DUJASE Vol. 6 (2) 49-58, 2021 (July) https://doi.org/10.3329/dujase.v6i2.59218

An Efficient Handover Mechanism for SDN-Based 5G HetNets

Shaikhum Monira[1], Upama Kabir[1*], Mosarrat Jahan[1] and Uchswas Paul[2]

[1]*Department of Computer Science and Engineering, University of Dhaka, Dhaka, Bangladesh*
[2]*Department of Computer Science and Engineering, University of Information Technology and Sciences, Dhaka, Bangladesh*

[*]*E-mail: upama@cse.du.ac.bd*

Received on 27 April 2021, Accepted for publication on 19 September 2021

ABSTRACT

Handover is crucial for data portability, real-time data generation, and data processing in mobile technology. Up to 4G, handover efficiency reached optimal stability. However, with the entrance of 5G, the cellular network has turned into a complete heterogeneous network (HetNet) with enormous diversity due to the integration of Internet of Things (IoT) devices with mobile networks. Resource-constrained IoT devices differ notably in operational features from traditional mobile devices. Those devices usually need a smaller geographical cell with better connectivity coverage than conventional large cells of the same size. Hence, to support IoT, 5G splits large geographical cell areas into small cells and allows bandwidth sharing during Device-to-Device (D2D) communication. In a nutshell, 5G infrastructures and architectures have been changed a lot from the previous generations, and handover needs to be re-thought for efficient mobility management. This paper has incorporated the concept of Software-defined Network (SDN) in a 5G cellular network to simplify HetNet and provide efficient handover management within it. We illustrate our proposed handover management concept within this simplified HetNet that utilizes idle time scanning and pre-authentication to reduce handover delay. The experimental implementation shows a significant 42% delay optimization during inter-domain reactive handover with 50% less communication overhead than the existing scheme.

Keywords: SDN, 5G, HetNet, Handover, Mobile Communication.

1. Introduction

5G cellular technology emerges intending to realize the next-generation network where machines, objects, and devices work together. The development of sensor devices, data sensing, data collection from the environment, data sharing, and analysis of the collected data to provide improved services are now getting priorities to ease our daily life activities. Especially, the Internet of Things (IoT) devices are contributing a lot to real-time, valuable data generation for smart home security, agriculture, transportation, education, industrial automation, disaster detection, early warning [1 - 4], etc. Due to the continuous expansion of such usages, these devices are gradually entering into the era of 5G technology. Hence, one of the major targets of 5G is vast accessibility to various IoT devices. 5G facilitates the IoT devices revolutionarily by providing immense advantages in data speed, and communication delay (< 1ms) [5].

The massive involvement of IoT includes enormous diversity in 5G HetNet. IoT devices are different both in respect of their hardware infrastructure and software. Hardware variation from CPU type, networking interfaces, available sensors/actuators, etc., results in diversity in devices' processing power and coverage [6]. Due to low processing capability and coverage, IoT devices cannot directly connect to the traditional cellular base stations responsible for geographical cells. Hence, 5G splits standard cells into smaller geographical areas and incorporates different small cells such as microcell, picocell, and femtocell in the 5G network to support network access to those devices [7]. On the other hand, software diversity in IoT comes from different operating systems, programming languages, libraries, stacks, etc., based on which communication protocols changes [8]. Both hardware and software diversities make handover challenging within 5G HetNet. The simultaneous collaboration of different types of cells and devices with varying software configurations creates heterogeneous networks (HetNets) in 5G. The high mobility rate of these devices causes a frequent change in connection with cellular stations associated with small cells. A quick handover that supports an unnoticeable delay of passing data from one cell to another is crucial for 5G to continue mobile devices' faster operation. Thus, optimizing the delay of handover in 5G is an exciting research direction [9].

The involvement of IoT devices with countless diversity makes handover more complicated when resource-constrained IoT devices have the low processing power to generate enough signal strength to directly communicate with the cellular network. In such a case, devices need the assistance of an intermediate device to send data in the network, known as the device-to-device (D2D) communication [10 - 11]. Hence, a new question arises about the efficient management of the handover process using D2D. Besides, the diversity of the 5G network and resource-constrained devices' participation creates difficulties in ensuring network access by the legitimate network components, affecting the network's correct functioning.

In literature, Bi et al. [12] proposed a comprehensive mobility management scheme that utilizes SDN to optimize packet transmission routes. Although this scheme supports authentication during the handover process, the authors did not mention how authentication is reinforced in a distributed environment. Moreover, this scheme does not remember the previous interactions of the network components. Hence, every inter-domain handover should verify the communicating entities before starting the handover process, which causes message overhead for repetitious authentications. Besides, Ozhelvaci and Ma [13], and Duan and Xang [14] proposed authentication solution for the 5G network. These works lack the complete design of the handover process and do not address the diverse communication requirements of 5G. None of the works support handover for D2D communication scenarios.

In this paper, we propose an SDN-based simplified handover scheme to reduce the handover complexities due to the heterogeneity of 5G HetNets. Besides, we propose an authentication mechanism for the 5G network environment. Moreover, we minimize the handover delay through an idle scanning mechanism. In particular, our contributions are as follows:

- We propose an SDN-based 5G handover solution to optimize handover delay by addressing the diversity of 5G network with the help of SDN.
- We propose an authentication mechanism where a centralized authentication server establishes mutual trust among the domain controllers to ensure the credibility of the connected network components.
- We present an idle scanning solution that separates authentication from handover and performs the controller-to-controller authentication in advance to speed up the handover process.
- We implement the proposed scheme and evaluate its performance through extensive experiments. The results show that our scheme achieves an overall 42% delay reduction through idle scanning.

The rest of the paper is organized as follows. Section 1.1 presents a summary of the related works. Besides, Section 2 demonstrates the system model of the proposed scheme as well as discusses the detailed operation of the proposed scheme. Section 3 presents our experimental results. Finally, Section 4 concludes the paper with some future direction of works.

