Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.022480
Article

Tech Science Press

Enhanced Reliability in Network Function Virtualization by Hybrid Hexagon-Cost Efficient Algorithm

D. Jeyakumar* **and C. Rajabhushanam**

Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, 600126, India
*Corresponding Author: D. Jeyakumar. Email: jeyakumarjk789@gmail.com
Received: 09 August 2021; Accepted: 01 December 2021

Abstract: In this,communication world, the Network Function Virtualization concept is utilized for many businesses, small services to virtualize the network node function and to build a block that may connect the chain, communication services. Mainly, Virtualized Network Function Forwarding Graph (VNF-FG) has been used to define the connection between the VNF and to give the best end-to-end services. In the existing method, VNF mapping and backup VNF were proposed but there was no profit and reliability improvement of the backup and mapping of the primary VNF. As a consequence, this paper offers a Hybrid Hexagon-Cost Efficient algorithm for determining the best VNF among multiple VNF and backing up the best VNF, lowering backup costs while increasing dependability. The VNF is chosen based on the highest cost-aware important measure (CIM) rate, which is used to assess the relevance of the VNF forwarding graph.To achieve optimal cost-efficiency, VNF with the maximum CIM is selected. After the selection process, updating is processed by three steps which include one backup VNF from one SFC, two backup VNF from one Service Function Chain (SFC),and two backup VNF from different SFC. Finally, this proposed method is compared with CERA, MinCost, MaxRbyInr based on backup cost, number of used PN nodes, SFC request utility, and latency. The simulation result shows that the proposed method cuts down the backup cost and computation time by 57% and 45% compared with the CER scheme and improves the cost-efficiency. As a result, this proposed system achieves less backup cost, high reliability, and low time consumption which can improve the Virtualized Network Function operation.

Keywords: Network function virtualized (NFV); hybrid hexagon-cost efficient algorithm (HH-CE); cost-aware important measure (CIM); reliability; network services

1 Introduction

NFV is contrasting with, conventional server-virtualization strategies, such as those utilized in venture IT. A VNF may comprise one or more virtual machines running distinctive programs and forms, switches, and capacity gadgets. It is also used in custom hardware appliances in the network infrastructure to grow the IT visualization technologies. What's more is, NFV enables the elasticity and scalability of the system

by decoupling the NFV function (identity provider (IDP), In building solution (IBS)) from their infrastructures. These network functions are utilized for a low price and more alert product hardware. In addition, the stylization of network and SFC concerns more attraction to the future network structures which give more reliability and flexibility. The expenditure and initial amount of these networks are very low hence it gains more benefit to the organization where the virtualization concept is used. Apart from the utilization of VNF, when compared to traditional network properties, VNF failure causes more damage to the network. In expansion, as the benefit of subscribers is within the frame of SFC comprising of efficient associated VNFs, the dependability of end-to-end benefit isn't calculated by a solitary module hence it needs full equipment to analyze the function. To increase the reliability of VNF, the sufficient backup chosen is important. A Series of studies have been done to clarify the reliability trickily. In the previous approach, two steps are followed to solve the problem simultaneously where the first step is the selection process and the next is the mapping process.

NFV framework is a virtualization structure where hardware and software are used to perform the network function through VNF is conveyed. The Network functions virtualization foundation can span a few areas. Organizing a giving network between these areas is considered a portion of the NFV foundation. To manage the NFV, the NFV-MANO [Network functions virtualization - management and orchestration] architecture framework is used which consists of a collection of functional block data, data depositories utilized by these blocks, reference data, and transferring information to organize the NFV-MANO framework and VNF's.

Many, NFV structures are deliberately used for end-to-end communication over the network channel with more reliability. In the modern world, the need for NFV is automatically increased exponentially to build a virtualized network to perform the services required for various organizations. The increased number of network users, automation traffic car control,and the number of growing network structures lead to flow the traffic in the network services. Hence the application of network services is required to operate on any scalable, flexible, dynamic channel. In the existing method, VNF mapping and VNF backup are proposed but there is no profit and reliability improvement for the backup and mapping of the primary VNF.The main objective of the proposed HH-CE methodology is to select the best VNF among the previously updated VNF to get maximum cost-efficiency in the selection process. The full paper is systematized as followed: Section 2 gives information regarding NVF and SFC request and the topology model is explained in Section 3. The proposed methodology and experimental setup are described in Sections 4 and 5. The result and discussion are demonstrated in Section 6. Finally, the conclusion part is explained in Section 7.

2 Related Works

Many, NFV structures are deliberately used for end-to-end communication over the network channel with more reliability. Hence the enforcement is considered as a security for the VNF network. To drop the packet in the communication path, path filters are mostly used which depends on the source address, destination address, source IP protocol, etc. In addition, filter known as a packet filter is used for the default action with the help of its prioritized order [1]. For any kind of application layer filter, the behavior should be known for which it needs to clarify data. For this purpose, the control fall is utilized and the decision is made. Based on the decision, the classification function determines the communication stateful information and different types of protocols.

