BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 70(5), 2022, Article number: e142652
DOI: 10.24425/bpasts.2022.142652

Mode selection, caching and physical layer security for fog networks

Rabeea BASIR[1]*, Naveed Ahmad CHUGHTAI[2], Mudassar ALI[2,3], Saad QAISAR[1,4], and Anas HASHMI[4]

[1] School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology, Islamabad, Pakistan
[2] Military College of Signals, National University of Sciences and Technology, Rawalpindi, Pakistan
[3] Telecommunication Engineering Department, University of Engineering and Technology, Taxila
[4] Department of Electrical and Electronic Engineering, University of Jeddah, Jeddah, Saudi Arabia

Abstract. Fog networks facilitate ultra-low latency through the use of data availability near the network edge in fog servers. Existing work in fog networks considers the objective of energy efficiency and low latency for internet-of-things (IoT) for resource allocation. These works provide solutions to energy efficiency and low latency resource allocation problem without consideration of secure communication. This article investigates the benefits of fog architecture from the perspective of three promising technologies namely device-to-device (D2D) communication, caching, and physical layer security. We propose security provisioning followed by mode selection for D2D-assisted fog networks. The secrecy rate maximization problem is formulated first, which belongs to mixed-integer nonlinear programming (MINLP) problem. It is NP-hard, that is why an exhaustive search for finding the solution is complex. Keeping in view the complexity, a nonlinear technique namely outer approximation algorithm (OAA) is applied. OAA is a traditional algorithm, whose results are compared with the proposed heuristic algorithm, namely the security heuristic algorithm (SHA). Performance of the network is observed for the different numbers of eavesdroppers, IoT nodes, and fog nodes.

Key words: IoT; fog networks; secrecy; optimization.

1. INTRODUCTION

In the future, the main requirement of Internet-of-Things (IoT) applications, is low latency and high data transfer with reliability. Fog computing is one of the promising 5G network architectures from which these requirements of low latency and reliable communication can be achieved [1–3]. Fog networks involve the presence of data in the close vicinity of devices which reduces the latency experienced by users. Fog computing as an evolving architecture will support many future smart applications. There are many case studies in different fields such as healthcare, vehicular ad-hoc networks (VANETS), and smart cities where operations are practically done using the benefits of fog computing [4–8].

Cache storage near the users promotes the IoT applications in terms of fewer delays, high data rate, less energy consumption, fewer resource usage, and security. For future 5G and beyond 5G networks, efficient content delivery techniques are required to support all IoT applications. Cache-enabled fog servers can deliver popular content to users with high speed and reliability. The size of cache storage significantly affects the performance of the network in terms of latency. More cached content available in the near vicinity of users results in very fewer delays [9–11].

Device-to-device (D2D) communication in 5G fog networks is a key solution to deal with challenges of spectrum utilization, bandwidth management, and energy consumption. The direct communication between the users results in less delay, as it does not involve offloading from fog servers [12, 13]. As users could get required files from a nearby D2D device, this mode selection will promote less delayed and more reliable communication. Future dense wireless networks which will be composed of an enormous number of smart heterogeneous devices may face high latency and failure in communication by using traditional cryptographic techniques [14]. To keep the confidentiality of messages in the presence of eavesdroppers in the network, physical layer security (PLS) is a new technology that is less complex. PLS does not use the complex management of distribution keys over different layers. The application of PLS is very promising for future IoT networks, it involves the secrecy rate calculation under the consideration of the randomness of wireless networks.

This article provides a resource management scheme for a D2D-assisted fog network in consideration of caching and security. We have assumed a system network in which PLS gives secure communication against an eavesdropper, caching and D2D gives low latency to the users. The organization of this article is as follows. We have built motivation based on the benefits of promising techniques in the introduction part. Then we did a literature review to find the previous researcher's contributions to these technologies. We illustrate mode selection, caching, and PLS in Section 3. Section 4 describes the algorithm used to find

*e-mail: rabeeabasir@gmail.com

Manuscript submitted 2022-02-21, revised 2022-05-30, initially accepted for publication 2022-06-25, published in October 2022.

the solution for the formulated problem. Section 5 represents the simulation results followed by the conclusion.

2. RELATED WORK

Authors in [15] provide numerical results for the comparison of total capacity, secrecy capacity, and wiretap capacity concerning the number of eavesdroppers and the distance between the transmitter and the eavesdropper. The correlation matrix was formed with two 5G radio communication technologies non-orthogonal multiple access (NOMA) and multiple input multiple outputs (MIMO). An experiment is done for both rural and urban areas with consideration of wiretap (less distance between eavesdropper and legitimate receiver) and 5G network (anywhere far distance between eavesdropper and legitimate receiver) channel model. The correlation matrix is formed on channel gains and noise calculation for legitimate receivers and eavesdroppers. Authors in [16] have calculated system performance experimental results and compared them with the theoretical results. They have calculated secrecy capacity for both Amplify-and-Forward (AF) and Decode-and-Forward (DF) protocols. Network performance is examined in terms of secrecy outage probability (SOP) and strictly positive secrecy capacity (SPSC). The authors conclude that for the proposed NOMA-based system model, secure communication depends on channel gains of the relay, strong user, and eavesdropper.

In [17], authors have considered a system model where a primary user (PU) will get confidential information from the satellite and a secondary user (SU) will receive it from the base station (BS) which is surrounded by several eavesdroppers. They have formulated a non-convex optimization problem that maximizes the achievable secrecy rate (ASR) of SU, under constraints of maximum power threshold of BS and maximum interference threshold of the primary user. The secrecy rate is calculated for both coordinated (CE) and un-coordinated eavesdroppers (UE). Two different algorithms were proposed as a solution for both cases. [18] observed two optimization problems which are minimizing the average delay and maximizing the sum data rate of NOMA-enabled Fog Radio Access Networks. To solve the first problem authors have used McCormick and Lagrange relaxation method. The Lagrange partial relaxation method is used to decompose the original problem into three convex subproblems. These decomposed problems were solved using distributed algorithms. The second problem is solved which jointly considers the mode selection, power allocation, and subchannel assignment of fog users (F-UEs) to the fog access points (F-AP).

In [19], authors calculate PLS in terms of secrecy capacity calculation for vehicular networks. The secrecy capacity depends on the bandwidth of the radio side unit (RSU) and vehicular user (VU). They calculated their results in terms of secrecy outage probability, which depends on the VU offloading rate and allocated power, and RSU bandwidth. The relationship between transmit power and offloading rate will affect the value of secrecy outage probability. Afterward, the authors explain the performance affecting parameters that affect the secrecy provisioning in the proposed system. These are delay, computation at radio resources, and secrecy outage cost. Authors have described the benefits of heterogeneous networks with upcoming technologies PLS, caching, and most importantly energy harvesting techniques [20]. The considered network is composed of ultra-dense small cells, massive MIMO, and mmWave technologies. In the first half of the paper, the authors have encouraged the use of PLS, caching, and energy harvesting separately, along with a heterogeneous network. Secrecy rate in comparison with transmission rate is calculated for different densities of base stations.