1.1 Related Work

5G is the emerging cellular technology, which is under development for global deployment. Handover in 5G is a significant research issue. Both traditional LTE-based and Software-defined Network (SDN) based handover mechanisms exist in literature to support 5G handover [15 - 16]. Cellular Technology divides a geographical area into smaller hexagonal areas known as cells [17]. A base station is responsible for maintaining a cell and provides network coverage to various types of data transmission, such as voice or digital data. Mobile devices support a wireless connection with the base station for network access, where neighboring cells use different frequency ranges to avoid interference. Non-neighboring cells reuse non-overlapping frequency ranges. All base stations connect to a Mobile Switching Centre (MSC), which maintains handover among base stations [18]. In a Software-defined Network (SDN), the data plane and control plane are separated. Handover requests are resolved within the control plane where devices of the data plane generate handover requests based on different criteria (mobility models, signal strength, etc.) [12]. The recent SDN paradigm favors lots of blessings in comparison to the traditional network architecture. Complicated network architecture has become simplified, programmable, and scalable to a large extent through SDN deployment. In a conventional network, both the data plane and control plane are integrated, so incorporating a slight modification or security aspect requires an extensive alteration in the overall network. This process is not only time-consuming but also needs lots of effort and cost. On the other hand, decoupled SDN architecture is getting special attention day by day in terms of flexibility, scalability, and security. Hence, several works of literature attempt to resolve the handover challenges in 5G HetNet with the SDN paradigm.

The design and implementation of the recent 5G cellular network are subject to significant attention from both academia and industry. Jain et al. [19] explained thoroughly how the 5G mobility management requirement varies significantly from the existing, reliable 4G technology. 5G technology is expected to support several features such as the softwarization of the previous vendor-driven networks, user connectivity through several radio access technologies (RATs), mobility of access points (AP) and relay stations, and connectivity of the low-powered sensor and IoT devices. The authors also presented a comparison among different mobility standards such as IETF, 3GPP, LTE, and non-3GPP multi-connectivity solutions, and RSS-based handover management to determine their suitability for 5G in terms of scalability, reliability, and versatility.

In literature, several works focus on optimizing the handover process through delay reduction. For example, Bilen et al. [20] proposed an SDN-based handover management system for ultra-dense 5G networks to avoid unnecessary, frequent, and back-and-forth handovers generated due to the enormous number of devices. The authors proposed a Markov chain-based, SDN-enabled handover management scheme to resolve this issue. Besides, Basloom et al. [21] proposed an AP-based clustering approach to reduce the handoff delay in SDN-based 5G Networks. This work uses the K-mean algorithm and the genetic algorithm (GA) to construct hybrid AP clusters. When a device tends to change geographical area, it tries to find a new AP in the current cluster. Otherwise, it finds a new AP in a different cluster. If a new suitable AP is found, the device establishes a connection to it. Alongside, Park et al. [22] proposed an SDN-based handover framework for a smart factory consisting of various mobile devices. In this scheme, a handover decision is made based on the received signal strength (RSS) and the mobile devices' speed, aiming to reduce handover delay. Moreover, Duo et al. [23] proposed an SDN-based handover mechanism for Vehicular Ad Hoc Networks

(VANET) where each vehicle is an SDN-enabled device with an LTE interface and an 802.11p interface. In this scheme, a vehicle is selected as a cluster head that maintains communication with the cluster members and keeps another connection with the LTE eNB. An SDN controller monitors the network, detects possible handover, and updates the network topology information based on the information collected through the connected eNB. Likewise, Wang et al. [24] proposed an SDN-enabled mobility management scheme for LTE-based networks. In this scheme, user equipment (UE) communicates with the controller through Scells (eNodeB) to change its current Scell. When a UE changes a Scell cell, the old Scell forwards the UE's data to the new Scell under the controller's supervision. The controller keeps a threshold value for such chain communication. If the number of Scells involved in this chain communication exceeds the threshold value, the controller switches the path taking the advantages of multiple paths to the target Scell to avoid signaling and delay overhead. Besides, Chen et al. [25] analyzed 5G small cell networks' coverage and the handoff process's performance based on the fractal characteristic. The authors presented a multi-directional path loss model for the 5G fractal small cell networks. They analyzed the handover performance based on handover probability, handover rate, and various settings of this path loss model. Lastly, Bi et al. [12] proposed SDN-based solutions for both intra-domain and inter-domain handover mechanisms that apply to various networks such as WiFi, LTE, and 5G. The proposed network model consists of SDN Controller, Edge Switch (ES), and Forwarding Switch (FS). SDN controllers separate a network into different domains. ES provides wireless connections to the mobile nodes within its coverage while FS establishes connections between two different domains. The author proposed solutions for intra-domain and inter-domain handover mechanisms in both proactive and reactive modes. When a mobile node moves from one ES to another under the same controller, it is referred to as intra-domain handover. On the other hand, inter-domain handover occurs when a separate domain controller controls the destination ES for handover. This scheme does not provide any specific authentication mechanism and does not support D2D communication. On the contrary, in our work, we in-corporate periodic controller-to-controller authentication to reduce handover delay and provide authentication in D2D communication.

Ozhelvaci and Ma [13] proposed an SDN-based authentication scheme for the inter-domain handover process. In this scheme, Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is used to authenticate user equipment (UE), exchange keys, and encrypt data. The SDN controller contains a Handover Authentication Module (HAM) that checks UEs' positions and takes the necessary measures to prepare the base stations and APs for the handover process. Besides, Duan and Xang [14] proposed an SDN-based handover authentication mechanism for 5G HetNets. In this scheme, the control plane includes an Authentication Handover Module (AHM). The controller monitors and predicts users' location and makes handover decisions while AHM authenticates devices coming to the coverage of the controller. In contrast to the previous works, our scheme introduces a centralized authentication server to support authentication in the distributed environment of the 5G network containing several authoritative domains.

