Journal of Engineering and Applied Sciences 15 (2): 508-515, 2020
ISSN: 1816-949X

Fog Route: Distribution of Data using Delay Tolerant Network

S. Parameswari and K. Kavitha
Department of Computer Science and Engineering, Annamalai University,
608 002 Annamalai Nagar, India

Abstract: Fog computing is an extension of cloud computing. As in cloud computing, fog computing also provides data, compute, storage and application services to end-users. The difference is fog provides proximity to its end users through dense geographical distribution and it also supports mobility. Access points or set-up boxes are used as end devices to host services at the network. These end devices are also termed as edge network. Fog computing improves the Quality of Service(QoS) and also reduces latency. A fog computing system is of a three tier Mobile-Fog-Cloud structure, mobile user gets service from fog servers using local wireless connections and fog servers update their contents from cloud using the cellular or wired networks. This, however, may suffer high content update cost when the bandwidth between the fog and cloud servers is expensive, e.g., using the cellular network and is therefore inefficient for non-urgent, high volume contents. In this study, we address the issue by proposing a hybrid data dissemination framework which applies DTN (Delay Tolerable Network) approaches in fog computing. Here, it is decompose the fog computing network architecture with two planes where the cloud is a control plane to process content update queries and organize data flows and the geometrically distributed fog servers form a data plane to disseminate data among fog servers with delay tolerant network technique.

Key words: Fog computing, delay tolerant network, data dissemination inefficient, tolerant, technique

INTRODUCTION

Fog computing a term created by Cisco that refers to extending cloud computing to the edge of an enterprise's network. Also known as edge computing or fogging, fog computing facilitates the operation of compute, storage and networking services between end devices and cloud computing data centers. While edge computing is typically referred to the location where services are instantiated, fog computing implies distribution of the communication, computation and storage resources and services on or close to devices and systems in the control of end-users. Fog computing is a medium weight and intermediate level of computing power. Rather than a substitute, fog computing often serves as a complement to cloud computing. Fog computing concept, actually a cloud computing close to the 'ground', creates automated response that drives the value. Both cloud and fog provide data, computation, storage and application services to end-users.

However, fog can be distinguished from cloud by its proximity to end-users, the dense geographical distribution and its support for mobility. Fog computing typically has a three-tier mobile-fog-cloud structure (Luan *et al*., 2015). In the mobile tier, it could include all wireless devices such as smartphones, tablets, laptops. In the fog tier, fog servers provide services to the end users and synchronize data with the cloud. In the cloud tier, cloud provider provides content service required by geodistributed fog servers. Data dissemination between a mobile user and a fog server is occurred when this mobile user retrieves content. If this fog server has the required content, it sends the content to the mobile user. Otherwise, this fog server needs to send a query to its cloud provider to find and download it into its local storage. On another side, fog servers need to regularly check with their cloud providers whether the fog servers have the updated contents or not; if not, they need to update their storage by retrieving from the cloud via. either wired or wireless networks, e.g., cellar networks. Such data disseminations may involve a huge cost due to the large data volume. According to the report from Cisco (Stojmenovic and Wen, 2014), the overall mobile data traffic is expected to grow to 24.3 exabytes per month by 2019 and more traffic will be offloaded from cellular networks such as fog devices, than remains on cellular networks by 2016.

Security challenges: In spite of the fact that fog computing can play a central role in delivering a rich portfolio of services more effectively and efficiently to end users, it could impose security and privacy challenges. The major security and privacy challenges in fog computing are summarized below.

Trust model: Trust models based on reputation have been successfully deployed in many scenarios such

Corresponding Author: S. Parameswari, Department of Computer Science and Engineering, Annamalai University,
608 002 Annamalai Nagar, India

asonline social networks. Reputation-based trust model proposed by Cao and Sun (2012) has been successful in e-Commerce, Peer-to-Peer (P2P), user reviews and online social networks.

Research conducted by Lu *et al*. (2010) proposed a robust reputation system for resource selection in P2P networks using a distributed polling algorithm to assess the reliability of a resource beforedownloading. In designing a fog computing reputation-based reputation system, we may need totackle issues such as:

- How to achieve persistent, unique and distinct identity
- How to treat intentional and accidental misbehavior
- How to conduct punishment and redemption of reputation

There are also trusting models based on special hardware such as Secure Element (SE), Trusted Execution Environment (TEE) or Trusted Platform Module (TPM), which can provide trustutility in fog computing applications.