Energy cost minimization was done in [21] for MEC and D2D networks. Cache-enabled D2D communication is proposed which reduces the energy usage during transmission. To model, the behavior of requests by users, the Markov decision process (MDP) is applied. To deal with the complexity of devices and small base stations Q-learning (QL) and deep Q-network (DQN) algorithms are used, respectively. Cost of energy consumption is calculated for the proposed DQN algorithm, random caching, optimality, and without any user caching. Authors in [22] explain the benefits of fog networks for future distinctive IoT applications. The evolving 5G networks also initiate challenges regarding security, models, and regulations. The proposed system model is composed of legitimate and non-legitimate receivers (IoT nodes) and transmitters (fog nodes) in a static environment. A zero-sum game is formulated between the attacker and the receiver. Q-learning reinforcement technique is proposed to provide PLS for the proposed fog network. This learning algorithm considers the channel state information (CSI) to find parameters named as average time, reliability, false alarm rate (FAR), and average error rate (AER).

Authors have improved the delivery latency using D2D cooperation in the F-RAN which has cache-enabled edge nodes (ENs) in [23]. Under the normalized delivery time (NDT) metric, an optimal strategy is proposed which was based on compress-and-forward D2D communication. To improve the spectrum utilization of cellular networks, D2D communication is a promising technology. In [24], authors formulated a joint mixed-integer nonlinear optimization problem under power and security constraints. Cellular users (CUs) can use cellular links and D2D links simultaneously. The objective is to increase the security in terms of secrecy rate for all the CUs. Downlink secure resource management problem is investigated for both single-channel and multi-channel D2D communications. The proposed algorithms give win-win results for both users using both CU links and D2D links.

In [25], authors have formulated a joint mixed integer programming problem to maximize the secrecy rate under individual power constraints. The proposed model considered is composed of a dual-hop multi-carrier system that has a source node, relay node, destination node, and eavesdropper. The secrecy rate is calculated for the legitimate receiver which is maximized under the power allocation between the source node and relay node, and afterward between the relay node and destination node. The formulated problem is convex and the authors use the duality theorem to find the solution which involves the Karush-Kuhn-Tucker (KKT) optimal conditions. The problem is redefined for the assumption of uniform power allocation at relaying

nodes and source allocation. Extensive simulations are done to provide a sub-optimal solution for the formulated problem using power optimization. [26] proposes a method that is secure and efficient in computation. Using blockchain technology, the D2D-associated fog model is proposed which is decentralized and secure. The proposed method does not require special authentication or any external party for authentication. For mutual authentication for fog devices Ethereum smart contracts are considered. Authors have proposed four algorithms that do initialization, registration, authentication, and location validation phases. Performance metrics for which methodology is studied are cost, time, and minor fees. In [27] authors proposed Fog-

Table 1
Related work contributions

Ref. no.	Mode selection	Security	Caching	Objective	Constraints	Contribution
[15]		☑		Secrecy capacity	Radio frequency (RF) environment	Secrecy capacity is calculated for two radio frequency (RF) environments, urban and rural. Correlation matrices are calculated to see the effects of the number of eavesdroppers and distance in both environments.
[16]		☑		Secrecy capacity		Secrecy capacity is calculated for NOMA-based amplify-and-forward (AF) and decode-and-forward (DF) protocols.
[17]		☑		Max. secrecy rate	power, interference	Maximum achievable secrecy rate is calculated for 5G cellular networks coexisting with satellite networks which is operating on mmWave frequency.
[18]	☑		☑	Min. delay & Max. rate	power, channel allocation	Two problems are solved. To minimize the delay, joint caching placement and association strategy is studied. For maximizing the data rate, joint mode selection and power allocation are studied.
[19]		☑		Max. secrecy outage probability	rate, power	Secrecy rate is calculated for vehicular computation offloading networks. Authors provide a resource management scheme for vehicular users keeping in mind the presence of an eavesdropper.
[20]		☑	☑			A brief survey was written keeping in view the benefits of PLS, caching, and energy harvesting technologies for dense wireless heterogeneous networks.
[21]			☑	Min. energy cost	traffic amount	An RL approach is proposed to cater the energy cost issue in a D2D-assisted cache-enabled MEC network. Energy calculation was done under four different approaches, against different cache hit ratio and user preference.
[22]		☑		Max. utility		PLS is proposed for fog networks to tackle the attack of impersonation. Performance of the network is observed in presence of both non-legitimate transmitter and receiver.
[23]	☑		☑	Min. latency		D2D communication can be used for minimizing the delay which is added during the delivery of content. It can also reduce the fronthaul links traffic by balancing the traffic on links.
[24]	☑	☑		Max. secrecy rate	power, security	PLS is added to cellular networks which are assisted with D2D communication. A secure resource management optimization problem is formulated.
[25]		☑		Max. secrecy rate	power	End-to-end secrecy rate is maximized using a high signal-to-noise ratio (SNR) for relay assisted multi-carrier wireless transmission which uses dual-hop orthogonal frequency division multiplexing (OFDM) power allocation scheme.
[26]		☑		Authentication		Blockchain technology is used which provides all requirements of security namely, data confidentiality, authentication, integrity, and anonymity. The results show that the proposed method is resilient against cyberattacks.
This work	☑	☑	☑	Max. secrecy rate	power, rate & security	A mixed-integer nonlinear secrecy rate maximization problem is formulated for D2D assisted fog network. To find the solution a security heuristic algorithm (SHA) is proposed in comparison with the conventional linearization technique named as an outer approximation algorithm.

Engine solution for IoT applications with on-premises processing capabilities. The solution reduces the size of data, reduces data transmissions, and lowers the cost of cloud usage. Case studies for smart homes and smart monitoring systems are also discussed. In [28] authors review the security drawbacks that are exhibited in Fog communication platforms. Investigation and analysis are carried out on flaws that include access control, authentication, privacy and trust management, evolving threats and attacks, and security audits.

