EDAA - An Efficient DDoS Association Analysis using Hypergraph Clustering in Fog Computing

[1]K. Arun Kumar, [2]C. Santhosh, [3]S. Shanmugapriya
[1, 2, 3]*Assistant Professor,*
[1, 2]*Department of IT,* [3]*Department of Commerce*
[1]*School of CS & IT, Jain University, Bengaluru,*
[2]*Nandha Engineering College, Erode,* [3]*Dr. NGP Arts and Science College, Coimbatore.*

Abstract

The evolution of fog computing has given rise to many security threats. Distributed denial of service (DDoS) attacks by intruder on fog nodes will cause system resources to be illegitimately fitting. Intrusion detection system (IDS) is a powerful technology that can be used to resist DDoS attacks. I propose a fog computing intrusion detection system (FC-IDS) framework. In this paper, the DDoS attacks under the framework of FC-IDS is mainly analyzed and modeled. I also propose a hypergraph clustering model based on Apriori algorithm. This model can effectively describe the association between fog nodes which are suffering from the threat of DDoS. Through simulation, the resource utilization rate of the system can be effectively promoted through the DDoS association analysis has been verified.

Keywords - *DDoS, Fog computing, Hypergraph Clustering, Intrusion detection system, Association analysis*

I. INTRODUCTION

Fog computing offers a highly virtualized platform that provides compute, storage, and networking services between end devices and data centers. As with the cloud, fog is predicated on the availability of compute, storage, and connectivity resources. These resources must be located within close physical proximity to users to alleviate problems associated with cloud computing. Fog nodes may take the form of servers or networking equipment with additional computational resources. They may even be integrated into wireless access points. Fog nodes will typically be located at the edge of the network, within close proximity to end users.

Fog computing, as a new computing paradigm, is consistent with the idea of edge computing as in [2], which pushes computing tasks to the edge of the network. The whole network is usually divided into three layers in fog computing as in [3]: cloud service layer, fog service layer, and user layer. Fig. 1 shows a network structure diagram of fog computing in radio environment. The user layer generates data, which is a source of data. Fog service layer is a layer closest to users, mainly composed of fog nodes, which is used to provide data services directly to users. The cloud server is in charge of the management and control of the fog nodes, which is connected to the fog service layer by the core network. As a new computing paradigm, the security problem of the fog computing cannot be underestimated as in [4]. The main service node, the fog node, may be composed of a gateway, a router, a server at the edge of the network, and other devices, because fog service layer is a unique layer in fog computing as in [5]. Fog nodes have the following characteristics:

(1)The distribution of fog nodes is distributed geographically and has high distribution;

(2)Fog nodes are limited in computing resources and storage resources compared with cloud servers;

(3) Fog nodes need to deal with heterogeneous data from the user layer locally, and

(4)Fog nodes should have high heterogeneous compatibility.

These characteristics make the fog node particularly vulnerable to attack from the outside, such as DDoS, R2L, PROBE, U2R, and so on. Once the fog node is attacked by DDoS especially due to limited resources, the performance of the network will be greatly reduced, which will not provide services for users. This requires effective detection and prevention of DDoS attacks as in [6]. The traditional network security technology such as physical security technology as in [7] is difficult to resist the multi-source and cross-domain intrusion. Intrusion detection system (IDS) as in [8] is an effective technology to ensure the security of fog computing. A fog computing intrusion detection system (FC-IDS) for detecting and defending against external attacks on fog is proposed in our previous study as in [9]. Some research has been done to effectively detect and defend against intrusion as in [10] on this basis.

The defense and analysis of DDoS has not been involved in the previous work, which is the focus of this paper. The DDoS in the fog computing is an illegal occupation of bandwidth resources and computing resources of the fog node. An attack process has been studied and hypothesized in a fog computing environment where intruders perform DDoS attacks on multiple fog nodes at different

frequencies. Some fog nodes have the possibility of being frequently coordinated during a period of time. It is necessary to perform data mining on the relationship of the attack of the fog node in order to analyze the intruder's strategy more deeply and seek its deep-level attack intention.