Ouali et al. [26] proposed an SDN-based handover management scheme for D2D communication. During D2D communication, the leader node (device via which another device communicates with base stations) measures the radio resource control (RRC) information. Suppose it finds a handover tendency in its follower nodes. In that case, it reports to the current base station that communicates with the target base station to establish a connection with the particular follower device. Finally, the target base station informs the SDN controller to update the change in the network topology. In contrast to this work, we present a handover mechanism for D2D communication considering the high mobility of leader/relay nodes. In 5G, due to the small cell area, handover occurs so frequently, so in our handover scheme, each node can move independently without affecting other nodes' handover or communication.

Monira et al. [27] proposed a secure and delay-efficient handover mechanism for SDN-enabled 5G HetNet. This scheme achieves efficiency by reducing message communication and security by using encrypted communication suitable to low-power devices. In contrast to our work, this scheme emphasizes the security of the information transmitted through 5G HetNets. It supports authenticated users in the network through device authentication and information privacy through an encryption mechanism. Finally, it provides a rigorous security analysis to demonstrate the security features of the proposed scheme.

2. Proposed Scheme

2.1 System Model

We introduce the system model of the proposed scheme in Fig. 1. In this model, the SDN-enabled 5G network consists of several distinctive authoritative domains. Each authoritative domain is a vendor-specific network comprising HetNets of different 5G frameworks. It supports various geographical cells to enable connectivity to various end devices. Besides, each network component in the System model is associated with a Universally Unique Identifier (UUID), a 128-bit number used to identify a network entity exclusively [28].

An SDN controller, also known as domain controller is responsible for coordinating the operations of the associated authoritative domain. It can trace any network components such as switches and end devices working within its authoritative domain.

An OpenFlow-enabled SDN switch, also known as cell switch is responsible for managing the cells within the authoritative domain. In the traditional networks, cells are often managed by different cellular stations such as base stations, picocells, and femtocells. In the proposed model, we replace them with OpenFlow-enabled SDN switches to simplify the diversity of cellular stations. This can also be performed by deploying an OpenFlow module inside typical cellular stations. A cell switch manages a 5G geographical cell under the supervision of the associated domain controller. It connects different end devices such as cell phones, IoT devices, and sensor devices within its geographical coverage area following the rules set by its domain controller. It also handles different data packets and participates in the handover process. The cell switches may differ in terms of coverage area, infrastructures, or connected devices, but they can maintain communication with each other using the OpenFlow protocol.

End devices generate, communicate and receive data. Usually, various devices such as laptops, mobile phones, IoT devices, and sensor devices communicate through the 5G network. For a 5G network, a significant portion of the end devices such as IoT devices and sensor nodes are resource-constrained in terms of processing, storage, and communication capacity.

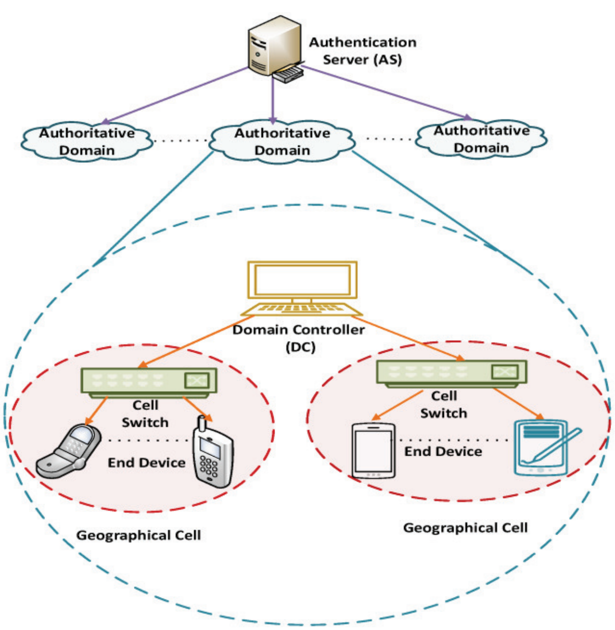


Fig. 1. System model for SDN-enabled 5G HetNet.

An authentication server (AS) is a globally accessible server connecting all domain controllers of the 5G network. It may follow a centralized or distributed architecture but ensures reliable and full-time stable accessibility. The primary responsibility of the AS is to authenticate domain controllers and establish mutual trust among them. A domain controller trusts different domain controllers if they are certified by the AS. In such cases, a controller believes in the credibility of network components verified by the other controllers [29]. Besides, AS maintains a list, L_{C_i} to store the domain certificates of the known controllers of C_i.

To simplify the network design, we assume that the 5G network consists of *n* authoritative domains, each supporting *m* geographical cells. Therefore, the 5G network includes a total number of n domain controllers C_i where $1 \leq i \leq n$. Each C_i is responsible for managing m cell switches S_j where $1 \leq j \leq m$. Further each cell switch S_j provides connectivity to *p* devices D_k where $1 \leq k \leq p$.

Within each authoritative domain, there exists simple SDN architecture to simplify the 5G HetNet. Such a design provides SDN blessings in 5G HetNet in terms of vast scalability and centralized security. Authentication Server (AS) serves as an external service provider in our decoupled system model. In this respect, features like scalability, security have no dependency on AS. The interaction with the AS adds an insignificant amount of message communication cost, which is negligible as it becomes optimized with the overall handover cost.

In the following sections, we present our proposed scheme with a detailed discussion of its working principles in three steps. Our proposed method starts with a network initialization step to set up the network. After configuring the network, our scheme starts preparing to handle future handovers through idle scanning to reduce future handover delays. Finally, we explain how different handover requests are being processed on demand.

2.2 Network Initialization and Authentication

When the 5G network is formed for the first time, authoritative domains are uniquely specified. Each domain controller C_i responsible for a particular authoritative domain communicates with the Authentication Server (AS) to get a unique authentication certificate. AS checks the credibility of C_i, and if C_i is a legitimate controller then AS generates a unique and time stamped certificate X_{C_i} and sends it back to C_i. The certificate X_{C_i} contains a unique domain ID to identify a specific authoritative domain. Each C_i shares this certificate with all the intra-domain devices such as switches and end devices. It can authenticate and attach a device with the possession of the certificate X_{C_i}. When C_i attaches a device for the first time, it shares its certificate X_{C_i} with that connected device. When a device is legitimate to C_i, it is also reliable to the other domain controllers authenticated by the AS. When X_{C_i} expires, C_i requests for a new certificate to the AS.