Research conducted by it wassuggested that to design a trust model based on reputation in the IoT, we need to tackle how to maintain the service reliability and prevent accidental failures, handle and identify misbehavior issues, identify malicious behavior correctly and bootstrapbuilding a trust model based on reputation in large-scale networks.

Rogue FOG node: A rogue fog node would be a fog device or fog instance that pretends to be legitimate and coaxesend users to connect to it. For example in an insider attack, a fog administrator may beauthorized to manage fog instances but may instantiate a rogue fog instance rather than alegitimate one. Have demonstrated the feasibility of man-in-the-middle attack in fogcomputing, before which the gateway should be either compromised or replaced by a fake one. Once connected, the adversary can manipulate the incoming and outgoing requests from endusers or fog, collect or tamper user data stealthily and easily launch further attacks.The existenceof fake fog node will be a big threat to user data security and privacy. This problem is hard toaddress in fog computing due to several reasons:

- Complex trust situation calls for different trust management schemes
- Dynamic creating, deleting of virtual machine instance make it hard to maintain ablacklist of rogue nodes

A rogue IoT node has the potential to misuse user's data or provides malicious data toneighboring nodes to disrupt their behaviors. Addressing this problem could be difficult in the IoT due to the complexity in trust management in various schemes. However, a trust measurement-based model could be applied to detect rogue nodes in IoT environment's which canprovide limited security protection.

Authentication: Authentication is an important issue for the security of fog computing since services are offeredto massive-scale end users by front fog nodes. Have considered the main security issue of fogcomputing as the authentication at different levels of fog nodes. Traditional PKI-basedauthentication is not efficient and has poor scalability. Cisco (2014) have proposed a cheap, secure anduser-friendly solution to the authentication problem in local ad-hoc wireless network, relying on aphysical contact for pre-authentication in a location-limited channel.

As the emergence of biometric authentication in mobile computing and fog computing such asfingerprint authentication, face authentication, touch-based or keystroke-based authentication, etc., it will be beneficial to apply biometric-based authentication in fog computing.

Access control: As per Bonomi *et al*. (2012), access control is a security technique to ensure that only authorized entities canaccess a certain resource such as an IoT device or the collected data. In the IoT, we need accesscontrol to make sure that only trusted parties can perform a given action such as accessing IoTdevice data issuing a command to an IoT device or updating IoT device software.

Research conducted by Gao *et al*. (2015), propose a policy-based resource access control in fog computing, tosupport secure collaboration and interoperability between heterogeneous resources. In fog computing how to design access control spanning client-fog-fog at the same time meet thedesigning goals and resource constraints will be challenging.

Intrusion detection: As per Intrusion detection techniques are widely deployed in fog system to mitigate attackssuch as insider attack, flooding attack, port scanning, attacks on VM and hypervisor. In fogcomputing Intrusion Detection System (IDS) can be deployed on fog node system side to detectintrusive behavior by monitoring and analyzing log file, access control policies and user logininformation. They can also be deployed at the fog network side to detect malicious attacks suchas Denial-of-Service (DoS), port scanning, etc. In fog computing, it provides new opportunities toinvestigate how fog computing can help with intrusion detection on both client-side and thecentralized fog side.

Research conducted by a foglet mesh based security framework which can detectionintrusion to distance fog, securing communication among mobile devices, foglet and fog. There are also challenges such as implementing intrusion detection in geo-distributed, large-scale, high mobility fog computing environ men to meet the low-latency requirement.

Literature review: Armbruster *et al*. quantify comparisons between cloud and conventional computing and identify the top technical and non-technical obstacles and opportunities of cloud computing. The emergence of cloud computing has established a trend towards building massive, energy-hungry and geographically distributed Internet data centers as cloud servers.

Due to their enormous energy consumption, Targhetta *et al*. (2014) and Zhuo *et al*. (2013) investigate how to coordinate the collection of data centers so as to minimize the electricity expense while maintaining the quality of the cloud computing service. Our research extends from the existing related papers on cloud computing to a newly emerged paradigm named fog computing. However, the transition is not trivial, since, fog is quite different cloud in terms of location, distribution and computing capability.