In this digitized world, several network functions are utilized in many places such as conferences, network traffic detection, video calling, satellite communication, etc. These are based on the Multicasting fundamental where multicasting request is used to request the service chain in multicasting; it provides secure and reliable service. The throughput of the multicasting NFV in the SDN is increased by reducing

the cost of the implemented multicast request in the network function [2]. Ordinary IT security need has increased exponentially but the requirement of cot and scalability creates a great challenge in IT. In [3], the security of the smart device is achieved through network edge detection in the smart environment. From, the network edge detection scheme, the importance of NFV is determined. The entire model of the NETRA structure has achieved security through the IoT service interns of throughput, delay, memory, storage [4]. Mainly, the NVF and SDN are deployed to change the shape of the landscape in IoT security. If any threats are created in the IoT, the features of the NVF can be easily detected and locate the threats, and also can react towards the threats [5].

NFV can reshape the landscape of the security system in IoT. Such kind of security is introduced by the SDN which can be able to monitor, protect and react to the system [6]. Some conflicts are created when the network function hasa different resource with more restrictions. These kinds of conflicts are identified by the paramount before sending the NVF request to the embedded algorithm to avoid the unwanted behavior execution time. To check this conflict, the NV checker is used in the NVF environment which uses an ontology as Onto-NFV [7].

In many NVF/SDN, open systems are used to manage and orchestrate the networks. This kind of framework is utilized for programming systems to obtain a low-level particularity within the equipment machines that give the IT assets. Open-source optimization program activates the offline arranging, online provisioning, and organization of SDN/NFV systems [8].

Recently, VNF scheduling and implanting are researched to create the VN service in SDN/NVF network. This VNF embedding and schedules are created by mixed ILP having the objectives of lessening the expended basic assets and providing QoS-guaranteed VN benefit. In the same way, Energetic VNF implanting, and planning calculation is utilized to evacuate the NP-hardness of the MILP show [9].

The facilitated network checking is utilized for conveying the best-of-breed out of NFV frameworks whereas which voyages towards completely customized checking arrangements. The arrangement of observing sinks and the sending of network checking activity permits finer-grained network advisers with constrained overheads [10]. Virtualization controlling and monitoring are utilized in SDN/NFV network to get a coordinated network service. The CPS time of SDN is decreased by the Lifetime extension scheme. To coordinate the asset powerfully and productively, SDN and moment arrangement with NFV is exploited to switch the topology of hub styles of a CPS. Decision control topology is created by clustering the run time CPS [11].

The manufactured approach is based on the investigation of both network preparing strategies and user practices. A viable client behavior show is examined over 20TB genuine information from an administrator. Inactive client conduct demonstrates are received by gear manufacturers' stack test methods [12]. Each NVF node can access both calculating and transmission resources using the dominant resource processor which can give resource allocation and resource utilization. At the NVF node, the M/D/1 model is used to compute the packet delay and flow rate for each data flows in the transmission [13]. To progress the reliability in NVF, a very important method known as the redundancy effective method is planned in [14–17]. With the help of his redundancy effective technique, reliability estimation is achieved for the network services. For the further improvement of CIM, the VNF FG is involved to calculate the IM measurement; finally, the importance of VNF FG is obtained [18–20].

3 Topology Model

The network topology, reliability measurement, and problem definition of Virtual Network Function (VNF) are explained in this section. The reliability measurement mathematical equation and PN junction nodes are also briefly described [21–23].

3.1 Network Model

The network topology consists of Physical Network (PN) and nodes which are represented as G_{PN} (O, P). Where O and P represent the traditional PN nodes and links between the PN nodes respectively. The reliability of PN nodes is estimated by the notion of r_n which is determined by the MTBF. The capacity of the PN node is denoted as c_n for Virtual Network Function (VNF).

The total request from the subscribers is demonstrated as Q = {q j |j ∈ J}, where q_j is (F_j, Req_j). F_j, Req_j denotes the set of stands for the reliability requirement and VNFs reliability requirement. To determine the number of SFC requests, one formula is used, where the number of requests from the subscribers is denoted as Q. The formula is expressed as

$$\mathrm{Q} = \{q_j|\mathrm{j} \in \mathrm{J}\} \tag{1}$$

Hence the number of SFC requests is calculated and each SFC has two or more VNFs.

$$q_j = \left(F_j, Req_j\right) \tag{2}$$

F_j *and* Req_j denotes the set of reliability requirements, VNFs required reliability. In this paper, VNF FG topology is represented as G_{FG} (T, E), where T and D stand for the placement of the VNF set and virtual link respectively. For all kinds of VNF, VNF t ∈ T is connected with resource demand d_t.

3.2 Measuring the Reliability

The reliability measurement is an important factor in network function. Whenever the network creates a virtual network function for a particular service, the reliability of the network gets worst,and further, the performance is degraded exponentially. Hence in this paper, hardware fault is considered to determine the reliability. Mainly, the reliability of the network is determined based on the complexity which may be created by software or Hardware. In this paper, the reliability r_t of VNF is measured based on the PN node it operates on. And also, some backup processes are done in this paper. Hence decision binary variable x_n^t is expressed as:

$$x_n^t = \begin{cases} 1 & \text{if } VNF_t \text{ is instantiated on } n \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

And $\Delta_t \rightarrow$ Maximum number of VNF after the redundancy process.

$$\Delta_t = \left(1 - (1 - \tilde{r}_t) \prod_{n \in N} \left(1 - x_n^t r_n\right)\right) - \tilde{r}_t \qquad \text{for } t\varepsilon T \tag{4}$$

VNFs may be connected to serial or parallel to determine the reliability of the end-end services which is shown in Fig. 1. The disappointment of each PN node occurs autonomously hence the reliability calculation is shown in the below section.