2.3 Idle Scanning before Handover

Handover occurs when a mobile device changes its current cell and moves to a new cell. If a mobile device moves to a new cell within the same domain, no authentication is required between the present and new cell switches. On the other hand, if a mobile device proceeds to another authoritative domain and changes the attached cell, authentication must occur between the domains to continue the handover operation. Hence, the overall handover process consists of three major tasks such as 1) authentication of target cell, 2) connection establishment to the target cell, and 3) forwarding of data to the new cell during the handover process. Delay optimization is required in each of these steps to reduce the overall delay of the handover process. If authentication between the current cell and the neighboring cells can be decoupled from the handover process and performed in advance, the handover process becomes faster. As discussed before, when handover takes place within the same domain, authentication of the new cell is not required as both the current cell and the new cell reside within the same authoritative domain. In contrast, if handover occurs within cells located in different authoritative domains, the domain controllers must authenticate each other before proceeding to the handover process. Therefore, we propose an idle time scanning based solution for the controller-to-controller authentication that works as a background process and follows the steps shown in Fig. 2. The detailed procedure of the idle scanning is discussed below:

1) Each domain controller C_i periodically sends a request to the AS to get its current known controller list L_{C_i} .According to our proposal, a domain controller C_i is a known controller to another domain controller C_j if they share the same community policy or previously authenticated each other through AS.

2) In response, the AS sends the updated L_{C_i} to C_i.

3) C_i stores the received L_{C_i} in the local storage. Besides, it communicates each of its neighbor controllers with a request message containing its domain certificate X_{C_i}. In that message, C_i solicits its neighbor controller C_j to acknowledge it as a known controller.

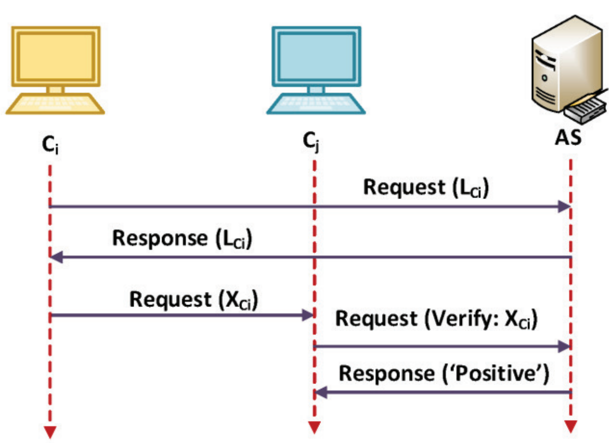


Fig. 2. Idle time scanning process.

4) Upon receiving the request message, each neighbor C_j checks its known list L_{C_j}t to identify whether the message comes from a known controller or not. If not, then C_j sends a request to the AS to learn about C_i.

5) If AS verifies C_i as an authentic controller, it updates both L_{C_i} and $L_{C_j}$by adding C_i and C_j to each other's known list and then sends a 'POSITIVE' acknowledgement to C_j. On the other hand, if C_i is not a verified controller, AS responds with 'NOT FOUND' response.

6) C_j adds C_i to its known list L_{C_j}after receiving 'POSITIVE' acknowledgement from the AS. If C_j receives 'NOT FOUND' response from the AS, it adds C_i to a bad list to avoid future requests from C_i.

2.4 Handover Scheme

Our proposed mechanisms modify the existing handover mechanism [12] to reduce handover delay in the 5G HetNet. If a device migrates to a new cell from its previously connected cell and both cells reside in the same domain, the handover is known as intra-domain handover. On the other hand, if a device moves to a new cell managed by a different domain controller, the handover is referred to as inter-domain handover. Moreover, devices may go through the handover process proactively or reactively in intra-domain or inter-domain environment. Suppose a device changes cellular station during real-time data generation, such as during phone call and data transfer, and initiates handover for better coverage without being completely disconnected from the current cellular station. In that case, the handover is a proactive handover. In contrast, if a device gets completely disconnected from the previous cellular station and performs handover in a new cellular station coverage, the handover is called reactive handover. These four handover types may occur with the device-to-device (D2D) communication or without it. In the subsequent sections, we discuss various handover mechanisms.

2.4.1 Intra-domain Proactive Handover without D2D Communication

Due to the mobility, an end device D_k changes its connectivity from its currently connected cell switch S_j to another cell switch S_q with better signal strength. In this case, both S_j and S_q reside in the same administrative domain. As shown in Fig. 3, device D_k sends a handover request to its domain controller C_i via the associated cell switch S_j. The handover request contains the UUID of the target switch S_q. On receiving the handover request, C_i checks S_q's authoritative domain. When it detects S_q as its subordinate cell switch, C_i simply sets rule for S_q to establish a new link between S_q and D_k. After the link establishment, C_i instructs S_j to drop the link with D_k.

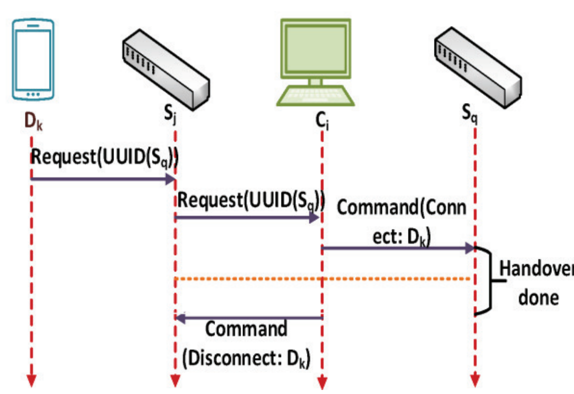


Fig. 3. Intra-domain proactive handover without D2D communication.