Cao and Sun (2012) presented fog computing taxono my in relation to the identified security challenges and its important features. They also reviewed various computing paradigms such as Mobile Edge Computing (MEC), Mobile Cloud Computing (MCC) and edge computing which extensions of cloud are computing. They also presented various security aspects and their challenges.

Khan *et al*. presented a draft copy on applications of fog computing to enable us to identify the common security problems. The ample collection of functionalities obsessed applications in-creases various security issues like data, network virtualization, malware and monitoring. It is also determined on the impact of the security issues and the possible solutions, future directions to im-plement the various solutions for fog system.

Targhetta *et al*. (2014) presented different characteristics and features of fog computing and discussed security and privacy issues such as storage of data, security computation and security of network. They also highlighted the privacy relevant to location, data and user which may face challenges and changes.

Zhuo *et al*. (2013) explored relationship between CPS and IoT and are presented to enhance the existing architectures, enabling the technologies issues of privacy, security and the amalgamation of IoT and fog computing and their applications. It also discussed several applications in fog based IoT environments that also includes the smart grid, smart transportation and smart cities are to be operate in real world environment.

Mithun Mukherjee *et al*. describe an overview of existing security and privacy concerns, their survey highlighted ongoing research efforts, open challenges and research trends security and privacy issues for fog computing.

MATERIALS AND METHODS

Problem description: Radio transmissions are heavily affected by shadowing effects commonly known as obstacle shadowing. Finding a solution for this problem plays an important role in establishing communication between vehicles in urban environments where buildings block radio propagation, as represented in Fig. 1. Assume Vehicle V1 is the sender that needs to broadcast critical messages to nearby Vehicles (receivers) V2-4.

To provide a solution, we divided this problem into three zones to denote Regions (R1-3) as represented in the form of green, yellow and red lines, respectively. Here, the nearby Vehicles V2-4 are located in the transmission range of a base station associated with a sender. The Vehicle V2 is in R1 where the message can be sent directly using a hopping technique, Vehicle V4 is situated in R3 and its radio transmissions are blocked by shadowing in the same region. It leads to a situation where the message is getting dropped in the middle without reaching the destination. The vehicle V3 is in region R2 where the message may be sent directly or may be dropped without reaching the destination (uncertain region) which increase the complexity of the system. To simplify and increase the probability of message delivery we combined the Regions R2 and 3 into a single Region R2 as shown in Fig. 1, to overcome the shadowing effects caused by obstacles like tall buildings in a Manhattan and other downtown regions, we developed a hybrid technique for the successful dissemination of critical messages reliably under these conditions. A detailed explanation of our proposed approach is illustrated in next study.

Proposed solution-hybrid VEHFOG: In a dense urban environment, it is difficult for vehicles in close proximity to reliably establish continuous communication between them due to obstacle shadowing delays and drops caused by intervening tall buildings. To promote continuously reliable communication between the vehicles we developed a hybrid architecture where the critical messages are delivered to the nearby vehicles within the transmission range of a base station sending messages either by using a multi-hop technique or the fog computing, as needed. In our approach, we concentrated only on the vehicles in the transmission region of a base station associated with a sender. Represents the proposed architecture for the dissemination of critical messages in which dissemination of critical messages using the fog computing is illustrated in case 1 and dissemination of critical messages broadcasting using a multi-hop technique is illustrated in case 2.

