An et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:249
https://doi.org/10.1186/s13638-018-1267-2

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system

Xingshuo An[1], Jingtao Su[1], Xing Lü[1] and Fuhong Lin[1,2*]

Abstract

The birth of fog computing has given rise to many security threats. Distributed denial of service (DDoS) attacks by intruders on fog nodes will cause system resources to be illegally appropriate. Intrusion detection system (IDS) is a powerful technology that can be used to resist DDoS attacks. In our previous research, we have proposed a fog computing intrusion detection system (FC-IDS) framework. In this paper, we mainly analyze and model the DDoS attacks under the framework of FC-IDS. We 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, we verify that the resource utilization rate of the system can be effectively promoted through the DDoS association analysis.

Keywords: DDoS, Fog computing, Hypergraph theory, Intrusion detection system, Association analysis

1 Introduction

Many computing paradigms have been put forward to solve different needs of services since the birth of the Internet. Fog computing, as a new computing paradigm, was first put forward by CISCO [1]. It is consistent with the idea of edge computing [2], which pushes computing tasks to the edge of the network.

The whole network is usually divided into three layers in fog computing [3]: cloud service layer, fog service layer, and user layer. Figure 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 [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 [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 [6].

The traditional network security technology such as physical security technology [7] is difficult to resist the multi-source and cross-domain intrusion. Intrusion detection system (IDS) [8] is an effective technology to ensure the security of fog computing. A fog computing intrusion detection system (FC-IDS) for

* Correspondence: FHLin@ustb.edu.cn
[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, People's Republic of China
[2]Beijing Engineering and Technology Research Center for Convergence Networks and Ubiquitous Services, University of Science and Technology Beijing, Beijing 100083, People's Republic of China

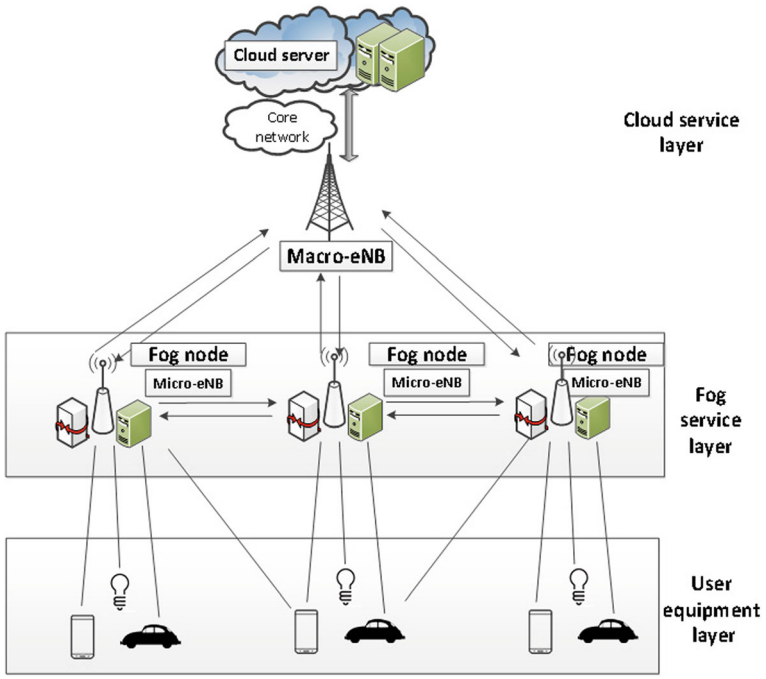

Fig. 1 Fog computing architecture in radio environment

detecting and defending against external attacks on fog is proposed in our previous study [9]. Some research has been done to effectively detect and defend against intrusion [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. 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.

The rest of this paper is organized as follows: Section 2 introduces some related work about DDoS attack in fog computing. DDoS in Intrusion Detection System Architecture of fog Computing is introduced in Section 3. Section 4 proposes the network model using Hypergraph theory and Apriori. The simulation is taken out in Section 5. In Section 6, a conclusion is drawn.

2 Related works

The security of fog computing has been attracting much attention. Many Refs. [11–13] review the network characteristics of fog computing and the security problems it faces. DDoS attack is a common network attack. In this section, we review the related works. Some studies focused on the DDoS in fog computing.

Whether in cloud computing or fog computing, DDoS will bring greater security threats to the network. Ref. [14] discusses how DDoS affects the cloud server and how fog computing can be used in a cloud environment to solve a variety of problems.