2.1. Contributions

It can be observed that existing works did not jointly consider the physical layer security and mode selection for cache-enabled fog networks. Using conventional security technologies researchers have provided solutions to network security. There is no work to the date where physical layer security, caching and mode selection are done for fog systems. Because of the above research contributions, we pay attention to the presence of eavesdroppers in the D2D-assisted fog network. This security research is still in its early stages. Therefore, in this work, we consider security, caching, and mode selection for the fog network. Moreover, this is the first work that jointly considers resource management and maximizes the secrecy rate that helps in achieving secure communication. The main contributions in this work are:

1. We have modeled a device-to-device (D2D) assisted fog network, which considers two modes of connection.
2. Network security is added in terms of physical layer security for cache-enabled fog networks.
3. A mixed-integer nonlinear optimization problem is formulated with the objective function of maximizing the secrecy rate for IoT nodes. This maximization of the secrecy rate for an IoT node in presence of an eavesdropper enhances secure communication.
4. The constraints of the formulated problem are secrecy rate threshold, power threshold, and association constraint.
5. We have proposed a security heuristic algorithm that first does the mode selection, whichever mode is selected secrecy rate is calculated for the network.
6. The performance of the proposed algorithm is compared with the conventional linearization algorithm outer approximation algorithm. Our proposed algorithm shows better results.

3. FOG SYSTEM ARCHITECTURE

This article considers fog network and D2D communication as shown in Fig. 1. Fog network consists of a cloud server and several fog servers. The cloud server is centralized signaling, computational, and processing unit, directly connected to all fog servers via wired backhaul links. Fog servers are with less storage capacity and processing capability as compared to the cloud server, placed at the near-end of the network. Fog servers have connections among each other to coordinate and share information via dedicated wireless links. Fog servers with cached data and being in close vicinity of users, provide low-latency, more reliable, and high data rate. Proposed system model considers the fog system model considering one cloud server which is responsible for heavy computation and processing to ensure non-stop communication. There is F number of fog servers which serve users based on required QoS measurements. There are two possibilities regarding file downloading, if the requested file is available in the memory of fog server it is directly passed to the user. While non-availability of file requires the file fetching from the far-away cloud server. There is N number of IoT users which can be connected to either fog server or in D2D connection mode. IoT users with high data rates and similar content requests can be served in D2D communication mode.

3.1. Resource allocation model

x_m^n represents the mode selection variable whether user n is in D2D mode or any fog server, where $m \in \mathscr{M} = \{\mathscr{D}, \mathscr{F}_1, \mathscr{F}_2, \mathscr{F}_3, ..., \mathscr{F}_\mathrm{F}\}$. Let there be f number of fog servers such that $f \in \mathscr{F} = \{1, 2, ..., F\}$. There are n number of users $n \in \mathscr{N} = \{1, 2, ..., N\}$, which support 5G IoT application scenario (industrial floor, healthcare, smart city, etc.). The fog servers are equipped with a limited storage capacity which can store S_f bits of popular data. Let $p_\mathscr{D}^n$ and $p_{\mathscr{F}_\mathrm{F}}^n$ be the power allocated to user n while connected in D2D mode or any fog server $\mathscr{F}_\mathrm{F}$ respectively. Channel gains in both modes $m = \{\mathscr{D}, \mathscr{F}\}$ denoted by $h_\mathscr{D}^n$ and $f_{\mathscr{F}_\mathrm{F}}^n$ with antenna gains of G_o and H_o respectively are given as follows:

$$h_\mathscr{D}^n = h_\mathscr{D}^{\tilde{n}} \xi G_o \left(\frac{d_o}{d_\mathscr{D}}\right)^\alpha, \tag{1}$$

$$f_{\mathscr{F}_\mathrm{F}}^n = f_{\mathscr{F}_\mathrm{F}}^{\tilde{n}} \xi H_o \left(\frac{d_o}{d_{\mathscr{F}_\mathrm{F}}^n}\right)^\alpha, \tag{2}$$

where $h_\mathscr{D}^{\tilde{n}}$ and $f_{\mathscr{F}_\mathrm{F}}^{\tilde{n}}$ are Rayleigh random variables for D2D and fog mode connection. ξ gives the value of lognormal shadowing and d_o represents the reference distance from far field antenna. Distances of user in both modes are given as $d_\mathscr{D}$ and $d_{\mathscr{F}_\mathrm{F}}$. α is the path loss constant. The $C_\mathscr{D}^n$ and $C_\mathscr{F}^n$ are the channel capacity of n-th user in D2D pair and in fog mode, respectively. The possible data rate in these two modes can be calculated using the following equations:

$$C_\mathscr{D}^n(p_\mathscr{D}^n) = \log_2\left(1 + \frac{p_\mathscr{D}^n h_\mathscr{D}^n}{N_o}\right), \qquad \forall n \in \mathscr{N}, \tag{3}$$

$$C_\mathscr{F}^n(p_{\mathscr{F}_\mathrm{F}}^n) = \log_2\left(1 + \frac{p_{\mathscr{F}_\mathrm{F}}^n f_{\mathscr{F}_\mathrm{F}}^n}{N_o}\right), \quad \forall n \in \mathscr{N}, f \in \mathscr{F}, \tag{4}$$

where channel noise suffered by the signal is given as N_o.

3.2. Secrecy rate calculation model

Secrecy rate is separately calculated for all users in both connection modes, i.e., fog mode and D2D pair communication mode. After the mode selection, we consider the physical layer security problem in the orthogonal frequency domain multiple access (OFDMA) based fog network which consists of multiple users, multiple fog servers, and an eavesdropper. We assume that channel state information for all users is known to the fog server and transmitter in a D2D mode pair. The eavesdropper is