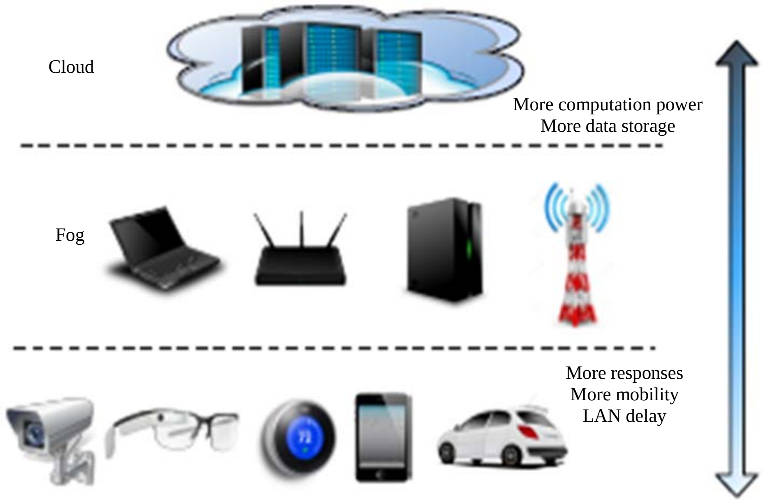

Fig. 1: An example of fog/cloud architecture

Case 1; Dissemination of critical messages using fog computing: In a connected vehicular environment such as VANET, vehicles are highly connected to each other at all times based on V2V and V2I techniques. But when vehicles encounter shadowing regions in dense urban environments, critical messages transmitted among vehicles can be dropped due to intermittent connections resulting from obstacle shadowing from obstacles such as tall buildings. In such cases, fog computing a crucial role in disseminating messages.

Fog layer is located at the edge of a network. It consists of fog nodes which includes access points, gateways, RSUs, base station, etc. In our approach, RSUs and base stations play a major role in disseminating the messages. Fog layer can be static at a fixed location or mobile on moving carriers such as in the vehicular environment. They are responsible for processing the information received from the vehicles and temporarily store it or broadcast over the network. It can be used widely for latency-sensitive applications like broadcasting emergency messages, etc., cloud in fog computing is used to keep track of the resources allocated to each fog node and to manage interaction and interconnection among workloads on a fog layer, popularly known as fog orchestration.

As the vehicles are aware of their locations in relation to the base station, the system deploys and broadcasts the critical messages to the fog layer and when it encounters the obstacle shadowing region. As a result, the messages are disseminated to the vehicles in the shadowing region seamlessly through the fog nodes.

Case 2; Dissemination of critical messages using multi-hop technique: Consider the same situation discussed in case 1 whereas the vehicles can communicate with each other directly using a multi-hop technique which means the vehicles are in non- shadowed regions, allowing communication to be established directly between vehicles. The main advantage of this approach is that vehicles are able to communicate with each other directly without any external technique such as fog computing In this approach, an On-Board Unit (OBU) is used to establish multi-hop communication between the vehicles. When a new vehicle enters the region, critical messages such as hazard alerts, can be delivered to the vehicle based on a multi-hop technique or the fog nodes based on its location.

Analysis of Hybrid-Vehfog: In this analysis, we calculated the power at a receiver end. Analogous to the approaches, we thus conceive our model to be a generic expansion of a well-established shadowing model. In general, it is expressed in the form of Eq. 1:

$$P_r = P_t + G_t + G_r - \sum L_X \tag{1}$$

Where:

P_r : The received power
P_t : The transmitted power
G_t : The antenna gain at the transmitter end
G_r : The antenna gain at the receiver end and
L_X : The loss of effect during transmission

In our system, the major transmission loss is due to obstacle shadowing as formulated in next sub section.

RESULTS AND DISCUSSION

Problem formulation: In this study, we aim to improve the latency of all data flows by balancing workloads among BSs/fog nodes. Considering both the communications latency and computing latency, we denote the latency ratio of the fog network as

$(\eta) = \Sigma_{j\in J}\ \mu_j + \hat{\mu}_j$. Our problem is to optimally associate IoT devices to BSs (i.e., balancing loads among BSs/fognodes) in order to minimize the latency ratio of the fog network. Therefore, the problem can be formulated as follows:

$$\text{P1}: \min_{\eta} L(\eta) \tag{15}$$

$$\text{s.t}\ \sum\nolimits_{j\in J}^{\eta} \eta_j(x) = 1, \forall x \in A \tag{16}$$

$$0 \le \rho_j \le \rho_{max}, \forall_j \in J \tag{17}$$

$$0 \le \hat{\rho}_j \le \hat{\rho}_{max}, \forall_j \in J \tag{18}$$

$$\eta_j(x) \in \{0, 1\}, \forall_x \in A, \forall_j \in J \tag{19}$$

Here, Constraint (Eq. 16) indicates that each location can be associated with only one BS. Constraint (Eq. 17) imposes the traffic load in BS j not to exceed the maximum load threshold of the BS. Constraint (Eq. 18) imposes the computing load in fog node i to be less than the maximum load threshold of the fog node.