2.4.2 Intra-domain Reactive Handover without D2D communication

Excessive load on the current cellular station or low signal strength due to the mobility causes a device D_k to get disconnected from its currently attached cellular station managed by a cell switch S_j. In such a case, a device D_k checks for the available coverage and requests a new cell switch S_q for connection. Here, S_j and S_q belong to the same authoritative domain, and hence, they are managed by the same domain controller C_i. As shown in Fig. 4, D_k sends a handover request to C_i via S_q that contains the UUID of S_q and the domain certificate of its previously connected controller, in this case X_{C_i}. When C_i receives a handover request from D_k, C_i recognizes D_k as a verified device under its domain due to the possession of X_{C_i}. It simply sets a rule to connect D_k with the cell switch S_q.

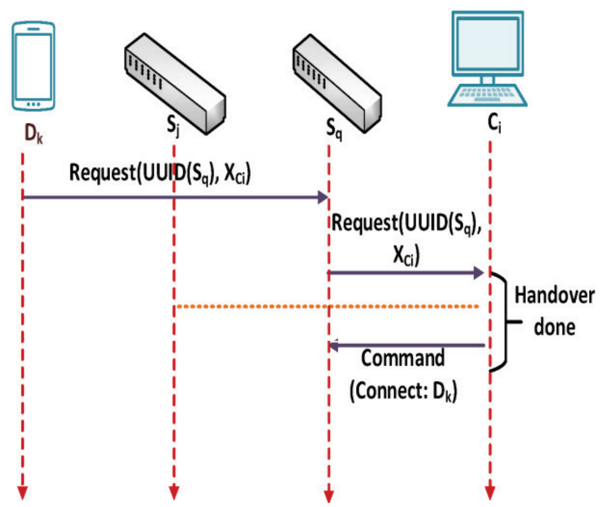


Fig. 4. Intra-domain reactive handover without D2D communication.

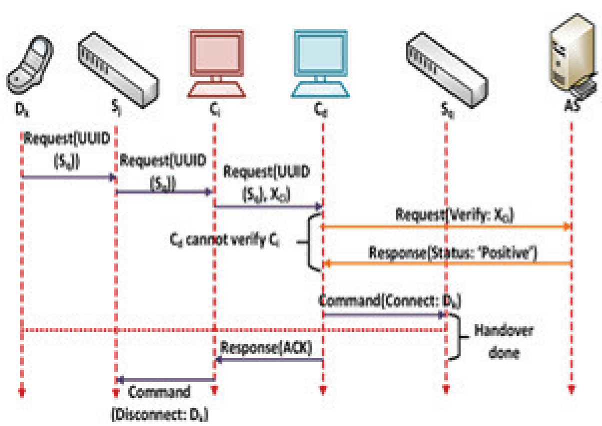


Fig. 5. Inter-domain proactive handover without D2D communication.

2.4.3 Intra-domain Proactive Handover with D2D Relay Communication

Device-to-device (D2D) communication occurs when a device D_k is under the coverage of a cell switch S_j and due to low capability D_k is unable to communicate directly with S_j. Hence, D_k uses a relay device RD to communicate with S_j. Handover can occur even if the device D_k is exchanging information through D2D communication. Due to mobility, D_k may come to a geographical region where the coverage of another cell switch S_q overlaps with the current cell switch S_j, and the signal coverage of S_q is greater than S_j. In this case, the initial handover request of D_k is forwarded to S_j via RD. The remaining handover procedure exactly follows intra-domain proactive handover without D2D communication discussed in **Section 2.4.1.** After changing the geographical coverage, D_k may directly communicate with the new cell switch S_q if the signal strength permits. Otherwise, D_k selects a new relay node RD by device scanning algorithms [30] to communicate with S_q.

2.4.4 Intra-domain Reactive Handover with D2D Relay Communication

The reactive handover occurs after a device D_k gets disconnected from its connected cell switch S_j. Therefore, previous D2D relay communication (if any) also terminates automatically. In this scenario, D_k identifies a cell switch S_q to connect, D_k sends a handover request to S_q. The remaining handover process follows the intra-domain reactive handover without D2D communication discussed in **Section 2.4.2.** After handover, D_k may select a relay node RD to communicate with S_q if it fails to maintain direct communication with S_q

2.4.5 Inter-domain Proactive Handover without D2D communication

Inter-domain proactive handover occurs when a device D_k moves to a new switch S_q in a different administrative domain in a running data transfer stage. As shown in Fig. 5 the handover process starts when D_k sends a handover request to its domain controller C_i via its connected cell switch S_j. This handover request contains the target cell switch S_q's UUID. After receiving the handover request, C_i checks whether S_q is a subordinate cell or not. In this case, C_i detects that a different controller C_d manages S_q. Hence, C_i sends a handover initialization request to C_d with the UUID of S_q and its domain certificate X_{C_i}. After receiving the request, C_d checks whether C_i is known to it using its current known controller list L_{C_d}. If C_i is not known, C_d sends a request to the AS to verify X_{Ci} . Based on the decision of AS, C_d takes the necessary decisions. If AS sends positive feedback, C_d establishes a new connection link between D_k Then it sends an acknowledgement to C_i and C_i instructs S_j to drop the link with D_k. On the other hand, if AS sends negative feedback, C_d sends a response message to C_i informing handover is not possible.

Our proposed idle scanning technique speeds up the inter-domain handover process by periodically performing controller-to-controller authentication. This increases the possibility that C_d identifies C_i in its known controller list L_{Cd} which reduces the overall handover time by eliminating the waiting time for the AS to verify the authenticity of C_i

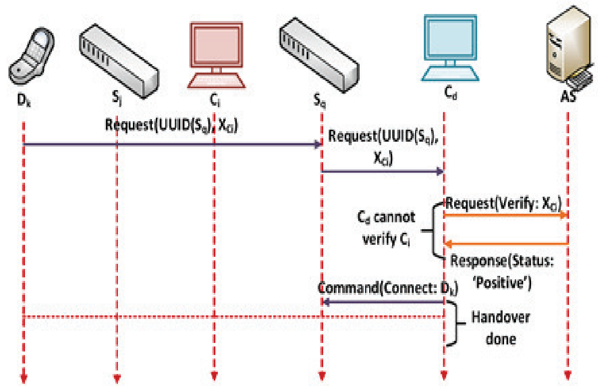


Fig. 6. Inter-domain reactive handover without D2D communication.