The discovery of associations can help the cloud server to implement further security policies. For example, the cloud server can infer the scope of the attacker's geographic location for intrusion tracking by combining the geographic location information of the fog nodes. In addition, the cloud server is in charge of the management and control of the fog node. The resource of the fog node can also be deployed after the cloud server obtains the result of the DDoS association analysis of the fog node. This paper models and analyzes DDoS attacks in fog clusters based on hypergraph clustering algorithm and can find the relationship between fog clusters and DDoS attacks.

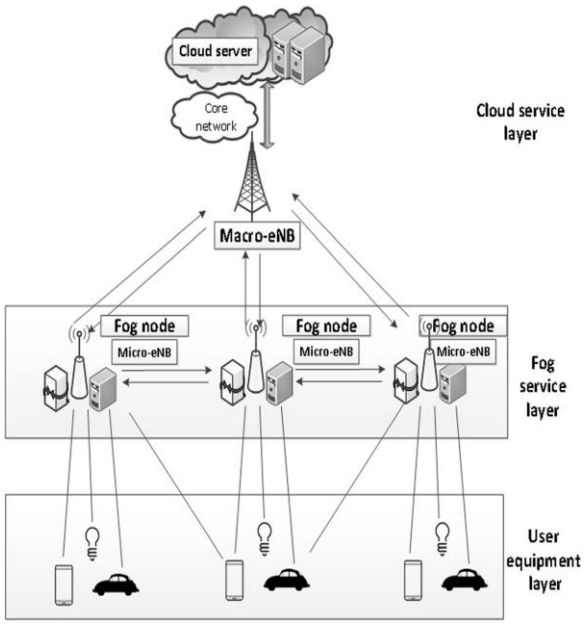

Fig.1. Fog Computing Architecture

The main contributions of this article are the following:

(1) The attack process of DDoS was analyzed in the fog computing environment, and

(2) The relationship was modeled between fog nodes and DDoS based on hypergraphs.

A. Related Works

The authors in [15] propose a Fog CompUting based Security (FOCUS) system to protect the IoT against malware cyber attacks. This system mainly deals with man in the middle attack and DDoS attack. In addition, FOCUS is implemented in fog computing to achieve a fast response and an efficient network consumption. The authors in [16] propose a multi-level DDoS mitigation framework (MLDMF) to defend against DDoS attacks for edge computing, fog computing, and cloud computing. A framework as in [17] specifically used to defend against DDoS attacks is proposed. The main purpose of this framework is to protect the cloud through fog nodes. The authors in [18] build a novel mathematical framework based on game theory and epidemic theory to investigate the interplay between user incentives and interdependent security risks (DDoS) in mobile edge computing. A general fog computing IDS framework is proposed as in [9], and the fog computing intrusion detection classifier model based on the sample selection extreme learning machine is studied under the framework. The classifier in this architecture can effectively solve the problems of low intrusion detection efficiency and poor precision due to the characteristics of finite fog computing resource constraints. In this framework, the authors as in [19] studied the problem of the allocation of system defense resources and proposed a single layer advantage and maximum minimum equitable distribution strategy, which divided the multi-level resource requirements into a series of single layer resource requirements. This research improves the performance of intrusion detection

B. Distributed denial of service (DDoS) attacks

DDoS attack is a distributed, large scale coordinated at-tempt of flooding the network with an enormous amount of packets which is difficult for victim network to han-dle, and hence the victim becomes unable to provide the services to its legitimate user and also the network performance is greatly deteriorated. This attack exhausts the resources of the victim network such as bandwidth, memory, computing power etc. The system which suffers from attacked or whose services are attacked is called as "primary victim" and on other hand "secondary victims" is the system that is used to originate the attack. These secondary victims provide the attacker, the ability to wage a more powerful DDoS attack as it is difficult to track down the real attacker. Denial of Service (DoS) attacks is used to consume all the resources of the target machine (victim's services) Distributed denial of service (DDoS) attack is some sort of malicious activity or a typical behavior, which cooperate the availability of the server's resources and prevents the legitimate users from using the service. DDOS attacks are not meant to alter data contents or achieve illegal access, but in that place they target to crash the servers, generally by temporarily interrupting or suspending the services of a host connected to the Internet. DOS attacks can occur from either a single source or multiple sources. Multiple source DOS attacks are called distributed denial-of service (DDOS) attacks. A Denial of Service (DoS) attack is an attempt to make a computer resource unavailable to normal users. The Dos attacks are becoming more powerful due to bot behavior. Attack that leverages multiple