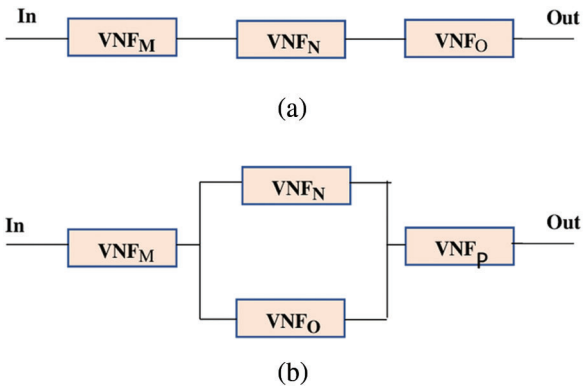

Figure 1: Reliability measurement of serial and parallel VNFS connection. (a) rSerial = rA. rB. rC (b) rParallel = rM. rNUO. rP

3.3 Problem Definition

The mapping of the primary VNF is not efficient to meet the requirement of reliability while backup typically works for no profit for an extended period. Hence this paper considers the cost efficiency as a parameter to expand the consistency of the VNF by dismissal back-up. Meanwhile, the redundancy problem in this paper is explained. In the topology, mapped SFC requests for some VNF backup. To select the VNF cost-efficient, each VNF should take the responsibility of maximum CIM value VNF backup with the optimized algorithm. Hence maximum cost efficiency is expressed as,

$$\eta = \underset{x_n^t, \Delta}{max} \frac{\Delta Reliability}{Backup\ cost} \tag{5}$$

Reliability requirement of each SFC request,

$$\text{s.t} r_j(\tilde{r} + \Delta) \quad \geq Req_j \qquad for\ j \varepsilon J \tag{6}$$

The capacity limitation of each SFC request is given as,

$$\sum_{t \varepsilon T} x_n^t d_t \leq \quad for\ t \varepsilon T, n \varepsilon N \tag{7}$$

From Eq. (5), the global optimal number of backs up will be determined

$$x_n^t \in \{0, 1\} \tag{8}$$

To solve the redundancy problem in this paper, two steps are followed, the first one is the selection model, and the second is the updated model.

4 Proposed Methodology

In this section, two techniques are proposed for the selection and updating of VNF in the Virtualized Network Function (VNF) framework which is shown in Fig. 2. The first is, VNF selection based on the HH-CE algorithm, the second technique is updating proper backup VNF for the required SFC request. To select the VNF backup, the Cost Importance Measure (CIM) factor is used which should have a higher value.

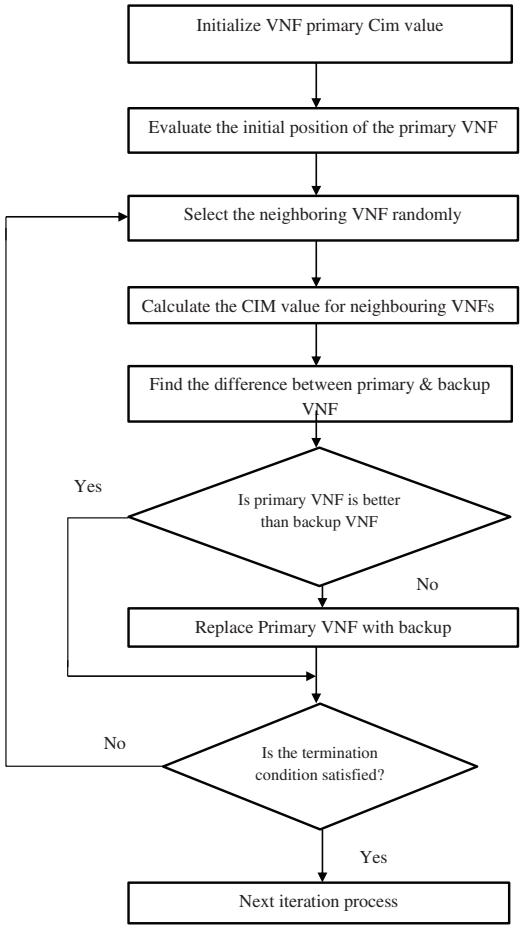

Figure 2: Flow chart of the proposed methodology

4.1 Proposed Hybrid Hexagon-Cost Efficient (HH-CE) Based VNF Selection

The main aim of the proposed HH-CE methodology is to select the best VNF among the previous updated VNF to get maximum cost-efficiency in the selection process. For this reason, compute the CIM value for each VNFs in the SFC request VNF, from the computed CIM, the best VNF is selected. The maximization function is considered the best backup VNF function. The evaluation is done by two conditions.1) Compare the primary VNF (CIM value initialized) with backup VNF (CIM value of updated VNF) and 2) if the present VNF is greater than primary VNF, then assign current VNF as the new best VNF. The process will continue until the last iteration is reached. There are four steps involved in the calculation of the best backup VNF. Initialization, training phase, update phase, stop criteria are explained in the below section.