2.4.6 Inter-domain Reactive Handover without D2D communication

This type of handover starts when a device D_k gets disconnected from its current cell and identifies a new cell to connect which is located in a different authoritative domain. As shown in Fig. 6 the device D_k sends a handover request consisting of the UUID of new cell switch S_q and the domain certificate of its previous domain, in this case X_{C_i}, to S_q. S_q forwards this message to its domain controller C_d. When C_d receives the handover request of D_k it checks whether D_k's previous controller domain C_i is known to it or not. If they are known, C_d simply tells S_q to connect D_k. Otherwise, C_d communicates with the AS to verify X_{C_i}. After AS sends positive confirmation, C_d allows S_q to connect D_k. On the other hand, if AS sends negative response, then C_d simply discards the handover request.

2.4.7 Inter-domain Proactive Handover with D2D Relay Communication

During D2D, D_k cannot directly communicate with S_j and needs the help of a relay device RD. This type of handover process is almost similar to inter-domain proactive handover process without D2D Relay Communication discussed in **2.4.5.** The only differences are: 1) D_k sends the initial handover request to S_j via RD, and 2) D_k may need to perform a device scanning algorithm to find a new relay node after the handover process if it cannot directly communicate with the destination switch S_q.

2.4.8 Inter-domain Reactive Handover with D2D Relay Communication

During reactive handover, D_k gets dis-connected from its current cell switch S_j. Hence, D_k finds a new cell switch S_q in a different authoritative domain to connect. It sends a handover request to S_q, and the handover takes place in the same way discussed in **2.4.6.** At the end of the handover process, D_k may select a relay device by performing a device scanning algorithm, if required.

3. Experimental Result and Discussion

3.1 Experimental Setup

To evaluate the performance of the proposed scheme, we configured a 5G network using Mininet ver. 2.2.1 [31] and Python-based remote Pox controller ver. 2.7.12 [32]. Mininet was used to construct the network topology and Pox controller was used to control the authoritative domains remotely. Besides, we used socket programming to establish communication among hosts and switches. Table 1 presents various parameters used in the simulation environment.

Table 1: Simulation Parameters

Parameter	Value
Number of maximum controllers (Domain setup)	16
Number of SDN switches per controller	2
Number of end devices per switch	16
Link speed	100 Mbps
Number of maximum concurrent handover requests	128

The primary notion of this research is to process each handover request efficiently irrespective of mobile users' diverse mobility models within HetNet and devices' diversity. Our concern is to reduce handover delay significantly with meager communication overhead in 5G HetNet, disregarding how those requests are generated within devices, how diverse D2D or M2M influence handover request generation. We used handover time. number of message communication and controller's response to parallel requests to evaluate the performance of the proposed scheme. Our results were averaged over 100 iterations of the experiments, where error bars in all graphs present 95% confidence interval.

3.2 Handover Time

Handover times for intra-domain handover scenarios are shown in Fig. 7. From our proposed scheme, it is apparent that idle scanning has no impact on intra-domain handovers as the placement of both the old and new cell switches in the same authoritative domain eliminates the need for domain-to-domain authentication. However, with D2D communication, handover time increases approximately 25% than the without D2D communication due to device-to-relay single-hop communication overhead shown in Fig. 7. Moreover, both intra-domain proactive and reactive handovers finish their execution simultaneously as they both require the same number of steps to complete the handover process.

Fig. 8 shows that idle scanning significantly reduces the handover time for inter-domain handover scenarios. Idle scanning eliminates controller-to-controller authentication in the handover process by performing it beforehand. As shown in Fig. 8(a), it optimizes delay by almost 21% and 20% for inter-domain proactive handover without D2D communication and with D2D communication, respectively.

Besides, Fig. 8(b) shows that reactive handover without D2D communication achieves approximately 42% delay reduction whereas reactive handover with D2D attains nearly 36% delay optimization. Although D2D communication increases delay by approximately 25% as shown in Fig. 7, the notable delay reduction by idle scanning suppresses its effect.

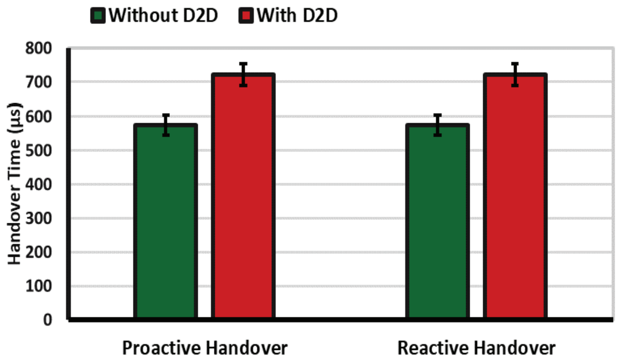
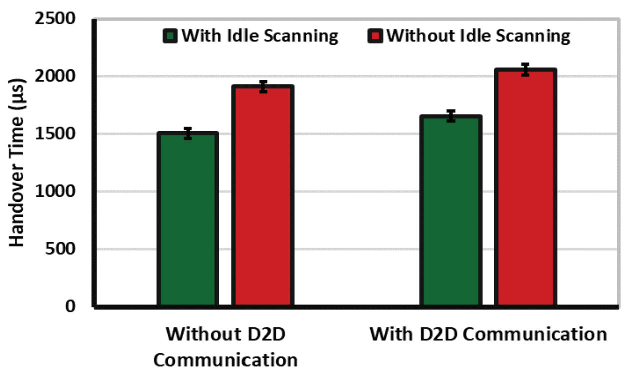
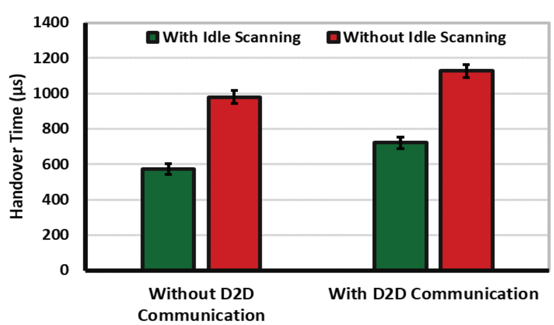


Fig. 7. Handover time for intra-domain handover.