sources to create the denial-of-service condition is known as The Distributed Denial of Service (DDoS) attack. DDoS attacks are big threats to internet services. HTTP flooding attack is one of the typical DDos attack, in that hosts are sending large amount of request to target website to exhaust its resources. Now a day there is massive growth in internet traffic. Due to this many DDoS attack detection systems facing a problem. A Distributed Denial of service (DDos) attack can employ hundreds or even thousands of computers that have been previously flooded by HTTP GET packet.

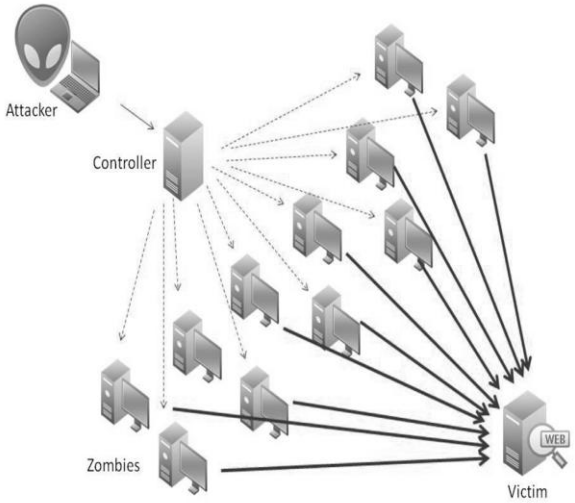

Fig.2. DDOS Attack

II. INTRUSION DETECTION SYSTEM ARCHITECTURE

DDoS attacks refer to the use of a large number of requests
to access the fog cluster, thereby achieving the purpose of occupying the network resources of the fog node. The intruder first controls a large number of devices at the user layer in the user layer by means of implanting Trojans and viruses in the fog computing. The "infected" device is controlled by the attacker, and then a large number of illegal requests are made to the fog node to form a DDoS attack. The attack source comes from the user layer as shown in Fig. 3. The fog nodes are geographically distributed, and the devices accessing each fog node are different in the entire fog cluster. In addition, there are differences in processing power, memory size, and network bandwidth resources of different fog nodes. That is to say, the network environment faced by the fog nodes and their network computing resources are greatly different. This difference gives the attacker the option of intrusion. Intrusion
strategies have been discussed for intruders and response strategies for fog clusters in previous studies as in [10]. The attacker will initiate a DDoS attack on different fog node i at different times ri(t) at a certain timet. An intruder's distributed attack on the network resources of the fog node may have the following consequences as shown in Fig. 4:

1. The path of legitimate access by occupying or interfering with the network port of the fog node is blocked.
2. The fog node is overloaded by submitting a large number of illegal requests to the fog node
3. The normal access rights of the original legitimate users are blocked
4. The communication between the fog node and the cloud service layer or user layer is blocked.

The DDoS from the outside can be dealt with by FC-IDS. Fig. 5 is the architecture of FC-IDS although the intruder will cause serious loss to the fog computing through DDoS of different frequencies. FC-IDS has the following effects in dealing with DDoS:
(1) The detection layer of FC-IDS can effectively detect DDoS attacks and form a database of security logs on the fog nodes to record the situation where the fog nodes are attacked.
(2) The cloud server monitors and analyzes the situation that the fog node suffers from DDoS in real time. The behavior and attempts of the intruder can be described through the overall monitoring and data mining of the fog cluster.
(3) The most appropriate intrusion response is made to the intruder's behavior for the results of the detection and the conclusion of the information analysis.