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 [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 [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, Fuhong et al. [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 system through resource allocation.

In summary, some of the above studies have introduced DDoS in fog computing, and some have analyzed resource allocation in intrusion environments. Although these studies have expanded new ideas for our research, there is no research on the association analysis of DDoS in the fog environment.

3 DDoS in intrusion detection system architecture of fog computing

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. 2.

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 [10]. The attacker will initiate a DDoS attack on different fog node i at different times $r_i(t)$ at a certain time$t$. An intruder's distributed attack on the network resources of the fog node may have the following consequences as shown in Fig. 3:

1. The path of legitimate access by occupying or interfering with the network port of the fog node is blocked.

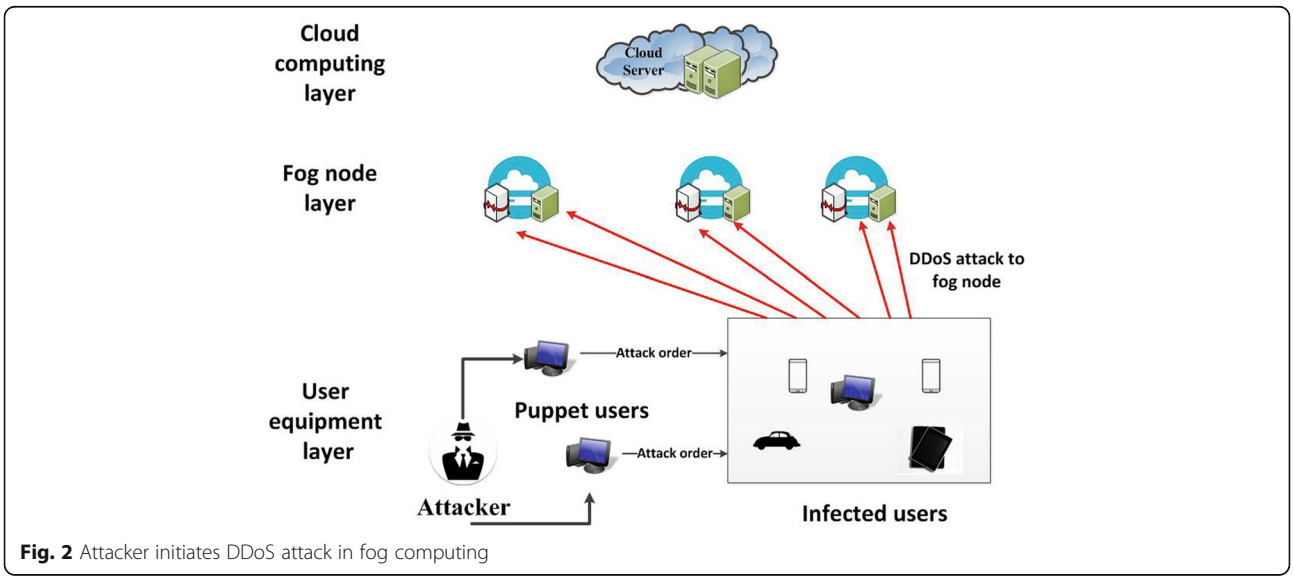

Fig. 2 Attacker initiates DDoS attack in fog computing

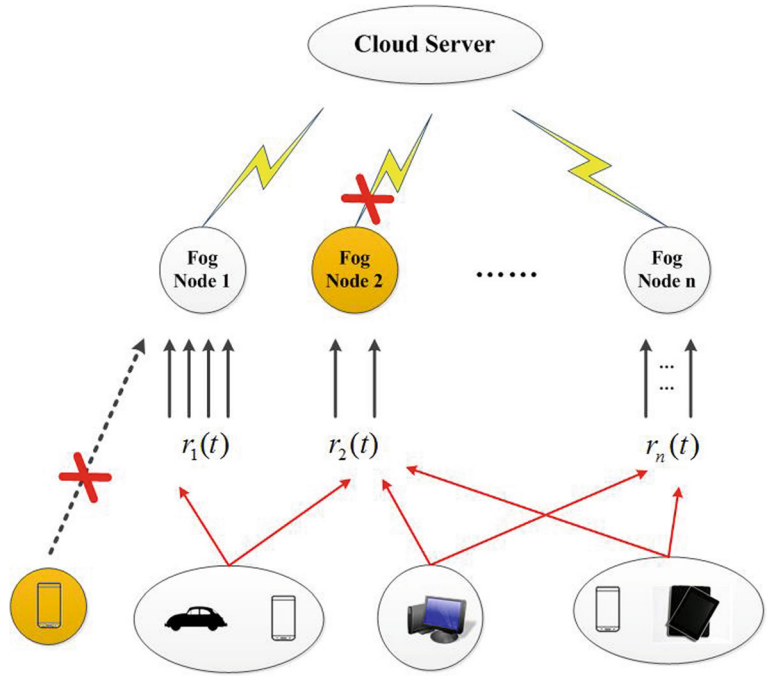

Fig. 3 The damage caused by DDoS in the fog computing

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. Figure 4 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