4.1.1 Training Phase

The training phase means taking off the VNFs from the SFC request. The Network function virtualization attempts to expand the learning of VNF to calculate the CIM value and to make the SFC request to get extraordinary reliability. Let M_j^i be the network function of the VNF and the CIM calculation of the SFC request in subjects given by,

$$CIM_t = \frac{\sum_{j\&J} IM_j^t}{\lambda_t} \tag{9}$$

where, $x_n^t \rightarrow$ decision binary variable which is given in Eq. (1); $d_t \rightarrow$ resource demand at each SFC request; $\Delta_t \rightarrow$ increment of VNF; $M_j^t \rightarrow$ VNF function for each SFC request. The feasible solutions are upgraded by moving their situations towards the situation of the best attainable arrangement by thinking about the present CIM calculation. All the recognized feasible VNF are preserved and it is given to the updated model of the backup VNF.

4.1.2 Comparison Phase

Here, the VNF forwarding graph gains information through shared correspondence. A VNF1 (V_1) discovers some information from other VNF (V_2) of the SFC request if V_2 has more knowledge than V_1. Thusly, if V_2 is superior to V_1, then V_1 is moved towards V_2. Otherwise, V_1 is stimulated far from V_2. The learning rationality of this stage is recreated as beneath:

Two VNFs are haphazardly chosen from the one SFC request, where V_1, V_2 are the two arbitrary numbers of VNFs and $V_1 \neq V_2$.

If

$$F\left(X_{V_1}^i\right) > F\left(X_V^i\right) \tag{10}$$

$$X_{new\ Vp,\ V_1,j}^i = X_{V_1,j}^i + r\left(X_{V_1,j}^i - X_{V_2,j}^i\right) \tag{11}$$

Else

$$X_{new\ Vp,\ V_1,j}^i = X_{V_1,j}^i + r\left(X_{V_2,j}^i - X_{V,j}^i\right) \tag{12}$$

End

Where F(X) is a fitness function. After the evaluation of fitness function, the best solution can be obtained by using the below conditions,

If

$$F\left(X_{new\ Vp,V_1}^i\right) > F\left(X_{new,V_1}^i\right)$$

$$X_{new,V_1}^i = X_{new\ Vp,V_1}^i$$

Else

$$X_{new,V_1}^i = X_{new\ ,V_1}^i$$

End

Where, X_{new,V_1}^i represents the best VNF backup. The HH-CE algorithm has the following steps,

Step 1: The number of VNF present in the SFC request, primary VNF, the termination conditions are initialized.

The VNF function for every SFC request is estimated using Eq. (13) which is expressed as,

$$M_j^t(k) = \left(m_i^1(k), m_i^2(k), \ldots, m_i^d(k), \ldots, m_i^n(k)\right), \quad i = 1, 2, \ldots, N. \tag{13}$$

Consider X (t) = (x_1, x_2, x_3, …, x_n),

Let consider t = Time,

Where {x_1, x_2,…, x_n} are VNFs position.

Step 2: Evaluate the initial position of the primary VNF and generate the neighboring VNFs randomly.

Step 3: [Training Phase] After the primary VNF initialization, find the best backup VNF among the randomly generated VNF and find the mean difference between the first VNF and best VNF using CIM calculation. This CIM is calculated for all neighboring VNF.

Step 4: [Comparison Phase]: If the backup VNF frame is better than the current VNF frame, then replace the current VNF with the best VNF backup.

Step 5: The algorithm stops its execution if the most extreme number of iterations is accomplished and the solution which is holding the maximum CIM VNF is optimal. The HH-CE algorithm is shown in Fig. 3.

Algorithm: Hybrid Hexagon-Cost Efficient Reliability Model

Input: $G_{PN}(N,L)$, $G_{PN}(T,E)$, Q = $\{q_j \mid j \in J\}$, $\{r_n \mid n \in N\}$, $M_j^t(k) = \left(m_i^1(k), m_i^2(k), \ldots, m_i^d(k), \ldots, m_i^n(k)\right)$, $i = 1,2,\ldots,N$.

Output: The redundancy plan $\{x_n^t \mid t \in T, n \in N\}$

Initialize the primary VNF, the iteration termination

Evaluate the initial position of the primary VNF and generate the neighbouring VNFs randomly

Calculate the CIM value for all VNF $CIM_t = \frac{\sum_{j\epsilon j} IM_j^t}{\lambda_t}$

x_n^t →decision binary variable which is given in the (1) equation;
d_t →resource demand at each SFC request; Δ_t→increment of VNF; M_j^t → VNF function for each SFC request

If $F(X_{V_1}^i) > F(X_V^i)$

$X_{new\ Vp,V_1,j}^i = X_{V_1,j}^i + r(X_{V_1,j}^i - X_{V_2,j}^i)$

else

$X_{new\ Vp,V_1,j}^i = X_{V_1,j}^i + r(X_{V_2,j}^i - X_{V,j}^i)$

end

Select the VNF t_i with maximum CIM and placed it on PN node n_i (based on the selection model).