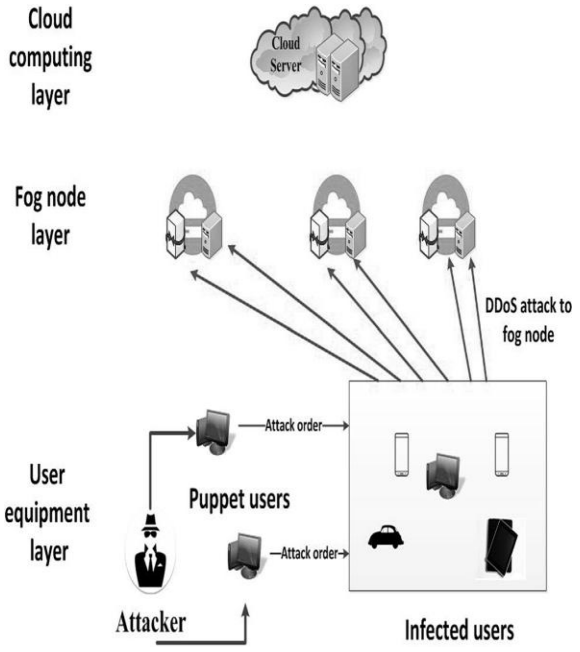

Fig.3. DDoS Attack in Fog Computing

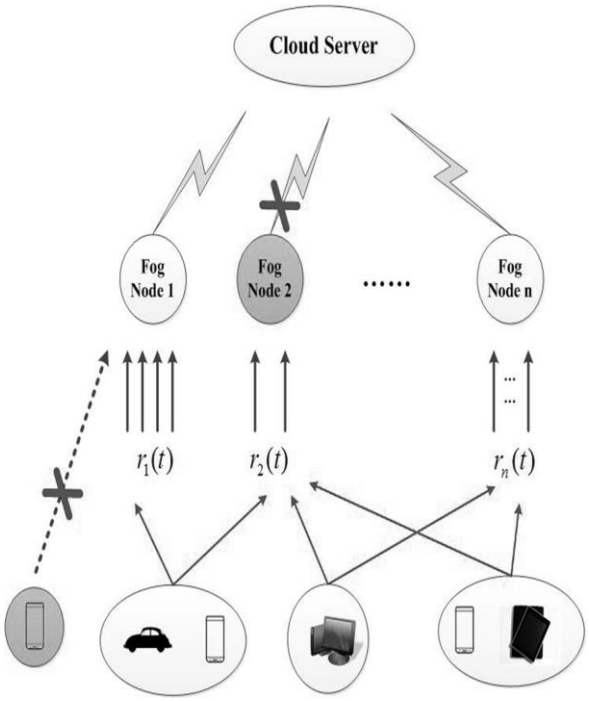

Fig.4. DDoS Attacked in Fog computing

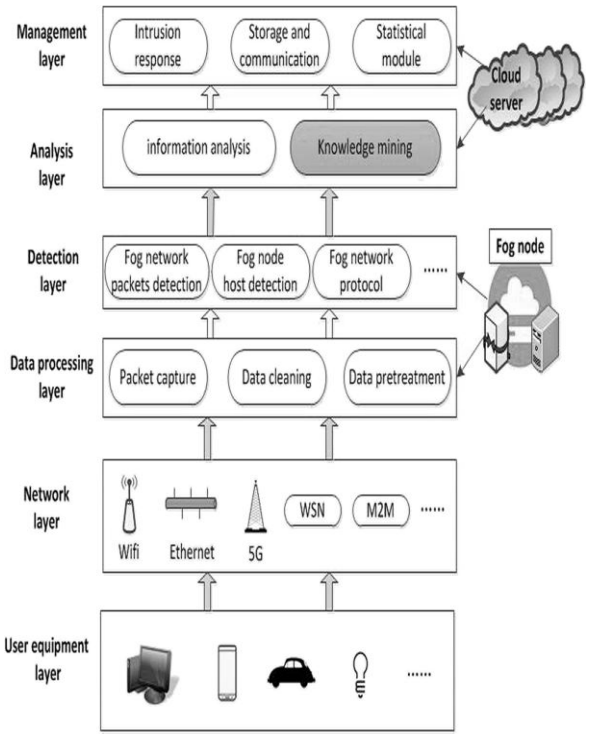

Fig.5. Fog Computing Intrusion Detection Framework

III. DDOS ASSOCIATION ANALYSIS OF HYPERGRAPH CLUSTERING

Based on the hypergraph clustering, the DDoS of the fog node is modeled the Apriori algorithm for correlation analysis is used. It is assumed that the fog cluster faces only one attacker. The cluster of fog nodes is simultaneously attacked by DDoS at time t. FC-IDS can be used to calculate the DDoS attacks on the fog nodes at different times, which constitute a priori data set of the fog nodes. It is necessary to define resource-related parameters in fog nodes to describe hypernodes and hyperedges in hypergraphs. The hypergraph is used to model the network bandwidth resources of the fog node when an intruder conducts a DDoS attack. The set of the fog node resources includes a resource ID, a bandwidth B, a power P, a current transmission rate R, a channel gain H of the user corresponding fog node, and a resource state S

Definition 1 Hypergraph model for the fog computing network: G = (F, E). F is a fog node and is a hypernode in
the hypergraph. E is the hyperedge of the hypernode connected to the hypergraph.

It is supposed that F = {f1, f2,.., fn} is a fog cluster
composed of fog nodes. There are n fog nodes in the cluster, i ∈ [1, n]. Where fi represents the ith fog node, and the resources are independent on the fog node.

The ID is used to identify the RRH; B is the bandwidth when the UE establishes communication with the node; P is the power when the node communicates with the
UE; H is the channel gain; and Load represents the load of the resource node.
fS = {fNormal, fCongestion, fFree, fInvalid} respectively
represent the four states of the fog node: Network service is normal, network congestion, network idle, and loss of connection. It is the state of fNormal when the user traffic on the fog node is normal. The state changes to fCongestion, which means that the fog node has the possibility of being threatened by DDoS when there is excessive traffic access on the fog node. It indicates that the fog node has no network data flow when the fog node is at fInvalid. The fInvalid is used to indicate that the network resources of the fog node are exhausted.