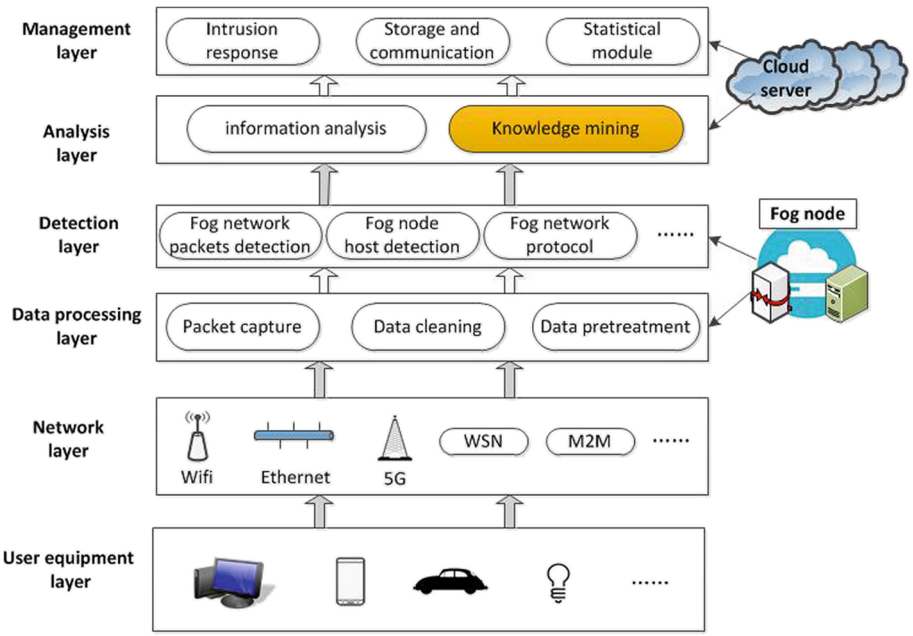

Fig. 4 Fog computing intrusion detection system framework

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. The first part and the second part have been studied in Ref. [9] and Ref. [10] among them. The second part is the focus in this paper: Correlation analysis of frequent items is performed for statistical data of fog node intrusion detection. The highlighted portion is the location of the study in the FC-IDS as shown in Fig. 4.

4 DDoS association analysis of hypergraph clustering in fog computing

Section 3 analyzes the threat of DDoS to fog nodes and users. This section discusses the analysis of DDoS under the FC-IDS architecture. Then, based on the hypergraph theory, we model the DDoS of the fog node and use the Apriori algorithm for correlation analysis.

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 $F = \{f_1, f_2, \cdots\cdots, f_n\}$ is a fog cluster composed of fog nodes. There are n fog nodes in the cluster, $i \in [1, n]$. Where f_i represents the ith fog node, and the resources are independent on the fog node.

$$f_i = \{ID_i, B_i, B_{\max i}, P_i, P_{\max i}, H_i, Load_i, fS_i, R_i, R_{\max i}\}$$

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.

$$\text{Load}_i = \sum_{i \in Rmatch} \omega_{match} B_i + \sum_{i \in Rdoing} \omega_{doing} B_i \tag{1}$$

$fS = \{fNormal, fCongestion, fFree, fInvalid\}$ 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 state of the fog node is determined by the load factor ϕ_{Load}.

$$\phi_{Load} = \frac{Load_i}{B_{\max}} \tag{2}$$

It is assumed that$\theta_{Load}$is the resource threshold. fS = *fNormal* when $0 < \phi_{Load} \le \theta_{Load}$=1. fS = *fNormal* when $\phi_{\text{Load}} > \theta_{Load}$. fS = *fFree* when $\phi_{Load} = 0$. fS = *fInvalid* when $\phi_{Load} \gg \theta_{Load}$.