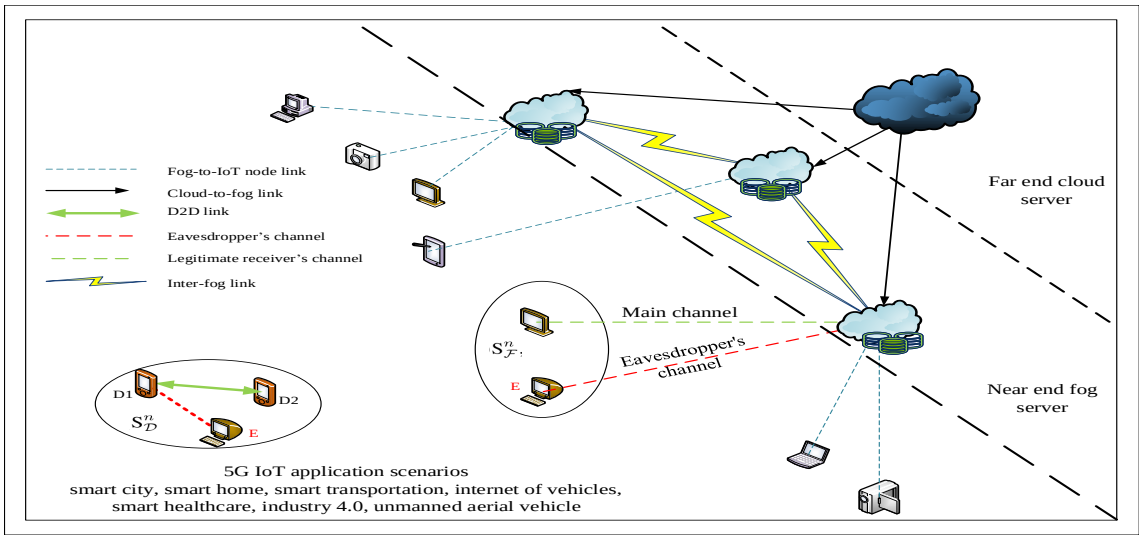

Fig. 1. Fog D2D-assisted system model

in close vicinity of the user and being passive targets the information of all the nearby users. Let us assume an eavesdropper e is trying to steal information from user n which is legitimate receiver as shown in the figure. Physical layer security can be added by maximizing the user's secrecy rate. Secrecy rate of a user can be calculated by the difference of channel capacities of user and eavesdropper. (4) and (5) give the received channel capacity of user n in downlink transmission for both modes of communication. For calculating the channel data rate received by eavesdropper e, let us assume that the channel gain is given as:

$$g^e = \tilde{g^e}\,\xi K_o \left(\frac{d_o}{d^e}\right)^{\alpha}, \tag{5}$$

where d^e is the distance of eavesdropper e, K_o is the antenna gain, $\tilde{g^e}$ is the Rayleigh random variable and ξ is the lognormal shadowing. The data rate received by eavesdropper using above equation can be given as:

$$C^e(p^e) = \log_2\left(1+\frac{p^e g^e}{N_o}\right). \tag{6}$$

To calculate secrecy rate, fog node must know the perfect knowledge about signal-to-noise ratios of user n and eavesdropper e. The secrecy capacity in fog mode of connection can be expressed as [29]:

$$\mathrm{S}^n_{\mathscr{F}}(p^n_{\mathscr{F}_\mathrm{F}}, p^e) = C^n_{\mathscr{F}}(p^n_{\mathscr{F}_\mathrm{F}}) - C^e(p^e), \tag{7}$$

$$\mathrm{S}^n_{\mathscr{F}}(p^n_{\mathscr{F}_\mathrm{F}}, p^e) = \log_2\left(1+\frac{p^n_{\mathscr{F}_\mathrm{F}} f^n_{\mathscr{F}_\mathrm{F}}}{N_o}\right) - \log_2\left(1+\frac{p^e g^e}{N_o}\right). \tag{8}$$

Similarly, the secrecy rate calculation for a user in D2D mode of connection is given as:

$$\mathrm{S}^n_{\mathscr{D}}(p^n_{\mathscr{D}}, p^e) = C^n_{\mathscr{D}}(p^n_{\mathscr{D}}) - C^e(p^e), \tag{9}$$

$$\mathrm{S}^n_{\mathscr{D}}(p^n_{\mathscr{D}}, p^e) = \log_2\left(1+\frac{p^n_{\mathscr{D}} h^n_{\mathscr{D}}}{N_o}\right) - \log_2\left(1+\frac{p^e g^e}{N_o}\right). \tag{10}$$

Using (7)–(10), the total network secrecy rate can be calculated as:

$$\mathrm{S}(p^n_{\mathscr{F}_\mathrm{F}}, p_{\mathscr{D}}{}^n) = x^n_m \mathrm{S}^n_{\mathscr{D}}(p^n_{\mathscr{D}}, p^e) + (1-x^n_m)\mathrm{S}^n_{\mathscr{F}}(p^n_{\mathscr{F}_\mathrm{F}}, p^e). \tag{11}$$

In (11), the mode selection is given as: $x^n_m \in [0,1]\ \ \forall n \in \mathscr{N}, m \in \mathscr{M}$. If an n user gets the requested file from a near-by D2D user, then x^n_m will be equal to 1. If fog mode is selected then $x^n_m = 0$, only second factor of equation will be counted for calculation of secrecy data rate. Table 2 shows all symbols and parameter descriptions used in this article.

3.3. Problem formulation

Considering the factors of mode selection, caching, and physical layer security, our aim is to maximize the network secrecy rate. The maximization optimization problem under QoS (power, rate and security) constraints can be written as:

$$\mathscr{U}_{(x^n_m, p_{\mathscr{F}_\mathrm{F}}, p_{\mathscr{D}})} = \max \sum_{n\in\mathscr{N}} \sum_{m\in\mathscr{M}} \mathrm{S}(p^n_{\mathscr{F}_\mathrm{F}}, p_{\mathscr{D}}{}^n)$$

subject to following constraints:

$$\begin{aligned}
&\mathrm{C1}: \quad \sum_{m\in\mathscr{M}} x^n_m \le 1 \qquad \forall n \in \mathscr{N},\\
&\mathrm{C2}: \quad \mathrm{S}(p^n_{\mathscr{F}_\mathrm{F}}, p_{\mathscr{D}}{}^n) \ge \theta^n_{min} \quad \forall n \in \mathscr{N},\\
&\mathrm{C3}: \quad x^n_m p^n_{\mathscr{D}} \le P_{\mathscr{D}} \qquad \forall n \in \mathscr{N}\\
&\mathrm{C4}: \quad \sum_{n\in\mathscr{N}} p^n_{\mathscr{F}_F} \le P^{max}_{\mathscr{F}_F} \qquad \forall f \in \mathscr{F},\\
&\mathrm{C5}: \quad p^n_{\mathscr{D}} \ge 0,\ p^n_{\mathscr{F}_F} \ge 0 \qquad \forall n \in \mathscr{N}.
\end{aligned} \tag{12}$$

The objective function in (12) is sum-secrecy rate maximization while satisfying constraints C1 to C5. Constraint C1 ensures the association of a user in only one mode, i.e. $m = \{\mathscr{D}, \mathscr{F}\}$. Constraint C2 ensures the security of each IoT node in a fog mode of connection, $\theta^n_{\min} \ge 0$ is the minimum secrecy rate for node n. Constraints C3 and C4 are power constraints for D2D

and fog mode, respectively. In the case of D2D communication, C3 ensures that the power experienced by D2D should be less than the maximum threshold power $P_{\mathscr{D}}$. C4 ensures that the total power allocated to all users at fog $\mathscr{F}_F$ must be within the total available power $P^{\max}_{\mathscr{F}_F}$. Constraint C5 shows the non-negative power constraint.