The hyperedge is used to describe the relationship
between the fog nodes in this model. It is mined by the Apriori algorithm as in [20]. A two-dimensional scribing conditional bandwidth allocation hypergraph clustering algorithm is proposed based on Apriori clustering algorithm in the process of finding the association relationship.

Algorithm 1 Hypergraph clustering algorithm based on the Apriori

```
    L1 =find_frequent_1-itemsets(D);
    For (k=2; Lk-1 != null;k++){
// Produce a candidate and prune
      Ck =apriori_gen(Lk-1 );
   // D for candidates counting
      For each t in D {
        Ct =subset(Ck,t); // subset of t
        For each  c ∈Ct
          c.count++;
      }
      // Return an item set that is not less than minimum support
      Lk ={c∈Ck | c.count>=min_sup}
}
Return L= All frequent sets;
// First step: join.
Procedure apriori_gen (Lk-1: frequent(k-1)-itemsets)
    For each l1∈Lk-1
      For each l2∈Lk-1
        If ((l1 [1] =l2 [1]) && (l1 [2] =l2 [2]) && .....&& (l1 [k-2] =l2 [k-2]) && (l1 [k-1]
<l2 [k-1]))
then {
              c = l1 join to l2

              if has_infrequent_subset (c, Lk-1) then
                 delete c;
              else add c to Ck;
              }
        Return Ck;
// Second step: prune.
 Procedure  has_infrequent_sub  (c:candidate  k-itemset;  Lk-1  :frequent(k-1)-
itemsets)
       For each (k-1)-subset s of c
         If s ∉  Lk-1, then
           Return true;
         Return false;
```

Definition 2 E = {e1, e2,.., em} is a collection of hyperedges ej = {mj,Wj}, where mj is the number of nodes included in the hyperedge ej and Wj is the weight value of the hyperedge.

A key issue is to determine the relevant classes that
can be classified into hyperedges and determine the weight of each hyperedge in the hypergraph model. The hyperedge is connected to the fog node that suffers from DDoS in our model, which itself represents an association. The support and the amount of resources of the fog node is used to represent the weight of the hyperedge. There is a lot of work that can be done around this model through hypergraph clustering modeling. For example, MaxW j is obtained by comparing Wj at a certain time. The corresponding set of fog nodes is the fog node that was attacked by the DDoS attack at the previous moment. The security of the fog nodes can be effectively protected by focusing on the monitoring and defense of these collections.