The maximum communication rate of the fog node is characterized as after the user establishes a connection with the fog node.

$$R_{\max i} = B_{\max i} \log_2\left(1 + \frac{P_{\max i} H_i}{N}\right) \tag{3}$$

where $B_{\max i}$ represents the maximum bandwidth reserved by the current fog node; $P_{\max i}$ is the maximum power that the fog node can provide; H_i is the channel gain when the user communicates with the node, and N is noise.

The hyperedge is used to describe the relationship between the fog nodes in this model. It is mined by the Apriori algorithm [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.

1. A set of data sets consisting of node ID is written, which is composed of a priori database of DDoS through the fog node. D
2. The state value of S is traversed in the $f_i = \{ID_i, B_i, B_{\max i}, P_i, P_{\max i}, H_i, Load_i, fS_i, R_i, R_{\max i}\}$ in the dataset, the ID_i of fS_i = $Sunavailable_i$ is pruned and the new dataset D is gotten.

3. The hyperedge (candidate itemsets) E_k with a single ID node is generated, and the support degree of each ID in the dataset D is calculated.
4. The ID combination is eliminated in the hyperedgeE_k and support less than the threshold ψ, and form frequent itemsets L_{k-1} according to the support degree.
5. L_{k-1} connects itself to generate a new hyperedge candidate E_{k+1}. E_{k+1} does not contain the ID combination that has been eliminated in the previous round of finding frequent itemsets, and its support is counted.
6. Iterative operations are repeated, and all the ID combinations which are larger than the threshold ψ are found. The hypergraph $E = \{e_1, e_2, \quad , e_m\}$ is composed of its hypernodes, and the collection of fog nodes contained in each hyperedge is the frequent item of the invader's attack on the fog cluster.

Definition 2 $E = \{e_1, e_2, \cdots\cdots, e_m\}$ is a collection of hyperedges $e_j = \{m_j, W_j\}$, where m_j is the number of nodes included in the hyperedge e_j and W_j 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. Support can be expressed as

$$St_e = \frac{\|e_j\|}{N} \tag{4}$$

N is the number of data entries for the a priori data set. This can be obtained.

$$W_j = \frac{\sum_{v_i \in e_j} R_{\max i}}{m_j} \cdot \frac{\|e_j\|}{N} \tag{5}$$

There is a lot of work that can be done around this model through hypergraph clustering modeling. For example, Max_{W_j} is obtained by comparing W_j 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.

The pseudo code of the algorithm is as follows:

Algorithm 1 Hypergraph clustering algorithm based on the Apriori

```
    L1 =find_frequent_1-itemsets(D);
  For (k=2; L_{k-1} != null;k++){
// Produce a candidate and prune
    C_k =apriori_gen(L_{k-1} );
  // D for candidates counting
    For each t in D {
      C_t =subset(C_k,t); // subset of t
      For each  c ∈ C_t
        c.count++;
    }
    // Return an item set that is not less than
minimum support
    Lk ={c∈C_k | c.count>=min_sup}
}
Return L= All frequent sets;
// First step: join.
Procedure apriori_gen (L_{k-1}: frequent(k-1)-itemsets)
  For each l_1∈L_{k-1}
    For each l_2∈L_{k-1}
      If ((l_1 [1] =l_2 [1]) && (l_1 [2] =l_2 [2])
&& ……&& (l_1 [k-2] =l_2 [k-2]) && (l_1 [k-1] <l_2
[k-1]))
then {
          c = l_1 join to l_2
          if has_infrequent_subset (c, L_{k-1}) then
           delete c;
          else add c to C_k;
          }
       Return C_k;
// Second step: prune.
 Procedure has_infrequent_sub (c:candidate
k-itemset; L_{k-1} :frequent(k-1)-itemsets)
      For each (k-1)-subset s of c
        If s ∉ L_{k-1,} then
          Return true;
        Return false;
```

Table 1 Cooperation set data of the FN that once cooperated

ID	Transcendental cooperation data	Times
1	FN1、FN3、FN4、FN5	2
2	FN1、FN2、FN3	3
3	FN2、FN3、FN5	1
4	FN1、FN4、FN5	1
5	FN3、FN5	2
6	FN1、FN2、FN4	2