In the case of inter-domain reactive handover, when a device disconnects from the previous cellular station, it directly sends a handover request to the new cell switch without involving its previous domain controller. Hence, this handover is noticeably faster than inter-domain proactive handover due to the elimination of communication between the previous controller and the new controller.



(a) Inter-domain proactive handover



(b) Inter-domain reactive handover

Fig. 8. Handover time for inter-domain handover.

It is clearly visible from Fig. 8 that with-out D2D communication inter-domain reactive handover decreases delay by nearly 61% compared to the proactive handover. Besides, with D2D communication reactive handover achieves almost 56% delay minimization over proactive handover.

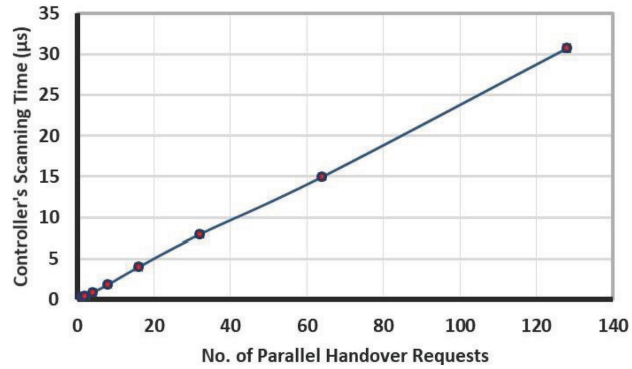


Fig. 9. Scanning time of a domain controller.

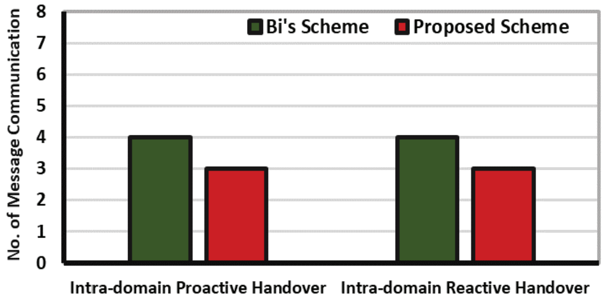
3.3 Domain Controller's Scanning Time

With the higher number of devices (both cell switches and end devices), the number of handover requests increases. Each handover request is an individual process that comes to the controller concurrently. Hence, the controller becomes busy with the increasing number of handover tasks with the growing number of devices. The overall performance of the 5G network depends on the controllers' performance. Fig. 9 presents the impact of the increasing number of handover requests on the scanning time of a controller. The curve growth seems linear where the scanning time changes slightly in microseconds for 128 parallel requests.

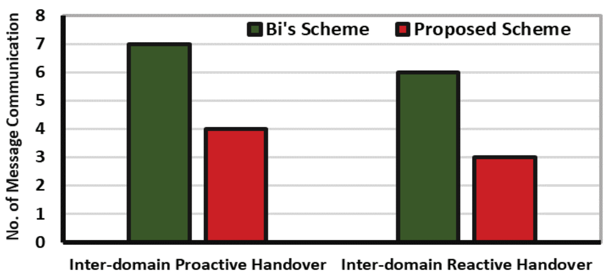
3.4 Comparison with Existing Scheme

We compared the performance of our proposed handover schemes with the performance of Bi et al. [12]'s mobility management schemes in terms of the number of messages exchanged. The Bi's scheme [12] proposed intra/inter-domain handover mechanisms for SDN-based networks without considering the D2D communication. As shown in Fig. 10(a), for intra-domain handovers, message communications are reduced by almost 25% for both proactive and reactive handover, which ultimately results in delay reduction. In Bi's Scheme, extra communication delay occurs as a switch sends a handover request confirmation message in addition to the device's handover request. On the other hand, Fig. 10(b) shows our proposed scheme reduces delay by approximately 43% and 50% for proactive and reactive handover, respectively. Bi's scheme did not mention authentication policy and did not consider the previous history of inter-actions. Hence, each inter-domain handover request goes through an authentication process which brings message overhead. In contrast, our scheme uses idle scanning to authenticate domain controllers periodically and eliminates the authentication for the known controllers in the handover process which ultimately improves the overall performance.

Table 2 presents a comparison of the proposed scheme with several other existing works based on several features. Our scheme considers an SDN-based 5G HetNet, whereas Ozhelvaci et al. [13] integrated SDN controller with traditional LTE architecture to resolve authentication in 5G HetNet through EAP-TLS protocol. Due to different



(a) Intra-domain handover



(b) Inter-domain handover

Fig. 10. Comparison with Bi Scheme [12].

network design principle, it is inconsequential to compare both schemes numerically in message communication. Besides, we abstract the overall concept of multilevel access points with a single cell switch which contrasts Duan & Wang [14]'s system model. Therefore, a comparison of the proposed scheme with Duan & Wang [14] would not be congruent. Hence, we provide a comparison based on features only. Table 2 shows that our scheme is a robust 5G handover scheme compared to the current works as it supports all the necessary characteristics of 5G handover such as handover authentication, SDN programmability, and D2D communication.