Generate a Generate a new forwarding graph $G_{FG}^{'}$ by removing the VNFs of the accepted SFC requests from G_{FG}

If $n_i \in N$ **then**

$x_{n_i}^{t_i}$=1

$t^{'}$ ← Generate a new VNF by consolidating the primary VNFs and backups using update model

Calculate the reliability r_j |j ∈ J of each SFC;

end

While r_j<Req_j, for ∀j ∈ J **do**

Update r_i, r_i for t∈T, j∈J

end

If (number of iterations=reached)

Stop

Else

Continue the process from second step

end

Figure 3: Proposed hybrid hexagon-cost efficient (HH-CE) algorithm

Theorem 1: This theorem proves that the maximum CIM of VNF will lead to improve reliability which can give maximum cost efficiency. Hence selecting the VNF is accomplished in this paper using the HH-CE algorithm.

Proof: The cost-efficiency of the backup VNF is analyzed using the CIM equation which is demonstrated in terms of the IM equation. The CER equation is expressed as,

$$\text{CER} = \frac{\sum_{j\epsilon j}\left(r_j(\bar{r}+\Delta) - r_j(\bar{r})\right)}{\sum_{t\in T}\lambda_t\Delta_t} = \frac{\sum_{t\in T}\sum_{j\in J} IM_j^t\Delta_t}{\sum_{t\in T}\lambda_t\Delta_t} \tag{14}$$

By using partial disproportion, the final result of the CER,

$$\text{CER} = \frac{\sum_{t\in T}\sum_{j\in J} IM_j^t \Delta_t}{\sum_{t\in T} \lambda_t \Delta_t} \leq \max_t \frac{\sum_{j\in J} IM_j^t}{\lambda_t} \tag{15}$$

The final optimal cost efficiency is

$$CER^* = maxCIM_t$$

The importance of the CIM is shown in the VNF FG of the multi SFCs request. The defeat of VNFs will create a world-spread administrations blackout, which isn't worthy of arranging administrators and endorsers. Other than, since the assets distributed for these reinforcements may not make as much profit as the essential VNF, the use for the repetition is anticipated to be as small as possible.

In the proposed method, the HH-CE algorithm is used to select the best CIM value. According to the value, the maximum CIM backup is selected for the selection process. Based on the selection, the next update process is accomplished. In the conclusion, the proposed algorithm improves reliability and cost-efficiency exponentially.

4.2 Update Model

When the selection of the best backup VNF completes, the upgrade of the essential VNFs will be processed. Some limits are allowed to place the backup, two VNF are permitted to occupy the same PN code. Hence the resource is utilized by sharing the backup between two PN nodes. And also, more backup won't create more reliability hence this shared resource will give a better development. Permitting two reinforcements set on the same PN hub is suitable. After the new possible backup is chosen, the placement of VNF in the SFC is done. The first one is, holding VNF in one SFC after embedding the VNF in the SFC structure. To keep pace with the calculation these primary and backup VNFs are considered as a new VNF in the next SFC which is shown in Fig. 4a.

The reliability of the new VNF is

$$r_{N'} = 1 - (1 - r_O)(1 - r_{N_O}) \tag{16}$$

Similarly, for the second one, one SFCholds two VNFs after embedding the VNF in the SFC structure. To be mentioned above, The CIM calculation of primary and backup VNFs is considered as a new VNF for the next SFC iteration which is shown in Fig. 4a. The reliability of the new VNF is

$$r_E = 1 - (1 - r_{N_O})(1 - r_N r_O) \tag{17}$$

The third procedure, which holds two VNF from two different SFCs, is a different model compared with the previous two models. The two VNFs are considered as the next VNF in the SFC iteration which is shown in Fig. 4b. Most importantly, the two SFCs use the same PN node hence the operating expenses are reduced which is shown in Fig. 4b. The performance of measuring the reliability is gotten by considering the backup and primary VNFs in the VNF forwarding graph.

5 Experimental Setups

The experiment setup is conducted in the network link. The physical network and SFC requests are explained below. In this paper, Physical Network uses 116 node network maps. For each physical network, 2000 units are utilized which offers different resources for VNFs to utilize and progress the data. The reliability of each node is set randomly between 0.9 and 0.99. SFC request contains more than two VNFs in the series VNFs structure. Hence the reliability requirement of each network function is defined. For example, the Google apps reliability requirement of each SFC is chosen among the

following reliability values [0.95, 0.98, 0.99, 0.995 and 0.999]. Normally, VNF-FG has 10 primary VNF instances and 1–30 resources which are located in the PN to apply 1100 SFC requests. The superiority of the proposed method is compared with the previous heuristic algorithm and CER algorithm.

