
1. Divide entire entropy field into four fields into normal, Lev1,Lev2 and Lev3
2. Initialize τ_1,τ_2,τ_3 and it should [θ<τ_1<τ_2< τ_3]
3. Let the h parameter be the property of H_C(M,δt),∀h∈H_c(M,δt)
If(|h-H(M,δt|<τ_1*θ) H=normal
Else if (a_1)*0 <|h-H(Mδt)|<τ_2*θ
{H=Lev1};
4. Else if(a_2*θ <|h-H(Mδt)|<τ_2*θ
{H=Lev2};
Else if(|h- H(M,δt)|> τ_3*θ
{H=Lev3};
5. If (H_c(M,δt)⊂Lev3)
//it means major difference comparing to H(M,δt)
{Return alert};// high rate DDoS attack
While (H_C(M,δt)⊂Lev2)
{//it may be low rate or flash crowd.}
If (rate of H_C (M,δt) shatter the threshold j)
{Return alert};//low rate
6. Else if (H_C (M,δt ⊂ Lv2)) until z*T seconds
{Return alert};//flash crowd
While ((H_C (M,δt ⊂ Lev1))
If (rate of H_C (M,δt) shatter the threshold j)
{Return alert};//low rate
7. Else if (H_C(M,δt ⊄ Normal) until l*T seconds
{Return alert};//low rate ddos
Else if ((H_C(M,δt ⊂ Normal)) until m*T seconds
{Return normal};

The NEB uses divide and conquer. The appropriate threshold is decided by τ, ideally the entire field is divided into different fields by distinct value τ,where τ is the designed parameter.

The novel entropy scheme - DDoS detection algorithm is explained as

1. The legal waves present in normal field. In certain condition the H(M,δt) ⊄ Normal so attack may happen. If so H_C(M,δt)⊂Lev3 is greater than H(M,δt)then it indicates high rate attack raises alarm.

2. The ((H_C (M,δt⊂Lev2)) condition is trivial to examine. The careful decision preferred to determine this as a flash crowd or an attack. The conditional rate of H_C(M,δt) is the threshold j,then it is considered as low rate. If(H_C (M,δt)⊂Lv2) until z*T seconds in other respects it should be a flash crowds.

3. When ((H_C (M,δt)⊂ Lev1)) the waves of legal traffic is normal in lev1. The traffic rate ofH_C(M,δt) is the threshold j, then it is alerted as low rate on the other side if(H_C (M,δt)) ⊄ Normal until l*T seconds then this is low rate DDoS. After all these the H_C(M,δt)⊂Normal until m*T seconds it alerts normal.

$$H(M,\delta t) = \varphi * H(M,\delta t) + (1-\varphi) * [H(M,\delta t) - H(M,\delta t)'] \quad (8)$$

$$\theta = \upsilon * \theta + (1-\upsilon) * (\theta - \theta') \quad (9)$$

Where $\theta < \phi < 1$, $\theta < \upsilon < 1$.

This proposed NEB algorithm ensures the detection of DDoS form flash crowd in an efficient way by flittering the legal waves and it works accurate in various network conditions. The upcoming filtering mechanism provides protection over the malicious user.

5 Filtering Mechanism

The last phase of FADM is the filter. After calculating the entropy from equation (8), if the value of the entropy for a specific source IP is indicated as a DDoS attack, the IP address is seen as anomalous. When abnormal traffic reaches the filter the anomalous IP address gets dropped and legitimate IP addresses are passed to the server. This phase uses the Bloom filter for determining which source IP addresses that are going to be dropped or continued. In order to decide this collision occurrence must be determined. The array of r bits is contemplated in a Bloom Filter and all items specified are equated to zero. Each S distinct hash functions plots or hashes fever elements, to distribute randomly in a uniform manner to allocate the position in an array. The bit array here in the proposed work is 2^{20} which is termed as m. The H_f is valued as 2, is used to execute the two hash functions. The IP addresses are represented by dotted decimals. The hash function is represented as

$$(X3+Y3+Z3+F3)\%2^{20} \quad (10)$$

$$(X3*Y3*Z3*F3)\%2^{20} \quad (11)$$

The IP address is passed to each hash function in equation 10 and equation 11 and the 2 array position is obtained and its position is set as one. The IP address must be present in the array in order to query an element. Again this is transmitted to the two hashes to obtain two positions now the bits in any position are turned to zero. Later the IP address is not used in the set, thus the limitation of conflict is fixed as $16*10^{-4}$. The bits are set as one when the IP address is present then the hash value also written as one. If not so, it will be a collision. The bloom flitter has two hash values and the hash table length is 2^{20} accompanies 20,000 aggregated address then the collision probability is evaluated as in equation 12.