Table 2 Simulation parameters

Parameters	Values
Transmission power	30 dBm (FN)
Path loss (macro-eNB)	$L = 35.3 + 37.6 \log(d)$, d = distance in meters
Shadow fading	Log-normal, 8 dB standard deviation(cloud server) and 10 dB standard deviation (FN)
Operating freq. of macro-eNB	2 GHz
Operating freq. of FN	3.5 GHz
System bandwidth for eNBs	5 MHz
Average transmission rate of user demand	10–1000 kbps
Cell layout	Hexagonal grid, 3-sector sites
Maximum allowed time delay	50 ms–5 s

5 The experimental method

In this section, we introduce the aim, design and parameter setting of the simulation experiment. The main purpose of simulation experiment is to verify that our hypergraph clustering model can play a key role in defending against DDoS. We simulate the performance of the system in the wireless fog computing environment when the system is attacked by DDoS. We simulate the radio communication system from the point of legal UE access number and radio resource utilization.

In the simulation environment, we assume that a radio communication system is composed of a cloud server and a plurality of fog nodes (FNs). We give a transcendental cooperation data table in Table 1, and the main parameters for the simulations are shown in Table 2, which consults Ref. [21]. The cloud server is simulated in the Windows 7 operating system (i7-2760QM, 2.4 GHz CPU, 8.00 GB RAM), and the hypergraph clustering model is implemented using Matlab 2014 a.

6 Results and discussion

First, we analyze the performance of fog computing network structure on the access number of legal UE. The two intensities of DDoS are used in the simulation. As shown in Fig. 5, 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. We simulate intruders to attack DDoS with different numbers of devices, so as to simulate the intensity of DDoS attacks. Through the association analysis, we combine the previous intrusion response strategy to simulate the resource utilization of fog nodes.

Figure 6 shows the radio resource utilization in fog computing. With the increase of the UE group size, the