Table 2
Fog network parameters description

Symbol	Description
N	Total number of users
F	Total number of fog servers
$p^n_{\mathscr{F}_\mathrm{F}}$	Downlink power of n-th user in fog mode
$p^n_{\mathscr{D}}$	Downlink power of n-th user in D2D mode
$P^{\max}_{\mathscr{F}_\mathrm{F}}$	Maximum power of a fog node
$P_{\mathscr{D}}$	Minimum threshold power for D2D mode
p^e	Downlink power of e-th eavesdropper
$\theta^n_{\min}$	Minimum secrecy rate requirement for a user
$h^n_{\mathscr{D}}$	Channel gain of n-th user in D2D mode
$f^n_{\mathscr{F}_\mathrm{F}}$	Channel gain of n-th user in F fog mode
g^e	Channel gain of e-th eavesdropper
G_o	Antenna gain for n-th user in D2D mode
H_o	Antenna gain for n-th user in F fog mode
K_o	Antenna gain for e-th eavesdropper
d_o	Reference distance
$d_{\mathscr{D}}$	Distance of n-th user from D2D transmitter
$d^n_{\mathscr{F}_\mathrm{F}}$	Distance of n-th user from F fog transmitter
d^e	Distance of e-th eavesdropper
$h^{\tilde{n}}_{\mathscr{D}}$	Rayleigh random variable of n-th user in D2D mode
$f^{\tilde{n}}_{\mathscr{F}_\mathrm{F}}$	Rayleigh random variable of n-th user in F fog mode
$f^{\tilde{n}}_{\mathscr{F}_\mathrm{F}}$	Rayleigh random variable of n-th user in F fog mode
$g^{\tilde{e}}_{\mathscr{F}_\mathrm{F}}$	Rayleigh random variable of e-th eavesdropper
ξ	Zero mean Guassian random variable
α	Path loss constant
N_o	Channel noise suffered by the signal

4. PROPOSED ALGORITHMS

The mathematical model in (11) is solved using the outer approximation algorithm (OAA) followed by a heuristic approach. OAA is a conventional optimization algorithm while a heuristic algorithm is developed on basis of the best SNR. The work is carried out in terms of performance analysis of the network under QoS factors.

4.1. Outer approximation algorithm

The formulated problem is NP-hard and belongs to MINLP class. It is a complex problem as it is composed of all types of variables (binary, continuous, and integer). The exhaustive search algorithm (ESA) can not be used to find the optimal solution because of the problem nature, i.e, complex and challenging. The complexity of ESA increases exponentially as the number of nodes in the system increases. Search space for ESA of finding the solution will be given as $2^{|n+f|}$, this means the algorithm has to solve $2^{|n+f|}$ optimization problems. This complexity analysis brings the use of OAA [30] to solve the problem. Algorithm 1 explained the pseudo-code of OAA.

OAA works on the principle of decomposition method in which a problem is decomposed into non-linear programming (NLP) sub-problems and mixed-integer programming (MILP) master problem. Four propositions are satisfied by the objective problem. To study these, let us consider $\digamma$ to be the objective and Δ_{C1-C5} to be the set of constraints of (12), $\rho = \{p_{\mathscr{D}}, p_{\mathscr{F}_F}\}$ and $\mathscr{X} = x \cup \rho$. The propositions are as follows:

- ρ is nonempty, compact, and convex in nature. For fix value of $\mathscr{X}$, the objective function $\digamma$ and constraints set Δ_{C1-C5} are convex in ρ.
- Objective function $\digamma$ and constraints set Δ_{C1-C5} are differentiable.
- Fixing $\mathscr{X}$, the NLP problem can be solved.
- Fixing $\mathscr{X}$, at the solution of each NL continuous subproblem, constraint qualification holds.

4.2. Security heuristic algorithm

This is a mode selection strategy, where n-th user gets requested files either in D2D mode or fog mode. Mode selection is based on keeping the maximum secrecy rate. Algorithm 2 explained the pseudo-code of SHA.

In the initial stage, first, the requested files are determined whether they are available in D2D mode or not. If not then fog mode is selected, for which $F \times N$ channel matrix is generated. Calculate the *SNR* using the second factor of (4) and the fog node with the maximum *SNR* determined for downlink transmission. Power is assigned to fog node f, and the data rate is calculated using (4).

4.3. Complexities of algorithms

Complexities of algorithms are calculated in this section. To find an optimal solution to a problem, the maximum required number of iterations gives the complexity of the algorithm. It is determined by the number of flops $\mathscr{F}$ count, which is given as a real floating point. [31] gives the quantitative intuition of flops for every operation. One flop is added for addition, multiplication division, assignment, and logical operations, and two and four flops are added for complex addition and complex multiplication operations, respectively. One flop is added when an element is added or subtracted from the set. $2abc$ flops are added on matrix multiplication of two matrices having dimensions of $a \times b$ and $b \times c$. Using this, the complexities of OAA and SHA can be calculated as $\mathscr{F}_{OAA}$ and $\mathscr{F}_{SHA}$.

$\mathscr{F}_{OAA}$ On basis of pseudo-code of OAA from statements 1 to 5, one flop is calculated, for 6th statement $2NF$ flops are added, for each 7th and 8th statement $4NF\delta$ flops are added, for 9th statement $2NF\delta$ flops are added, for 10th and 13th statements two flops are added, and for 11th statement, one flop is added. While δ is the constraint

count for the formulated problem.

$$\begin{aligned}\mathscr{F}_{OAA} &= 5+2NF+4NF\delta+4NF\delta \\ &\quad + 2NF\delta+1+3, \\ \mathscr{F}_{OAA} &\approx 2NF+10NF\delta.\end{aligned} \tag{13}$$

$\mathscr{F}_{SHA}$ As there are two modes involved, for both modes the complexities are calculated as:
For *fog mode:* For statements 4 and 5, 2 flops are added; for statement 6, NF flops are added, for statement 7, $N(N+2)$ flops are added. 2N flops are added for statement 8; N and F flops are added for statements 9 and 10, respectively. N and $N(N+5)$ flops are added for statements 11 and 12, respectively. For statement 15, FE flops are added and for statement 16, $E(E+2)$ flops are added. 2 flops are added for (11). (14) gives the numerical value for the complexity of SHA.

$$\begin{aligned}\mathscr{F}_{SHA} &= 2+NF+N(N+2)+2N+N+F+N \\ &\quad + N(N+5)+FE+E(E+2)+2, \\ \mathscr{F}_{SHA} &\approx 3F+12N+2N^2+FN+FE+E^2+3E, \\ \mathscr{F}_{SHA} &\approx 12N+2N^2+F(3+N+E)+E(E+3).\end{aligned} \tag{14}$$