In the load balancing process, the traffic load allocation and computing load allocation may affect each other. When the heavy workloads of some BSs are the main constraints of the fog network, the proposed scheme pays more attention on balancing the traffic loads among BSs. As a result, the potential traffic congestions in the overloaded BSs will be mitigated, thus, reducing the latency of data flows. However in the above process, IoT devices are allocated to balance the traffic loads among BSs that may incur the unevencomputing loads among the fog nodes to a certain extent. In contrast when some fog nodes become the bottleneck due to their heavy computing loads, the computing latency becomes the dominating factor of data flow’s latency. Hence, the proposed scheme will focus on balancing the computing loads among fog nodes by adjusting the IoT device associations among BSs. In this case, although, the communications latency may increase owing to the uneven traffic load allocations, the significant reduction of computing latency can still improve the latency of all data flows in the fog network.

LAB; A distributed IoT device association scheme: In this section, we present the LAB scheme where the communications latency in BSs and the computing latency in fog nodes are taken into account simultaneously. The proposed scheme consists of a BS side algorithm and an IoT device side algorithm. The former one iteratively estimates the traffic loads of BSs and the computing loads of fog nodes and then broadcasts them to IoT devices. In the latter algorithm, each IoT device selects the suitable BS based on both the updated advertised load information and its uplink data rates towards different BSs such that the latency ratio of the fog network L (η) is minimized.

The IoT device side algorithm: At the beginning of the k th iteration, all BSs broadcast their estimated traffic loads ρ_j and computing loads $\hat{\rho}_j$ to IoT devices. Based on the definition of L (η), we have:

$$\frac{\partial l(\eta)}{\partial \eta_j(x)} = \lambda(x)\frac{C_j(x)\left(1\text{-}\hat{\rho}_j(k)\right)^2 + r_j(x)\nu(x)\left(1\text{-}\rho_j(k)\right)^2}{C_j l(x)\left(1\text{-}\hat{\rho}_j(k)\right)^2\left(1\text{-}\rho_j(k)\right)^2} \tag{20}$$

Based on the broadcast message, each IoT device can select the suitable BS by:

$$p^k(x) = \arg\max_{j\in J} C_j r_j(x)\phi_j(k) \tag{21}$$

Where:

$$\phi_j(k) = \frac{\left(1\text{-}\hat{\rho}_j(k)\right)^2\left(1\text{-}\rho_j(k)\right)^2}{C_j l(x)\left(1\text{-}\hat{\rho}_j(k)\right)^2 + r_j(x)\nu(x)\left(1\text{-}\rho_j(k)\right)^2} \tag{22}$$

Here, $p^k(x)$ is the index of the BS selected by the user at location x and thus:

$$\eta_j^k(x) = \begin{cases} 1, \text{if } j = p^k(x), \forall_x \in A \\ 0, \text{if } j \ne p^k(x), \forall_x \in A \end{cases}$$

The BS side algorithm: At the side of a BS, it needs to estimate its traffic load and the computing load of its corresponding fog node in each iteration. Thus, it has to estimate an intermediate IoT association $\tilde{\eta}_j^k(x)$ for each IoT device in the iteration. Then, based on the estimated load information among BSs, IoT devices select their BSs/fog nodes by the IoT device sidealgorithm and then the current IoT device association inthe k th iteration becomes $\eta_j^k(x)$. Therefore, based on the intermediate $\tilde{\eta}_j^k(x)$ (estimated by a BS) and the current IoT device association $\eta_j^k(x)$ (decided by IoT devices) in the k thiteration, BS j can estimate the intermediate IoT association $\tilde{\eta}_j^k(x)$ for the IoT device at location in the next iterationas follows:

$$\tilde{\eta}_j^{k+1}(x) = (1-\beta)\eta_j^k(x) + \eta\tilde{\beta}_j^k(x) \tag{23}$$

where, $0\le\beta\le1$ is a system parameter. Consequently with the intermediate IoT device association in iteration k+1, the advertised traffic load of BS j can be estimated as:

$$\rho_j(k+1) = \int_{x\in A}\frac{\lambda(x)l(x)\tilde{\eta}_j^{k+1}(x)}{r_j(x)}dx \tag{24}$$

Similarly, the next advertised computing load of fog node j can be estimated as:

$$\tilde{\rho}_j(k+1) = \int_{x\in A} \frac{\lambda(x)\nu(x)\tilde{\eta}_j^{k+1}(x)}{C_j(x)}dx \tag{25}$$

The detailed procedure of the BS side algorithm is illustrated in Algorithm 1.