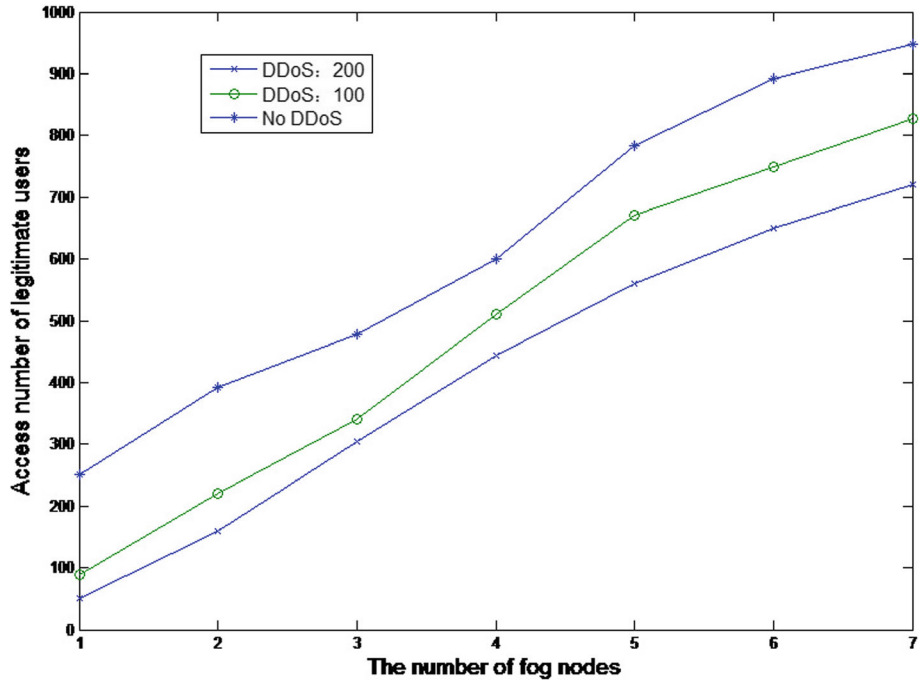

Fig. 5 Maximum number of UE access

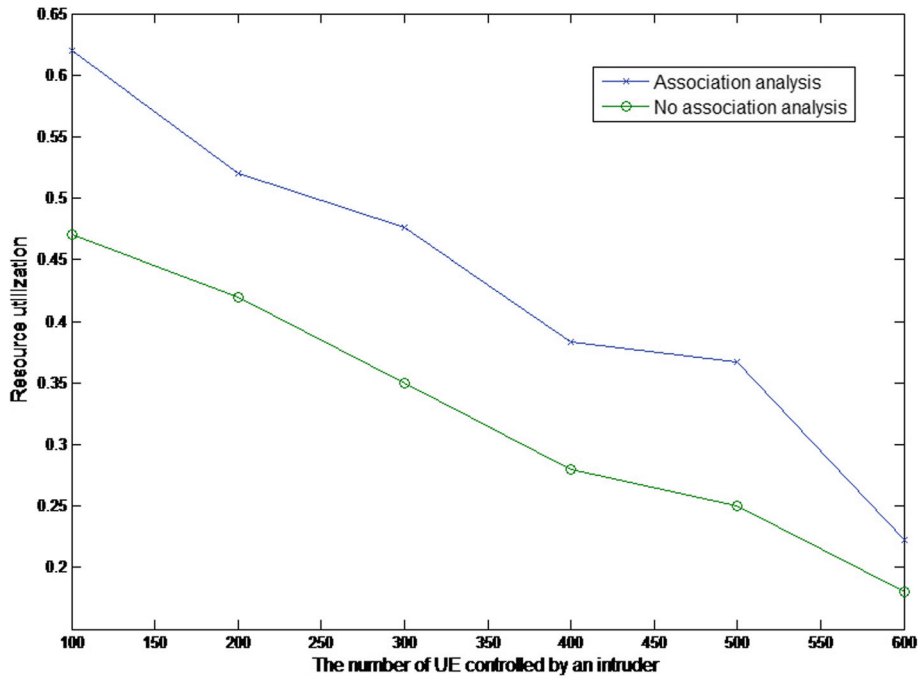

Fig. 6 Ratio of resource utilization

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, we analyze the test data and choose the confidence interval according to the 95% confidence level. In addition, we combine the influence of intrusion response strategy, 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.

7 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. Due to the limited references we have reviewed, the views we have expressed may have limited generalizability. In the future, we will conduct a more detailed study on the defense of DDoS in fog computing.

Abbreviations

DDoS: Distributed denial of service; FC: Fog computing; FC-IDS: Fog computing intrusion detection system; FN: Fog node; IDS: Intrusion detection system; Micro-eNB: Micro Evolved NodeB; UE: User equipment

Acknowledgements

We gratefully acknowledge the anonymous reviewers who read drafts and made many helpful suggestions.

Funding

This work is supported by the National Key R&D Program of China (2017YFC0820700), the Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-17-101), and the Foundation of Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services.

Availability of data and materials

The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Authors' contributions

XA provides ideas for this manuscript and finished writing it. JS contributes to the framework of fog computing and the analysis of DDoS. XL and FL modified the manuscript. All authors read and approved the final manuscript.

Authors' information

Xingshuo An received his master degree from University of Science and Technology Beijing, in 2014. He is currently a PhD student in School of Computer and Communication Engineering, University of Science and Technology Beijing, People's Republic of China. His research direction is fog computing and network security.

Jingtao Su is a PhD student of university of Science and Technology Beijing. His research interests include fog computing and satellite network.

Xing Lü received his PhD degree from Beijing University of Posts and Telecommunications, Beijing, P. R. China, in 2012, in computer science and technology. Now he is a professor in department of Computer and Communication Engineering, University of Science and Technology Beijing, People's Republic of China. China. His research interests include fog computing, soliton theory, symbolic computation and optical soliton communication.
Fuhong Lin, received his M.S. degree and Ph.D. degree from Beijing Jiaotong University, Beijing, People's Republic of China, in 2006 and 2010, respectively, both in electronics engineering. Now, he is an associate professor in the Department of Computer and Communication Engineering, University of Science and Technology Beijing, People's Republic of China. His research interests include edge/fog computing, network security, and big data. He won "Provincial and Ministry Science and Technology Progress Award 2" in 2017. His two papers won "Top 100 most Cited Chinese Papers Published in International Journals" in 2015 and 2016. He served as the co-chair of the first and third IET International Conference on Cyberspace Technology and general chair of the second IET International Conference on Cyberspace Technology. He was the leading editor of the special issue "Recent Advances in Cloud-Aware Mobile Fog Computing" for Wireless Communications and Mobile Computing. Currently, he also serves as a reviewer more than 10 international journals including IEEE Transactions on Industrial Informatics, IEEE Access, Information Sciences, IEEE Internet of Things Journal, The Computer Journal and China Communications. He received the track Best Paper Award from IEEE/ACM ICCAD 2017.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 31 July 2018 Accepted: 10 October 2018
Published online: 22 October 2018

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 w-event 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 Model-Based 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: C-Plane/U-Plane Split and Phantom Cell Concept. *Globecom Workshops (GC Wkshps), IEEE*. (2012)