IV. PERFORMANCE

The main purpose of simulation experiment is to verify that hypergraph clustering model can play a key role in defending against DDoS. The performance of the system in the wireless fog computing environment when the system is attacked by DDoS is simulated. The radio communication system from the point of legal UE access number and radio resource utilization is simulated. In the simulation environment, a radio communication system is composed of a cloud server and a plurality of fog nodes (FNs) is assumed. First, the performance of fog computing network structure on the access number of legal UE is analyzed. The two intensities of DDoS are used in the simulation. As shown in Fig. 6, we can see in fog computing, with the number of FNs increasing, the access number of legal UE in the system can increase. In the case of different DDoS attacks, the access amounts of legitimate users
have varying degrees of attenuation. When the fog nodes are invaded of DDoS, their resource utilization rate is decreasing. Simulation of intruders to attack DDoS with different numbers of devices is done, so as to simulate the intensity of DDoS attacks. Through the association analysis, the previous intrusion response strategy to simulate the resource utilization of fog nodes is combined. Fig. 7 shows the radio resource utilization in fog computing. With the increase of the UE group size, the radio resource utilization declines rapidly in the range of 100 to 400, and the decline rate slows down gradually in the range of 400 to 450.Comparing with no association analysis network, fog computing network has better performance in radio resource utilization. In the above experiment, the test data is analyzed and the confidence interval according to the 95% confidence level is chosen. In addition, the influence of intrusion response strategy is combined, such as calculating the maximum number of access to UE. It should be noted that the limitations of the experimental results are due to the fact that our hypergraph clustering model is greatly influenced by prior data sets.

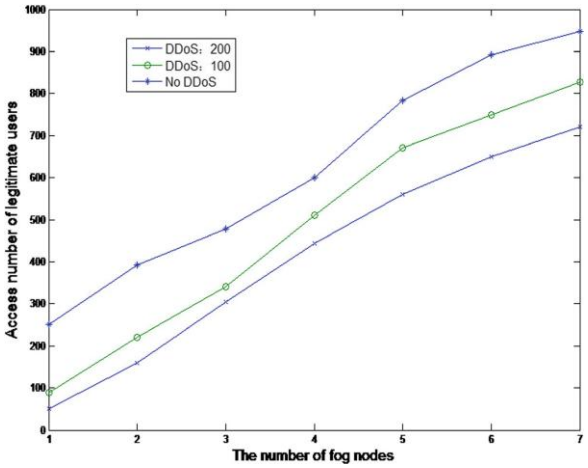

Fig.6. Maximum number of access

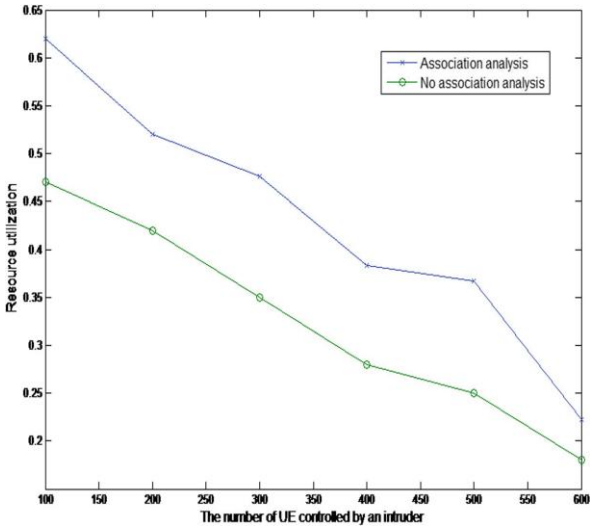

Fig.7. Resource utilization

V. CONCLUSIONS

The security problem restricts the deployment and development of fog computing. Among many security threats, DDoS is the most common means of network attack. DDoS attacks can reduce the resource utilization of fog nodes. Mining DDoS intentions from intruders through association analysis is a meaningful work. In this paper, a hypergraph clustering model is used to analyze the association of fog nodes which are suffering from DDoS. Because of the destruction of system resources by DDoS, we verified the performance of our model in resource utilization by combining intrusion response strategy in simulation. Because of the destructiveness of DDoS to system resources, we combine intrusion response strategy in simulation. Simulation results show that our model has better performance for resource utilization of fog nodes.