Algorithm 1; The BS side algorithm:

```
Input: IoT device's BS selection: $p^k(x)$, $\forall_x \in A$
The intermediate IoT device association vector $\tilde{\eta}^k$ in the kth iteration
Output: The estimated traffic loads of BSs $\rho(k+1)$ and the estimated computing loads of fog nodes $\hat{\rho}(k+1)$ in the (k+1)th iteration
1: Update the intermediate IoT device association for different locations based on: $\tilde{\eta}_j^{k+1}(x) = (1-\beta)\eta_j^k(x) + \beta\tilde{\eta}_j^k(x),\ x \in A,\ j \in J$
2: Calculate $\rho_j(k+1)$ and $\hat{\rho}_j(k+1)$ based on Eq. (24) and (25)
3: Return $\rho(k)$ and $\hat{\rho}(k+1)$
```

As we know, the feasible set of Problem P1 can be expressed as:

$$F = \left\{ \eta/\rho_j = \int_{x\in A} \frac{\lambda(x)l(x)\eta_j(x)}{r_j(x)}dx \right. \tag{26}$$

$$\sum_{j\in J}^{\eta_j}(x) \in \{0,1\}, 0 \le \rho_j \le \rho\max$$
$$\left. \sum_{j\in J}\eta_j(x) = 1,\ \forall_j \in J,\ \forall_x \in A \right\}$$

As $\eta_j(x)\in\{0, 1\}$, F is not a convex set. In order to derive suitable intermediate IoT associations to gradually reduce the average Latency ratio $L(\eta)$ in each iteration, we first relax the constraint to make $0 \le \eta^k \le 1$ and then prove that the traffic load and computing load vectors can finally converge in the feasible set. Then, the relaxed feasible set of Problem P1 can be expressed as:

$$\hat{F} = \left\{ \eta/\rho_j = \int_{x\in A} \frac{\lambda(x)l(x)\eta_j(x)}{r_j(x)}dx \right. \tag{27}$$

$$0 \le \eta_j(x) \le 1,\ 0 \le \rho_j \le \rho_{\max'}$$
$$\left. \sum_{j\in J}\eta_j(x) = 1,\ \forall_j \in J,\ \forall_x \in A \right\}$$

Lemma 1: The relaxed feasible set $\hat{F}$ is a convex set.

Proof: Since, the set includes any convex combination of it is a convex set.

Lemma 2: The objective function $L(\eta)$ is a convex function of η when is defined in $\hat{F}$.

Proof: This lemma can be easily proved by showing that $\nabla^2 L(\eta) > 0$ when η is defined in $\hat{F}$.

Analysis of the algorithm: In this study, we will analyze the convergence and optimality of the LAB scheme in the feasible set of Problem P1.

Lemma 3: When $\tilde{\eta}^{K+1} \ne \tilde{\eta}^k$, $\tilde{\eta}^{K+1}$ provides a descent direction for $L(\tilde{\eta})$ at $\tilde{\eta}^k$.

Proof: As $0 \le \tilde{\eta}_j^k(x) \le 1$, $L(\tilde{\eta})$ is defined in $\hat{F}$ as shown in lemma 2, $L(\tilde{\eta})$ is a convex function of $\tilde{\eta}$ and thus, we need to prove $\left\langle \nabla L(\tilde{\eta}^k),\ \tilde{\eta}^{K+1} - \tilde{\eta}^k \right\rangle < 0$: Thus, we have:

$$\begin{aligned} \left\langle \nabla L(\tilde{\eta}^k),\ \tilde{\eta}^{K+1} - \tilde{\eta}^k \right\rangle &= \int_{x\in A}\sum_{j\in J}\lambda(x)\nu(x)\frac{\tilde{\eta}_j^{k+1}(x) - \tilde{\eta}_j^k(x)}{C_j r_j(x)\phi_j(k)} \\ &= \int_{x\in A}\lambda(x)\nu(x)\sum_{j\in J}\frac{\tilde{\eta}_j^{k+1}(x) - \tilde{\eta}_j^k(x)}{C_j r_j(x)\phi_j(k)} \end{aligned} \tag{28}$$