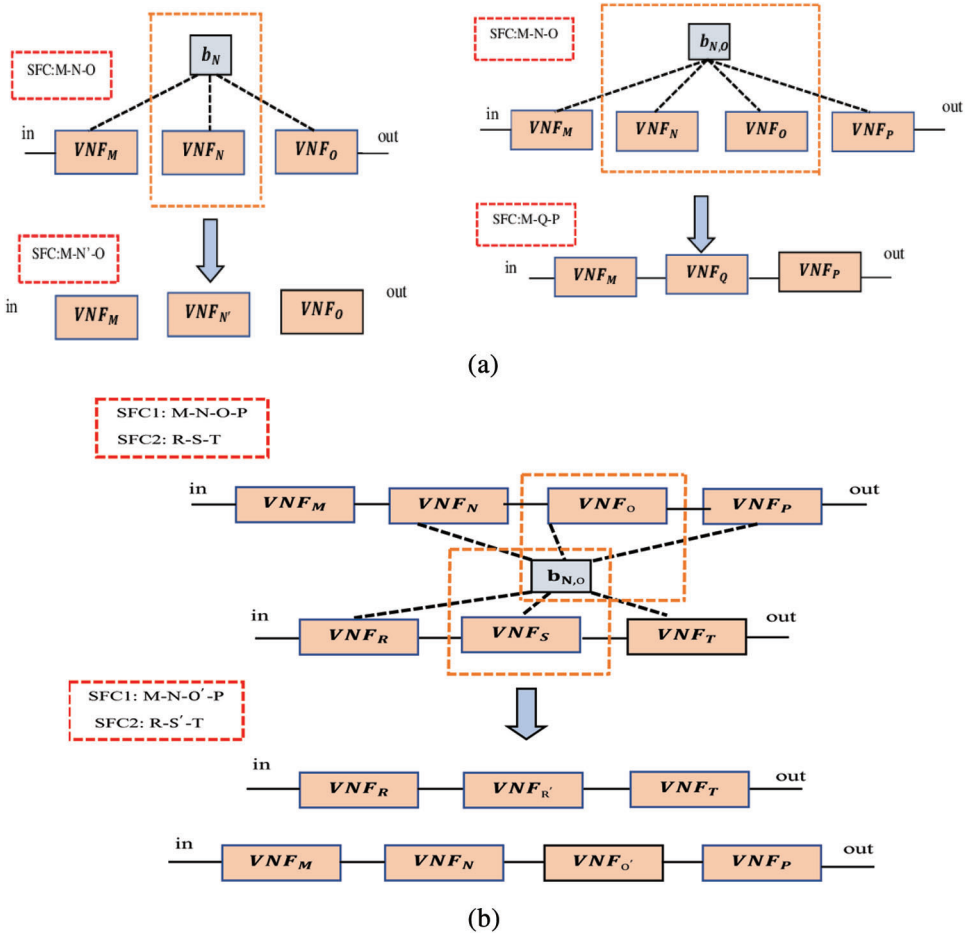

Figure 4: (a) One and two VNF backups from different SFCs (b) Two VNF back up from different SFCs

6 Results and Discussion

The performance of the proposed method is evaluated based on four parameters which include backup cost, number of used PN nodes, SFC request utility and latency. In this section, the outcomes are discussed to prove the superiority of the proposed method. In the proposed HH-CE algorithm-based selection model is compared with MinCost and MaxRbyInr method, the result shows that our method reduces the cost-effectively and increases the reliability. The format of selecting the VNF in MinCost and MaxRbyInris different from the proposed method where the VNF is selected based on the low demand of resources after that the next minimum reliable VNF is selected. The basic concept of MinCost is it chooses the VNF with minimum cost in each iteration. Similarly, for a MaxRbyInr, reliability measurement is calculated for each iteration, finally, the maximum reliability VNF is selected.

The initial cost of the proposed method is measured for different reliability under the backup cost. In this paper, the 1100 SFC request is considered for the VNF-FG. The backup cost of the proposed method has increased by 11.4%, 42.8%, 14.2% when compared with CERA, MinCost, and MaxRbyInr with a

reliability of 95%. Similarly, for 98% of reliability, the backup cost of the proposed method has increased to 11.4%, 42.8%, 14.2% when compared with CERA, MinCost, and MaxRbyInr. From Fig. 5, even when the requirement is 99.9, the proposed method still keeps a favorite place on using the least amount of backup cost.

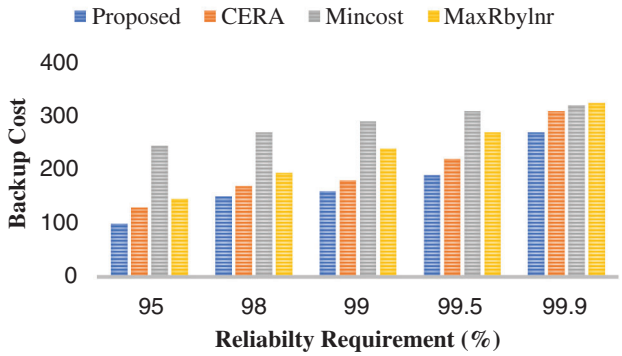

Figure 5: Reliability requirement *vs*. backup cost

Other than the principal money, network operation expenses are additionally utilized. Empowering a PN hub to back VNF occurrences will expend equivalent assets. Exploring the number of utilized PN hubs for repetition makes a difference appraise the OPEX of PN hubs. Fig. 6 shows the number of reliabilities *vs*. the number of used PN nodes plots. At the reliability of 95, the number of used PN nodes in the proposed OG-ES method is reduced to 11.1%, 22.34%, 50% than the previous CERA (Cost-Efficient Redundancy Algorithm), MinCost, and MaxRbyInr methods. Moreover, HH-CE only utilizes 9% of the PN nodes with the required rate of 99.5. At the condition of 99.5, the MaxRbyInr takes the advantage to reach its PN node usage to the highest range and backup with less.