$$\begin{aligned} POC &= lim_{r>>a}[1-(1-\frac{a}{r})^{H_f}]^{H_f} \\ &= lim_{r>>a}[1-(e-\frac{h_f a}{r})^{H_f}]^{H_f} \\ &< [(\frac{H_f a}{r})^{H_f}]^{H_f} < \frac{(2*2*10^4)}{(10^6)} \\ &= \frac{16}{10^4} \end{aligned} \tag{12}$$

6 Performance Evaluation

The simulation has been carried out to analyse the contribution of FADM for the DDoS. The elevated detection rate and false alarm rate are considered to process the implementation of the algorithm. The malicious ratio is determined by the probability of detection ratio and hence on the whole malicious user the malicious ratio is detected.

Likewise, the false alarm rate is judged by the standard probability of the malicious one, by monitoring the things, that are hitting indiscriminately at a specific probability attack ratio. The likelihood of the attacking is defined as the number of fraction, of malicious things and the entire malicious things number. The framework has 100 things set in a 100×100 square meter in the section area with random topology.

Fig.1shows performance between STM and our proposed work FADM.In this graph, by varying the number of attackers, we plot the graph for detection ratio. Detection ratio means the total number of attackers inside the network with how many attackers detected, so by increasing attackers the detection ratio decreases but while comparing to existing STM our proposed detection ratio is higher about 6%.

Fig.2shows performance between STM and our proposed work .In this graph, by varying the number of attackers, we plot the graph for false detection ratio. False detection ratio means the number of true things detected as attackers and attackers consider as true user, so by increasing attackers the false detection ratio increases but while comparing to existing STM our proposed detection ratio is lower about 8%.

Table 2: NETWORK PROPERTIES FOR SIMULATION

PARAMETER	VALUE
Simulator	NS-3.25
Topology	Random Node placement with IoT server and gateway
Number of things	100
Wifi Data Rate	1 Kbits/s to 10 M bits/s
Propagation Model	Log Distance Propagation Loss Mode
Traffic model	SURF
Channel Model	Yans, wifi channel Model
Simulation time	1000s
Protocols	FADM

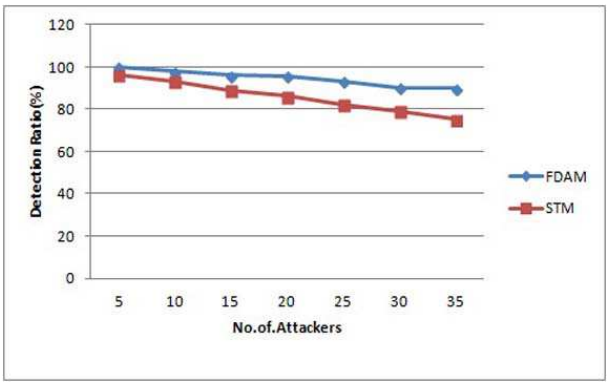

Fig. 1: Malicious user vs Detection Ratio

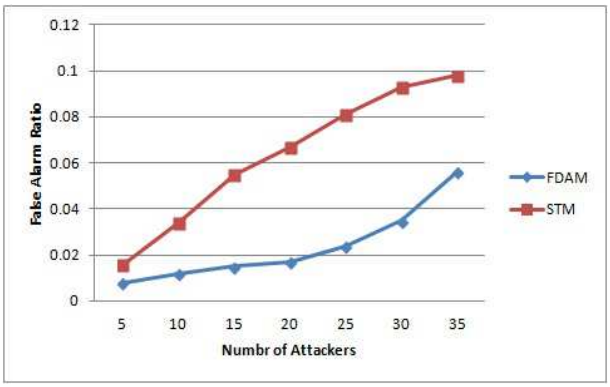

Fig. 2: Malicious user vs False Alarm Ratio

The outcome of the proposed FADM is differentiated with the spatiotemporal methodology in the DDoS probability. Fig.1 and Fig.2 illustrate the elevated detection rate and reduces the false alarm rate of FADM and Spatio-Temporal Methodology at heterogeneous attacks things from 5, 10,...,35 respectively. Evidently it is compared with the spatiotemporal methodology, ratio