Based on Eq. 23, we have:

$$\tilde{\eta}_j^{k+1}(x) - \tilde{\eta}_j^k(x) = (1-\beta)\left(\eta_j^k(x) - \tilde{\eta}_j^k(x)\right) \tag{29}$$

As we know:

$$\eta_j^k(x) = \begin{cases} 1, \text{ if } j = p^k(x) \\ 0, \text{ if } j = p^k(x) \end{cases}$$

Owing to the BS selection rule at the user side in the k th iteration, i.e., $p^k(x) = \arg\max_{j\in J} C_j r_j(x)\phi_j(k)$ arg, we can derive:

$$\sum_{j\in J}(1-\beta)\frac{\eta_j^k(x) - \tilde{\eta}_j^k(x)}{C_j r_j(x)\phi_j(k)} \le 0 \tag{30}$$

Since, $\tilde{\eta}^{k+1} \ne \tilde{\eta}^k$:

$$\sum_{j\in J}(1-\beta)\frac{\eta_j^k(x) - \tilde{\eta}_j^k(x)}{C_j r_j(x)\phi_j(k)} < 0 \tag{31}$$

Hence, we have proved $\left\langle \nabla L(\tilde{\eta}^k),\ \tilde{\eta}^{k+1} - \tilde{\eta}^k \right\rangle < 0$

Meanwhile as the LAB scheme is executed iteratively, we will also analyze if the BS selection rule at the IoT device side in each iteration is the best option by proving the following theorem.

Theorem 1: Given the advertised traffic loads of BSs and computing loads of fog nodes, the optimal IoT device association rule at the IoT device side is: $p^k(x) = \arg\max_{j\in J} C_j r_j(x)\phi_j(k)$.

Proof: In the k th iteration, η^k is the IoT device association achieved by the proposed IoT device side algorithm: $p^k(x) = \arg\max_{j\in J} C_j r_j(x)\phi_j(k)$ Meanwhile, let η' denoteany other possible IoT device association vector in the iteration. Thus, to prove this theorem, we just need to prove that_cannot reduce L(η) any more as compared to η^k, i.e., $\left\langle \nabla L\left(\eta^k\right), \eta'\text{-}\eta^k \right\rangle \geq 0$:

$$\left\langle \nabla L\left(\eta^k\right), \eta'\text{-}\eta^k \right\rangle$$

$$= \int_{x\in A} \sum_{j\in J} \lambda(x)\nu(x)\left(\eta_j^{'}(x)\text{-}\eta_j^k(x)\right)\frac{1}{C_j r_j(x)\phi_j(k)}dx \quad (32)$$

$$= \int_{x\in A} \lambda(x)\nu(x)\sum_{j\in J}\left(\eta_j^{'}(x)\text{-}\eta_j^k(x)\right)\frac{1}{C_j r_j(x)\phi_j(k)}dx$$

Since:

$$p^k(x) = \arg\max_{j\in J} C_j r_j(x)\phi_j(k) \quad (33)$$

$$\eta_j^k(x) = \begin{cases} 1, \text{ if } \ j = p^k(x) \\ 0, \text{ if } \ j \neq p^k(x) \end{cases}$$

Then, we have:

$$\sum\nolimits_{j\in J} \eta'_j(x)\frac{1}{C_j r_j(x)\phi_j(k)} \geq \sum\nolimits_{j\in J} \eta_j^k(x)\frac{1}{C_j r_j(x)\phi_j(k)} \quad (34)$$

Hence, $\langle \nabla L(\eta^k), \eta'\text{-}\eta^k \rangle \geq 0$. Therefore, η^k is an optimal IoT device association in the k th iteration. As we know, all BSs will estimate and broadcast the traffic load vector $\hat{\rho}$ and the compuitng load vectord $\hat{\rho}$ iteratively which can be employed by IoT devices to select the suitable BSs. Thus, we need to prove the convergence of ρ and $\hat{\rho}$ for the proposed scheme.