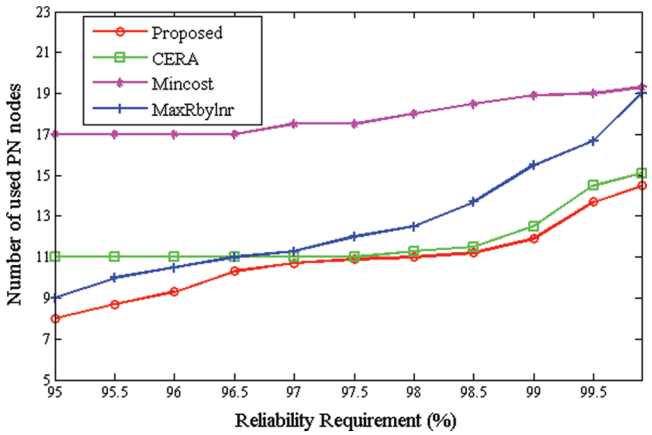

Figure 6: Reliability requirement *vs*. the number of used PN nodes

To evaluate the performance based on Cost-Efficient Ratio, the HH-CE is compared with previous techniques which are shown in Fig. 7a. At the reliability of 95, the cost-efficiency rate of the proposed HH-ES method is increased to 12.5%, 25%, and 18.75% than the previous CERA, MinCost, and MaxRbyInr methods. At the condition of 99.5, the proposed increased the CER to 12.5%, 25%, and 18.75% with previous CERA, MinCost, and MaxRbyInr schemes.

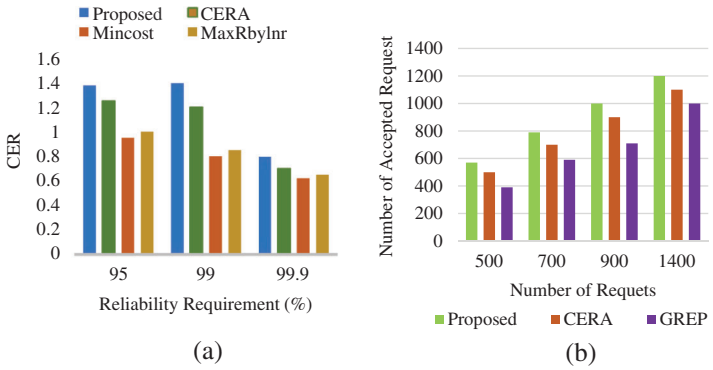

Figure 7: (a) Reliability requirement *vs.* CER (b) The number of requests *vs*. the number of accepted requests

The performance improvement of the proposed method based on the number of accepted requests is shown in Fig. 7b. For HH-CE, the chosen best VNF is very easy and accurate hence, the placement of these VNFs is done carefully. Even though the required PN node decreases, the resource utilization is increased and the risk of rejection of resource utilization is reduced. Finally, the VNF backup and data procession are done efficiently. When compared with the proposed method with CERA and GREP, the number of accepted requests is increased to 3.5% and 7%. At the request rate of 1100, the proposed method accepts 1200 requests among the SFC request which accomplishes almost 80% of requests.

The performance improvement of the proposed method based on the average resource utility's number of requests is shown in Fig. 8. When compared to the proposed method with VNF-SC, VNFSC-LC, VNF-SC-random, and CERA, the average resource utility is increased to 16.6%, 20%, and 10.7%. At the request rate of 80, the proposed method request utility reaches its maximum with the rate of 25. Fig. 9 shows the average service latency of the proposed method with previous methods such as VNF-SC, VNFSC-LC, VNF-SC-random,and CERA.The computation time of selecting the best backupVNF among the SFC request in the proposed method is reduced largely compared with other previous methods. Because the best is selected based on the HH-CE algorithm, which consumes only less amount of time to perform its operation.

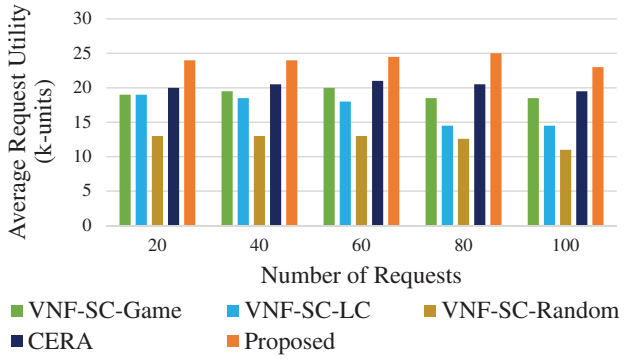

Figure 8: Number of requests *vs.* average request utility

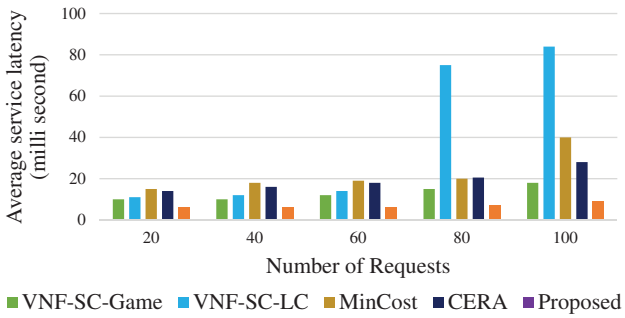

Figure 9: Number of requests *vs*. average service latency

7 Conclusion

This paper proposes a Hybrid Hexagon-Cost Efficient algorithm to get the best VNF among the various VNF and back up the best VNF which reduces the backup cost and increases the reliability. This was examined with a Physical Network of 116 node network maps where the backup cost and computation time were reduced by 57% and 45%. As a result, this proposed system achieves less backup cost, high reliability, and low time consumption which can improve the virtualized network function operation. In future work, the cost-efficient algorithm can be applied to whole case rather than a specific field.