of the detection is much better. Then the false alarm ratio is greatly demised by using the proposed method. As explained above, the elevated detection rate and false alarm rate are pretty stable, when the number of things is expanded. This result shows that the algorithm has agreeable scalability and suitable for compact on massive networks.

7 Conclusion

The initiated entropy-based approach is better while compared with existing algorithm Spatio-Temporal Methodology (STM), and the results highlights the improvements, creates sense in IoT. The new approach of DDoS mitigation provides the solution for inflated risk attacks in IoT environment. The simplicity and the adaptive nature assists a secure IoT environment for all levels of applications like, private smart home networks and big industrial IoT environments. The critical infrastructures with minimum and maximum complicity, make our proposed frame work to ensure the security in IoT environment. In the future, the manufacture can make sure to build the device with all these security features to protect IoT enabled devices, implicitly it avoids becoming a botnets. In order to realize this scheme a lightweight authentication scheme can be implemented to ensure the security and enhance its performance.

References

[1] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez H.A ,Survey of iot-enabled cyberattacks Assessing attack paths to critical infrastructures and services,*IEEE Communications Surveys and Tutorials*,Volume 20,3453-3495,(2018).

[2] K.Sonar and H. Upadhyay, A Survey DDOS Attack on Internet of Things, *Intl. Journal of Engineering Research and Development*, 10, 11, 58-63,(2014).

[3] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, DDoS-Capable IoT Malwares Comparative Analysis and Mirai Investigation, *Security and Communication Networks*,2018, 1–30, (2018).

[4] W. Aman, Waqas, *Assessing the feasibility of adaptive security models for the internet of things*, International Conference on Human Aspects of Information Security, Privacy, and Trust, springer International Publishing,201-211(2016).

[5] Vlajic, Natalija and Zhou, Daiwei, IoT as a Land of Opportunity for DDoS Hackers,*Computer*,5,26-34 (2018).

[6] Wessels, Duane, and Matt Weinberg.*Method and system for detecting and mitigating denial-of-service attacks*.U.S. Patent Application 15/392,700,(2018).

[7] Kalkan, Kübra, Levent Altay, Gürkan Gür, and Fatih Alagöz,JESS: Joint Entropy-Based DDoS Defense Scheme in SDN,*IEEE Journal on Selected Areas in Communications*36,2358-2372(2018).

[8] Bhatia, Sajal, Sunny Behal, and Irfan Ahmed. *Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions*,79, Versatile Cybersecurity, Springer, Cham,55-97 (2018).

[9] Karami, Mohammad and Park, Youngsam and McCoy, Damon,*Stress testing the booters: Understanding and undermining the business of ddos services*,in Proceedings of the 25th International Conference on World Wide Web,Switzerland Available,1033-1043,(2016).

[10] Khalaf, Bashar Ahmed, Salama A. Mostafa, Aida Mustapha, and Noryusliza Abdullah,*An Adaptive Model for Detection and Prevention of DDoS and Flash Crowd Flooding Attacks*,International Symposium on Agent, Multi-Agent Systems and Robotics(ISAMSR)IEEE,1-6,(2018).

[11] Nezhad, Seyyed Meysam Tabatabaie and Nazari, Mahboubeh and Gharavol, Ebrahim A,A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks,*IEEE Commun.Lett*, 20,700-703,(2016).

[12] Doshi, Rohan, Noah Apthorpe, and Nick Feamster,*Machine Learning DDoS Detection for Consumer Internet of Things Devices*, IEEE Security and Privacy Workshops(SPW),IEEE,29-35,(2018).