For *D2D mode:* N(N+2) flops are added for statement 18, DE flops are added for statement 19. For statement 20, $E(E+2)$ flops are added. 2 flops are added for (11). It is given mathematically in (15).

$$\begin{aligned}\mathscr{F}_{SHA} &= N(N+2)+DE+E(E+2)+2, \\ \mathscr{F}_{SHA} &\approx 12N+2N^2+DN+DE+E^2+3E, \\ \mathscr{F}_{SHA} &\approx 12N+2N^2+D(N+E)+E(E+3).\end{aligned} \tag{15}$$

Algorithm 1. Outer approximation algorithm

1: i $\leftarrow$ 1
2: Initialize $\mathscr{X}^i$
3: $\varepsilon \leftarrow 10^{-3}$
4:*Convergence* $\leftarrow$ *FALSE*
5:**While** *Convergence* == *FALSE* **do**
6: $\rho^i \leftarrow \begin{cases} arg\,min, & -F(\mathscr{X}^i,\rho); \\ subject\,to, & \Delta_{C1-C5}(\mathscr{X}^i,\rho)\leq 0 \end{cases}$
7: $Upper\_Bound \leftarrow F(\mathscr{X}^i,\rho^*)$
8: $(\mathscr{X}^*,\rho^*,\chi^*) \leftarrow \begin{cases} \underset{\mathscr{X},\rho,\chi}{arg\,min}\,\chi, \\ subject\,to, \\ \chi \geq -F(\mathscr{X}^i,\rho^i), \\ -\nabla F(\mathscr{X}^i,\rho^i)\binom{\rho-\rho^i}{0}, \\ \Delta_{C1-C5}(\mathscr{X}^i,\rho^i), \\ -\nabla\Delta_{C1-C5}(\mathscr{X}^i,\rho^i)\binom{\rho-\rho^i}{0}\leq 0 \end{cases}$
9: $Lower\_Bound \leftarrow \chi$
10: **if** $Upper\_Bound - Lower\_Bound \leq \varepsilon$ **then**
11: *Convergence* $\leftarrow$ *TRUE*
12: **else**
13: $i \leftarrow i+1$
14: $\mathscr{X}^i \leftarrow \mathscr{X}^*$
15: **end_if**
16: **end_while**

Algorithm 2 : Security Heuristic Algorithm

1: **The objective function**
2: first mode is selected and then total network secrecy rate is calculated based on the following steps.
3: **if** fog mode is selected (best fog node selection)
4: initialize the number of fog nodes with F.
5: initialize the number of IoT nodes with N.
6: create channel matrix by $F \times N$.
7: calculate *SNR*.
8: find fog node f having maximum SNR with node n in downlink transmission $[SNR_{\max}, Loc] = arg\ max_{f\in\mathscr{F},n\in\mathscr{N}}\ SNR$.
9: **for** $f \in \{1,...,F\}$ **do**
10 : **for** $n \in \{1,...,N\}$ **do**
11: in downlink node n associates with fog *F (1,n) Loc*.
12: assign power to fog *F (1,n) Loc* associated with node n in downlink and calculate data rate using (4).
13: **end for**.
14: **end for**.
15: find the data rate of eavesdropper e which is in close vicinity of node n and tried to steal the information, using (6).
16: calculate the secrecy rate using (7) and (8).
17: **else** D2D mode (more secure, operate at low power).
18: calculate the data rate using (3).
19: find the data rate of eavesdropper e which is in close vicinity of node n and tried to steal the information, using (6).
20: calculate the secrecy rate using (9) and (10).
21: put the values in (11).

5. SYSTEM PERFORMANCE

The system's performance is seen in this section for the proposed SHA algorithm in comparison with the conventional optimization technique OAA. OAA is implemented using Basic open source nonlinear mixed integer programming (BONMIN) software [32]. Performance is observed for parameters namely; mode selection, rate, and the number of resources.

5.1. Simulation parameters

The assumed system parameters are summarized in Table 3. For simulations, the minimum number of 10 and the maximum number of 80 users are taken. Four fog servers are assumed in the system for all results except one Fig. 6, where we observe the impact of the number of fog servers. The maximum power for fog nodes and D2D pair is set to 41 dBm and 35 dBm respectively. According to the antenna far-field, the reference distance is assumed as 20m. Antenna gain is 50, path loss exponent is 2, while zero-mean Gaussian random variable for shadowing is 10 dB. One eavesdropper is assumed for simulation results except in Fig. 5, where 14 eavesdroppers are taken to observe

the network performance. The minimum secrecy rate required by a user has been assumed as {500,1000,2000} kbps.

Table 3
System parameters [29, 33, 34]

Parameter	Value
Min. users	10
Max. users	80
User increment	10
Fog servers	4
$P_{\mathscr{F}_F}^{\max}$	41 dBm
$P_{\mathscr{D}}$	35 dBm
d_o	20 m
α	2
$\theta_{\min}^{n}$	{500,1000,2000} kbps
H_o	50
ζ	10 dB
e	1

5.2. Results and discussions

In Fig. 2, mode selection is shown against the number of users in the system. Users get attached to either D2D mode or any fog server depending upon the maximum secrecy rate calculation subject to the rate and power constraints. It can be seen that more users are selected in fog mode as compared to the D2D mode. D2D mode is selected less because of the lover availability of requested files in the nearby devices. Based on the best channel, the user gets associated with a particular fog node. The best channel is measured based on the maximum secrecy rate calculation. If a user does not satisfy all the constraints, then that user does not contribute to the secrecy rate calculation. This mode selection is a random choice because it considers all five constraints.

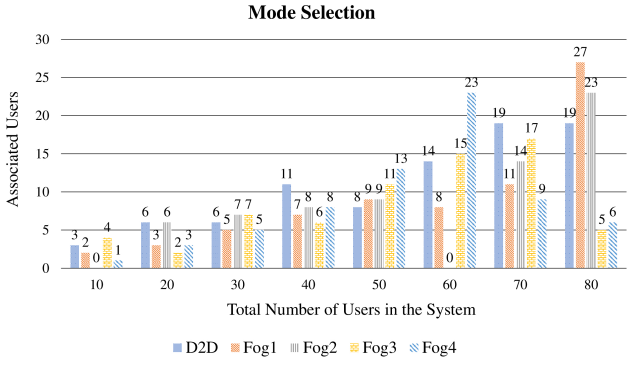

Fig. 2. Mode selection against number of users

The secrecy rate of the system is plotted against the total number of users {10-80} in Fig. 3. The total network secrecy rate is calculated considering all the constraints of (12). The performance of the network is observed under SHA and OAA