Theorem 2: At the BS side, the estimated traffic load vector and computing load vector converge to the optimal load vectorsd ρ*and $\hat{\rho}^*$ drespectively such that $L(\tilde{\eta})$ is minimized.

Proof: As shown in Lemma 3, $\tilde{\eta}^{k+1}\text{-}\tilde{\eta}^k$ provides a decent direction of $L(\tilde{\eta})$ at $\tilde{\eta}^k$ and hence, $L(\tilde{\eta})$ gradually, decreases in each iteration. Since, $L(\tilde{\eta}) > 0$, $\tilde{\eta}$ will eventually converge when $L(\tilde{\eta})$ is minimized.

According to Eq. 24 and 25, the traffic loads of BSs ρ and the computing loads of fog nodes $\hat{\rho}$ are determined by $\tilde{\eta}$. Thus when the intermediate IoT device association $\tilde{\eta}$ converges, the advertised traffic load vector ρ and computing load vector $\hat{\rho}$ also converge at the same time.

Lemma 4: Based on the optimal advertised traffic load vector and computing load vector $\hat{\rho}$, the IoT device side algorithm yieldsthe optimal IoT device association for the load balancing problemin the feasible set F.

Proof: The proof of this lemma is similar to the proof of theorem 1. As LAB is a gradient algorithm which is a classic algorithm for convex problems, the number of iterations required to ensure convergence can be found by.

CONCLUSION

We have outlined the vision and delayed key characteristics of fog computing, a platform to deliver a rich portfolio of new services and applications at the edge of the network. The motivating examples peppered throughout the discussion range from conceptual visions to existing point solution prototypes. We envision the fog to be a unifying platform, rich enough to deliver this new breed of emerging services and enable the development of new applications future work will expand on the fog computing paradigm in smart grid. In this scenario, two models for fog devices can be developed. Independent fog devices consult directly with the cloud for periodic updates on price and demands while interconnected. Fog devices may consult each other and create coalitions for further enhancements.

REFERENCES

Bonomi, F., R. Milito, J. Zhu and S. Addepalli, 2012. Fog computing and its role in the internet of things. Proceedings of the 1st International MCC Workshop on Mobile Cloud Computing (MCC'12), August 17, 2012, ACM, Helsinki, Finland, pp: 13-16.

Cao, Y. and Z. Sun, 2012. Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges. IEEE. Commun. Surv. Tutorials, 15: 654-677.

Cisco, 2014. Cisco delivers vision of fog computing to accelerate value from billions of connected devices. Cisco Press, Indianapolis, Indiana, USA. https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1334100

Gao, L., S. Yu, T.H. Luan and W. Zhou, 2015. Delay Tolerant Networks. Springer, Berlin, Germany, ISBN: 9783319181080, Pages: 84.

Lu, R., X. Lin, H. Zhu, X. Shen and B. Preiss, 2010. Pi: A practical incentive protocol for delay tolerant networks. IEEE. Trans. Wireless Commun., 9: 1483-1493.

Luan, T.H., L. Gao, Z. Li, Y. Xiang, G. Wei and L. Sun, 2015. Fog computing: Focusing on mobile users at the edge. Networking Internet Archit., Vol. 1, Pentland, A., R. Fletcher and A. Hasson, 2004. DakNet: Rethinking connectivity in developing nations. Computer, 37: 78-83.

Stojmenovic, I. and S. Wen, 2014. The fog computing paradigm: Scenarios and security issues. Proceedings of the 2014 International Federated Conference on Computer Science and Information Systems, September 7-10, 2014, IEEE, Warsaw, Poland, pp: 1-8.

Targhetta, A.D., D.E. Owen and P.V. Gratz, 2014. The design space of ultra-low energy asymmetric cryptography. Proceedings of the 2014 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS'14), March 23-25, 2014, IEEE, Monterey, California, USA., pp: 55-65.

Zhuo, X., W. Gao, G. Cao and S. Hua, 2013. An incentive framework for cellular traffic offloading. IEEE. Trans. Mobile Comput., 13: 541-555.