[13]]Jing, Xuyang, Zheng Yan, Xueqin Liang, and Witold Pedrycz,Network Traffic Fusion and Analysis against DDoS Flooding Attacks with a Novel Reversible Sketch,*Information Fusion,Elsevier*, 51,100-131,(2018).

[14] Procopiou, Andria, Nikos Komninos, and Christos Douligeris,ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network, *Wireless Communications and Mobile Computing,Hindawi*,2019,(2019).

[15] Moustafa, Nour and Hu, Jiankun and Slay, Jill,A holistic review of Network Anomaly Detection Systems:A comprehensive survey,*Journal of Network and Computer Applications,Elsevier*,128,33–55,(2019). FADMFAMS

[16] Doron, Ehud and Ilani, Nir and Aviv, David and Yotam, BEN and Bismut, Amit,*Distributed denial of service (ddos) defense techniques for applications hosted in cloud computing platforms*,US Patent App. 15/907,905,Google Patents,(2018).

[17] Patgiri, Ripon and Nayak, Sabuzima and Borgohain, Samir Kumar,Preventing DDos using bloom filter: A survey,*arXiv*,5,19,(2018).

[18] Simpson, Steven and Shirazi, Syed Noorulhassan and Marnerides, Angelos and Jouet, Simon and Pezaros, Dimitrios and Hutchison, David,An inter-domain collaboration scheme to remedy ddos attacks in computer networks,*IEEE Transactions on Network and Service Management,IEEE*, 15,879-893,(2018).

[19] C.X.Wang,T.T.N. Miu, X.P.Luo , and J.H.Wang,SkyShield: A Sketch-Based Defense System Against Application Layer DDoS Attacks,*IEEE Transactions on Information Forensics and Security,IEEE*,13,559-573(2018).

[20] Wang, An, Wentao Chang, Songqing Chen, and Aziz Mohaisen,Delving into internet DDoS attacks by botnets: characterization and analysis,*IEEE or ACM Transactions on Networking,IEEE*, 2018,2843-2855,(2018).

[21] Toklu.S and M. Şimşek.Two-Layer Approach for Mixed High-Rate and Low-Rate Distributed Denial of Service (DDoS) Attack Detection and Filtering,*Arabian Journal for Science and Engineering,Springer*, 43,7923-7931,(2018).

[22] Uchiyama, Yuichi and Waizumi, Yuji and Kato, Nei and Nemoto, Yoshiaki,Detecting and tracing DDoS attacks in the traffic analysis using auto regressive model,*IEICE TRANSACTIONS on Information and Systems*,87,2635–2643,year(2004).

[23] Sardana, Anjali, Ramesh C. Joshi, Tai-hoon Kim, and Sung Jang,Deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate DDoS attacks in ISP domain honeypot based approach,*Journal of Intelligent Manufacturing,Springer*, 21,623-634,(2010).

[24] *Attackers Use DDoS Pulses to Pin Down Multiple Targets Send Shock Waves Through Hybrids*,Technical Report,Imperva Incapsula,(2017).

[25] Peng, Tao and Leckie, Christopher and Ramamohanarao, Kotagiri,Survey of network-based defense mechanisms countering the DoS and DDoS problems,*ACM Computing Surveys CSUR,ACM*,39,3,(2007).

R. Radhika is currently pursuing her Ph.D program in the Department of Information Science and Technology, College of Engineering Guindy Campus, Anna University, Chennai, India. She has completed her M.E in Computer Science and Engineering from College of Engineering Guindy Campus, Anna University, Chennai, India. Her areas of Interests are Internet of Things, Networks Security and Data Science. She is a Lifetime member of Indian Society for Technical Education (ISTE).

K. Kulothungan is currently working as an Associate Professor in the Department of Information Science and Technology, College of Engineering Guindy Campus, Anna University, Chennai, India. He received his M.E and PhD form Sathyabama University and Anna university Chennai, India. He is the coordinator of CISCO networking Academy, Anna University Chennai and certified instructor (CCAI). Currently, he is guiding more than ten research scholars. His research areas include Wireless Sensor Networks, Network Security, Web design and Management, Embedded systems and Internet of Things. He has more than 12 research publications in national conferences, 21, research publications in international conferences and 16 research publications in international journals.