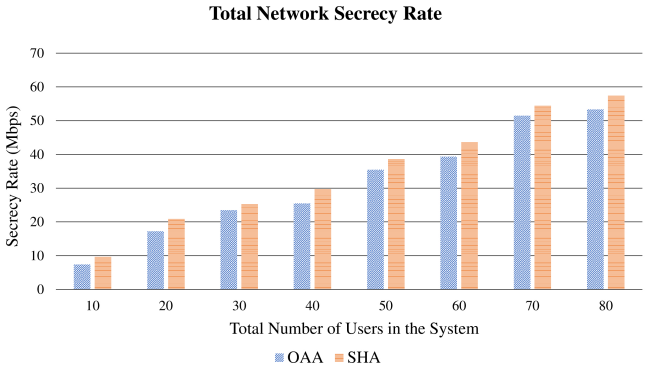

Fig. 3. System secrecy rate against number of users

algorithms. The graph shows that with the increase in the number of users in the system, the secrecy rate is increasing. More amount rate is generated when there are more users present in the network. The percentage increase in secrecy rate calculation is 86.19% and 83.19% for OAA and SHA respectively, when users are increased from 10 to 80. For the same simulation parameters, the proposed algorithm gives better results than the conventional OAA linearization algorithm. When there are 10 and 80 users in the system the percentage increase in secrecy calculation is 30.86% and 7.49% for OAA and SHA, respectively. More users in the system affect the rate of production and it would be difficult to keep secure communication. This fact is proved by the percentage increase calculation of both algorithms.

In Fig. 4, for the minimum required user rate of 500 kbps, 1000 kbps, and 2000 kbps, the secrecy rate of the system is calculated against the number of users in the system. With the increase in QoS rate requirement, the secrecy rate of the network is decreased. This is due to the fact of maintaining the rate requirement of the users so that they received more secure data. As the rate required for a user gets high, there is more power allocation to users so that the user association gets maximized. This fact can also be observed in this simulation result. A user is rejected by the system if the rate requirement is not satisfied.

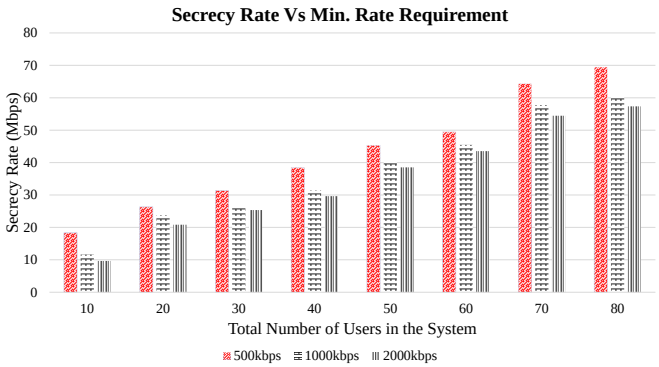

Fig. 4. System secrecy rate against minimum required user rate

The impact of the number of eavesdroppers in the system against rate calculation is seen in Fig. 5. The total rate depend-

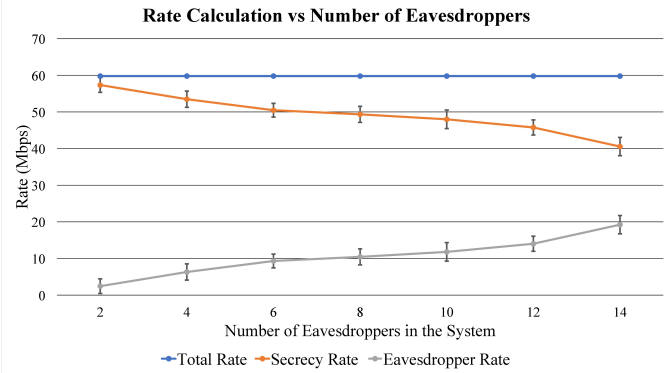

Fig. 5. System rate calculation against number of eavesdropper

ing upon the system capacity is constant. It is obvious that with the increase in the eavesdropper in the system, more data will be stolen. We can see the decline in the secrecy rate against an increase in the eavesdropper's rate from the graph. The graph shows average data rate results with standard deviation as confidence bars. For Figs. 2–5 results, four fog servers are considered in the system.

Similarly, the impact of the number of fog servers {4-20} on the secrecy rate can be observed in Fig. 6. The general secrecy rate increasing trend against the number of fog servers in the system can be seen. This is due to the availability of more resources, more fog servers ensure more data production. More number of fog nodes present in the system ensures more secrecy provisioning. For this simulation result, only two eavesdroppers are considered in the system. Performance of the network under the different number of fog servers is observed for both algorithms, and SHA shows better results. For the simulation results of Figs. 5 and 6, we kept 80 users that required a minimum rate of 500 kbps.

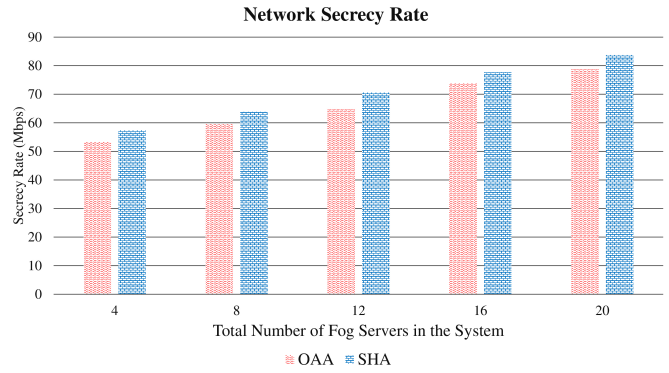

Fig. 6. System rate calculation against number of fog servers

6. CONCLUSION

In this article, for D2D-assisted fog network users, the physical layer security is enhanced. An MINLP maximization problem is formulated that maximizes the secrecy rate of a D2D-assisted fog network under constraints of QoS requirements. A conventional optimization algorithm, OAA has been used in comparison with a heuristic approach named SHA. Simulation results show that SHA has significantly improved the security of the proposed fog network. The performance of algorithms shows that the proposed algorithm gives better results as compared to the conventional solver. The impact of resources has also been observed in the simulation results.

REFERENCES

[1] S. Parveen, P. Singh, and D. Arora, "Fog computing research opportunities and challenges: A comprehensive survey," in *Proceedings of First International Conference on Computing, Communications, and Cyber-Security (IC4S 2019)*. Springer, 2020, pp. 171–181.

[2] C. Zhang, "Design and application of fog computing and internet of things service platform for smart city," *Future Generation Comput. Syst.*, vol. 112, pp. 630–640, 2020.