Acknowledgement: The authors with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Basile, F. Valenza, A. Lioy, D. R. Lopez, A. P. Perales *et al.,* "Adding support for automatic enforcement of security policies in NFV networks," *IEEE/ACM Transactions on Networking*, vol. 27, no. 2, pp. 707–720, 2019.

[2] Z. Xu, W. Liang, M. Huang, M. Jia, S. Guo *et al.,* "Efficient NFV-enabled multicasting in SDNs," *IEEE Transactions on Communications*, vol. 67, no. 3, pp. 2052–2070, 2018.

[3] R. Sairam, S. S. Bhunia, V. Thangavelu and M. Gurusamy, "NETRA: Enhancing IoT security using NFV-based edge traffic analysis," *IEEE Sensors Journal*, vol. 19, no. 12, pp. 4660–4671, 2019.

[4] I. Farris, T. Taleb, Y. Khettab and J. Song, "A survey on emerging SDN and NFV security mechanisms for IoT systems," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 812–837, 2018.

[5] M. Bonfim, F. Freitas and S. Fernandes, "A semantic-based policy analysis solution for the deployment of NFVservices," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 1005–1018, 2019.

[6] I. Alam, K. Sharif, F. Li, Z. Latif, M. M. Karim *et al.,* "A survey of network virtualization techniques for internet of things using SDN and NFV," *Computing Surveys*, vol. 53, no. 2, pp. 1–40, 2020.

[7] M. Garrich, F. J. M. Muro, M. V. B. Delgado and P. P. Marino, "Open-source network optimization software in the open SDN/NFV transport ecosystem," *Journal of Light Wave Technology*, vol. 37, no. 1, pp. 75–88, 2018.

[8] H. Cao, H. Zhu and L. Yang, "Dynamic embedding and scheduling of service function chains for future SDN/NFV-enabled networks," *IEEE Access*, vol. 7, pp. 39721–39730, 2019.

[9] R. Hohemberger, A. F. Lorenzon, F. Rossiand and M. C. Luizelli, "Optimizing distributed network monitoring for NFV service chains," *IEEE Communications Letters*, vol. 23, no. 8, pp. 1332–1336, 2019.

[10] J. Wu, S. Luo, S. Wang and H. Wang, "NLES: A novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2463–2475, 2018.

[11] X. Tian, W. Huang, Z. Yu and X. Wang, "Data driven resource allocation for NFV-based internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8310–8322, 2019.

[12] Q. Ye, W. Zhuang, X. Li and J. Rao, "End-to-end delay modeling for embedded VNF chains in 5G core networks," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 692–704, 2018.

[13] W. Ding, H. Yu and S. Luo, "Enhancing the reliability of services in NFV with the cost-efficient redundancy scheme," in *Proc. ICC*, Paris, France, IEEE, pp. 1–6, 2017.

[14] D. Chemodanov, F. Esposito, P. Calyam and A. Sukhov, "A constrained shortest path scheme for virtual network service management," *IEEE Transactions on Network and Service Management*, vol. 16, no. 1, pp. 127–142, 2018.

[15] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, A. Meddahi *et al.,* "NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3330–3368, 2018.

[16] A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz and A. Skarmeta, "Security orchestration and enforcement in NFV/SDN-aware UAV deployments," *IEEE Access*, vol. 8, no. 1, pp. 131779–131795, 2020.

[17] M. T. Raza, S. Lu and M. Gerla, "EPC-sec: Securing LTE network functions virtualization on public cloud," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3287–3297, 2019.

[18] J. Sun, G. Zhu, G. Sun, D. Liao, Y. Li *et al.,* "A reliability-aware approach for resource efficient virtual network function deployment," *IEEE Access*, vol. 6, pp. 18238–18250, 2018.

[19] H. D. Chantre and N. L. D. Fonseca, "Multi-objective optimization for edge device placement and reliable broadcasting in 5G NFV-based small cell networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2304–2317, 2019.

[20] T. Madi, H. A. Alameddine, M. Pourzandi and A. Boukhtouta, "NFV security survey in 5G networks: A three-dimensional threat taxonomy," *Computer Networks*, vol. 197, no. 13, pp. 108288, 2021.

[21] J. Fan, M. Jiang, O. Rottenstreich, Y. Zhao, T. Guanetet *et al.,* "A framework for provisioning availability of NFV in data center networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2246–2259, 2018.

[22] S. Yin, S. Huang, H. Liu, B. Guo, T. Gao *et al.,* "Survivable multipath virtual network embedding against multiple failures for SDN/NFV," *IEEE Access*, vol. 6, pp. 76909–76923, 2018.

[23] A. S. Sendi, Y. Jarraya, M. Pourzandi and M. Cheriet, "Efficient provisioning of security service function chaining using network security defense patterns," *IEEE Transactions on Services Computing*, vol. 12, no. 4, pp. 534–549, 2016.