REFERENCES

[1] Bonomi, F, et al. Fog computing and its role in the internet of things. Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM (2012)
[2] W.Shi et al., Edge computing: Vision and challenges. IEEE Internet of Things Journal 3(5), 637–646 (2016)
[3] S.Jingtao et al., Steiner tree based optimal resource caching scheme in fog computing. China Communications 12(8), 161–168 (2015)
[4] A.Alrawais et al., Fog computing for the internet of things: security and privacy issues. IEEE Internet Computing 21(2), 34–42 (2017)
[5] Y.Huo, C. Yong, Y. Lu, Re-ADP: real-time data aggregation with adaptive wevent differential privacy for fog computing. Wireless Communications and Mobile Computing, 1–13 (2018)
[6] R.Roman, J. Lopez, M. Mambo, Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. Future Generation Computer Systems 78, 680–698 (2018)
[7] Y.Huo, Y. Tian, L. Ma, X. Cheng, T. Jing, Jamming strategies for physical layer security. IEEE Wireless Communications 25(1), 148–153 (2018)
[8] D.E.Denning, An intrusion-detection model. IEEE Transactions on software engineering 2, 222–232 (1987)
[9] X.An et al., Sample selected extreme learning machine based intrusion detection in fog computing and MEC. Wireless Communications & Mobile Computing 2018, 1–10 (2018)
[10] X.An, F. Lin, S. Xu, L. Miao, and G. Chao, "A Novel Differential Game ModelBased Intrusion Response Strategy in Fog Computing,". Security and Communication Networks 2018, 9 (2018). https://doi.org/10.1155/2018/ 1821804
[11] Stojmenovic, I, and Sheng W. The fog computing paradigm: Scenarios and security issues. Computer Science and Information Systems (FedCSIS) 2014 Federated conference on. IEEE (2014).
[12] C.Thota et al., Centralized fog computing security platform for IoT and cloud in healthcare system. Exploring the convergence of big data and the internet of things. IGI Global, 141–154 (2018)
[13] I.Stojmenovic et al., An overview of fog computing and its security issues. Concurrency and Computation: Practice and Experience 28(10), 2991–3005 (2016)
[14] D.Chaudhary, K. Bhushan, B.B. Gupta, Survey on DDoS attacks and defense mechanisms in cloud and fog computing. International Journal of E-Services and Mobile Applications (IJESMA) 10(3), 61–83 (2018)
[15] Alharbi, S, et al. FOCUS: A fog computing-based security system for the Internet of Things. Proceedings of the IEEE Consumer Communications & NETWORKING Conference IEEE, (2018):1–5
[16] Q.Yan et al., A multi-level DDoS mitigation framework for the industrial internet of things. IEEE Commun. Mag. 56(2), 30–36 (2018)
[17] Deepali, and K Bhushan. DDoS attack defense framework for cloud using fog computing. Proceedings of the IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology IEEE, (2017): 534–538
[18] J.Xu, L. Chen, K. Liu, and C. Shen, Less is more: participation incentives in D2D-enhanced mobile edge computing under infectious DDoS attacks, arXiv (2017) [Online]. Available: http://arxiv.org/abs/1611.03841
[19] F.Lin, Y. Zhou, X. An, I. You and K. R. Choo, Fair Resource Allocation in an Intrusion-Detection System for Edge Computing: Ensuring the Security of Internet of Things Devices. IEEE Consum. Electron. Mag. 7(6), 45–50 (2018). https://doi.org/10.1109/MCE.2018.2851723
[20] R.Liang, W. Guo, D. Yang, Mining product problems from online feedback of Chinese users. Kybernetes 46(3), 572–586 (2017)
[21] Ishii, H, Y Kishiyama, and H Takahashi. A Novel Architecture for LTE-B: CPlane/U-Plane Split and Phantom Cell Concept. Globecom Workshops (GC Wkshps), IEEE. (2012)