[3] R. Basir, S. Qaisar, M. Ali, M. Aldwairi, M. I. Ashraf, A. Mahmood, and M. Gidlund, "Fog computing enabling industrial internet of things: State-of-the-art and research challenges," *Sensors*, vol. 19, no. 21, p. 4807, 2019.

[4] L. Mora, R. Bolici, and M. Deakin, "The first two decades of smart-city research: A bibliometric analysis," *J. Urban Technol.*, vol. 24, no. 1, pp. 3–27, 2017.

[5] M. Luthra, B. Koldehofe, and R. Steinmetz, "Transitions for increased flexibility in fog computing: A case study on complex event processing," *Informatik Spektrum*, vol. 42, no. 4, pp. 244–255, 2019.

[6] N.K. Giang, R. Lea, and V.C. Leung, "Developing applications in large scale, dynamic fog computing: A case study," *Software, Pract. Experience*, vol. 50, no. 5, pp. 519–532, 2020.

[7] B. Tang, Z. Chen, G. Hefferman, T. Wei, H. He, and Q. Yang, "A hierarchical distributed fog computing architecture for big data analysis in smart cities," in *Proceedings of the ASE BigData & SocialInformatics 2015*, 2015, pp. 1–6.

[8] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in *Proceedings of the 2014 IEEE 15th international conference on information reuse and integration (IEEE IRI 2014)*. IEEE, 2014, pp. 16–23.

[9] M.S. ElBamby, M. Bennis, W. Saad, and M. Latva-Aho, "Content-aware user clustering and caching in wireless small cell networks," in *2014 11th International Symposium on Wireless Communications Systems (ISWCS)*. IEEE, 2014, pp. 945–949.

[10] B. Ma, W. Guo, and J. Zhang, "A survey of online data-driven proactive 5g network optimisation using machine learning," *IEEE Access*, vol. 8, pp. 35 606–35 637, 2020.

[11] M.C. Gursoy, C. Zhong, and S. Velipasalar, *Deep Multi-Agent Reinforcement Learning for Cooperative Edge Caching*. John Wiley & Sons, Ltd, 2020, ch. 21, pp. 439–457.

[12] M. Sun, X. Xu, X. Tao, and P. Zhang, "Large-scale user-assisted multi-task online offloading for latency reduction in d2d-enabled heterogeneous networks," *IEEE Trans. Network Sci. Eng.*, vol. 7, no. 4, pp. 2456–2467, 2020.

[13] O. Khalid, I.A. Khan, R.N.B. Rais, and A.W. Malik, "An insight into 5g networks with fog computing," *Fog Comput., Theory Pract.*, pp. 505–527, 2020.

[14] Y. Zhu, L. Wang, K.-K. Wong, and R.W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, 2017.

[15] K. Xiao, S. Zhang, and Y. He, "On the secrecy capacity of 5g new radio networks," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018.

[16] J. Chen, L. Yang, and M.-S. Alouini, "Physical layer security for cooperative noma systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4645–4649, 2018.

[17] Z. Lin, M. Lin, J.-B. Wang, Y. Huang, and W.-P. Zhu, "Robust secure beamforming for 5g cellular networks coexisting with satellite networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 932–945, 2018.

[18] R. Rai, H. Zhu, and J. Wang, "Performance analysis of noma enabled fog radio access networks," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 382–397, 2020.

[19] Y. Wu, L.P. Qian, H. Mao, X. Yang, H. Zhou, X. Tan, and D.H. Tsang, "Secrecy-driven resource management for vehicular computation offloading networks," *IEEE Network*, vol. 32, no. 3, pp. 84–91, 2018.

[20] L. Wang, K.-K. Wong, S. Jin, G. Zheng, and R.W. Heath, "A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 49–55, 2018.

[21] J. Tang, H. Tang, X. Zhang, K. Cumanan, G. Chen, K.-K. Wong, and J.A. Chambers, "Energy minimization in d2d-assisted cache-enabled internet of things: A deep reinforcement learning approach," *IEEE Trans. Ind. Inf.*, vol. 16, no. 8, pp. 5412–5423, 2019.

[22] S. Tu, M. Waqas, S.U. Rehman, M. Aamir, O.U. Rehman, Z. Jianbiao, and C.-C. Chang, "Security in fog computing: A novel technique to tackle an impersonation attack," *IEEE Access*, vol. 6, pp. 74 993–75 001, 2018.

[23] R. Karasik, O. Simeone, and S.S. Shitz, "How much can d2d communication reduce content delivery latency in fog networks with edge caching?" *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2308–2323, 2019.

[24] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, 2018.

[25] W. Aman, G.A.S. Sidhu, H.M. Furqan, and Z. Ali, "Enhancing physical layer security in af relay–assisted multicarrier wireless transmission," *Trans. Emerging Telecommun. Technol.*, vol. 29, no. 6, p. e3289, 2018.

[26] A.A.-N. Patwary, A. Fu, S.K. Battula, R.K. Naha, S. Garg, and A. Mahanti, "Fogauthchain: A secure location-based authentication scheme in fog computing environments using blockchain," *Comput. Commun.*, vol. 162, pp. 212–224, 2020.

[27] F. Mehdipour, B. Javadi, A. Mahanti, G. Ramirez-Prado, and E. Principles, "Fog computing realization for big data analytics," *Fog Edge Comput., Principles Paradigms*, vol. 1, pp. 259–290, 2019.

[28] A.A.-N. Patwary *et al.*, "Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control," *Electronics*, vol. 10, no. 10, p. 1171, 2021.

[29] F. Irrum, M. Ali, M. Naeem, A. Anpalagan, S. Qaisar, and F. Qamar, "D2d-enabled resource management in secrecy-ensured 5g and beyond heterogeneous networks," *Phys. Commun.*, vol. 45, p. 101275, 2021.

[30] M.A. Duran and I.E. Grossmann, "An outer-approximation algorithm for a class of mixed-integer nonlinear programs," *Math. Program.*, vol. 36, no. 3, pp. 307–339, 1986.

[31] G. Golub and C. Van Loan, *Matrix computations*, 3rd ed. Baltimore: JHU Press, 2012.

[32] P. Bonami, "Basic Open-Source Nonlinear Mixed Integer Programming," [Online] http://www.coin-or.org/Bonmin/, Accessed on Nov. 18, 2020.

[33] M.S. Elbamby, M. Bennis, W. Saad, M. Latva-Aho, and C.S. Hong, "Proactive edge computing in fog networks with latency and reliability guarantees," *EURASIP J Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–13, 2018.

[34] R. Basir, S. Qaisar, M. Ali, and M. Naeem, "Cloudlet selection in cache-enabled fog networks for latency sensitive iot applications," *IEEE Access*, vol. 9, pp. 93 224–93 236, 2021.