Table 2: Comparison with Existing Works

Scheme	5G handover authentication	SDN programmable	5G handover scheme	D2D communication
Bi et al. [12]	yes	yes	yes	no
Ozhelvaci et al. [13]	yes	yes	yes	no
Duan & Wang [14]	yes	yes	yes	no
Our scheme	yes	yes	yes	yes

4. Conclusion

This paper formulated a novel and unified handover management scheme for 5G HetNets that incorporates SDN to simplify the design complexities. The proposed scheme optimizes the handover process by notably reducing delay through the idle scanning process. Besides, it offers an authentication scheme to assure network access by the permissible network components only. Moreover, the proposed scheme considers the D2D communication during the handover process. The analysis manifests that our scheme can minimize handover delay significantly by nearly 42% using idle scanning. Besides, our handover mechanisms optimize 50% communication overhead in inter-domain handover scenarios comparing to the existing scheme. As the real-time data processing by the mobile devices is becoming crucial, our scheme positively influences it by reducing latency in the mobility management mechanisms of 5G HetNets. Our work can be further extended to support handover in various wireless networks such as WiFi, WiMax, and Zigbee. Moreover, massive experiments can be run over different types of IoT devices in diverse sectors such as nanotechnology, VANET, and smart home to verify the acceptability of SDN-based handover mechanisms. We aim to develop a handover solution that would also process handover requests from D2D and M2M.

References

1. M. Stočes, J. Vaněk, J. Masner, and J. Pavlík, "Internet of things (IoT) in agriculture-selected aspects," *Agris on-line Papers in Econ. Inform.*, vol. 8, no. 1, pp. 83–88, 2016.
2. F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in *Proc. IEEE Int. Symp. Consum. Electron. (ISCE)*, pp. 1–2, 2015.
3. J.-i. Jeong, "A study on the IoT based smart door lock system," in *Inf. Sci. Appl. (ICISA),* Springer, pp. 1307– 1318, 2016.
4. A. Ali, "IoT based disaster detection and early warning device," *Int. J. MC Square Scientific Res.*, vol. 9, no. 3, pp. 20–25, 2017.
5. J. Pilz, M. Mehlhose, T. Wirth, D. Wieruch, B. Holfeld, and T. Haustein, "A tactile internet demonstration: 1ms ultra low delay for wireless communications towards 5G," in *Proc. IEEE Conf. Comp. Commun. Workshops (INFOCOMWKSHPS),* pp. 862–863, 2016.
6. S. Nastic, S. Sehic, D.-H. Le, H.-L. Truong, and S. Dustdar, "Provisioning software-defined IoT cloud systems," in *Proc. IEEE int. conf. future internet of things and cloud*, pp. 288–295, 2014.
7. T. Ma, F. Hu, and M. Ma, "Fast and efficient physical layer authentication for 5GHetNet handover," *in Proc. IEEE 27th Int. Conf. Telecommun. Netw. Appl. (ITNAC),* pp. 1–3, 2017.
8. R. Dautov and H. Song, "Towards IoT diversity via automated fleet management." in MDE4IoT/ModComp@ MoDELS, pp. 47–54, 2019.
9. S, Sönmez, I. Shayea, S. A. Khan, and A. Alhammadi, "Handover management for next-generation wireless networks: A brief overview," in *Proc. IEEE Microwave Theory Techn. Wireless Commun. (MTTW)*, vol. 1, pp. 35–40, 2020.
10. R. I. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. J. Rodrigues, "5GD2D networks: Techniques, challenges, and future prospects," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3970–3984, 2017.
11. M. H. Adnan and Z. Ahmad Zukarnain, "Device-to-device communication in 5G environment: Issues, solutions, and challenges," *Symmetry*, vol. 12, no. 11, p. 1762, 2020.
12. Y. Bi, G. Han, C. Lin, M. Guizani, and X. Wang, "Mobility management for intro/inter domain handover in software-

defined networks," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 8, pp. 1739–1754, 2019.

13. A. Ozhelvaci and M. Ma, "Secure and efficient vertical handover authentication for 5GHetNets," in *Proc. IEEE Int. Conf. Inf. Commun. Signal Process(ICICSP)*, pp. 27–32, 2018.

14. X. Duan and X. Wang, "Authentication handover and privacy protection in 5GHetNets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, 2015.

15. V. Yajnanarayana, H. Rydén, and L. Hévizi, "5G handover using reinforcement learning," in *Proc. IEEE 3rd 5G World Forum (5GWF)*, pp. 349–354, 2020.

16. J. Prados-Garzon, O. Adamuz-Hinojosa, P. Ameigeiras, J. J. Ramos-Munoz, P. Andres-Maldonado, and J. M. Lopez-Soler, "Handover implementation in a 5GSDN-based mobile network architecture," in *Proc. IEEE 27th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, pp. 1–6, 2016.

17. T. S. Rappaport, *Wireless communications: principles and practice*. Vol. 2, prentice hall PTR New Jersey, 1996.

18. J. F. Kurose, *Computer networking: A top-down approach featuring the internet, 3/E*. Pearson Education India, 2005.

19. A. Jain, E. Lopez-Aguilera, and I. Demirkol, "Are mobility management solutions ready for 5G and beyond?" *Comput. Commun.*, vol. 161, no. 1, pp. 50–75, 2020.

20. T. Bilen, B. Canberk, and K. R. Chowdhury, "Handover management in software-defined ultra-dense 5G networks," *IEEE Netw.*, vol. 31, no. 4, pp. 49–55, 2017.

21. S. Basloom, N. Akkari, and G. Aldabbagh, "Reducing handoff delay in SDN-based 5G networks using AP clustering," *Procedia Comp. Sci.*, vol. 163, pp. 198–208, 2019.

22. D. G. Park, J. W. Oh, and J. Jeong, "SFSH: a novel smart factory SDN-layer handoff scheme in 5G-enabled mobile networks," *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 5913–5925, 2020.

23. R. Duo, C. Wu, T. Yoshinaga, and Y. Ji, "SDN-based handover approach in IEEE 802.11p and LTE hybrid vehicular networks," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud and Big Data Comput., Internet of People and Smart City Innov.*, pp. 1870–1875, 2018.

24. Q. Wang, S. Zhao, and C. Hou, "UE assisted mobility management based on SDN," in *Proc. IEEE 11th Int. Conf. on Comput. Sci. & Educ. (ICCSE)*, pp. 689–695, 2016.

25. J. Chen, X. Ge, and Q. Ni, "Coverage and handoff analysis of 5G fractal small cell networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1263–1276, 2019.

26. K. Ouali, M. Kassar, T. M. T. Nguyen, K. Sethom, and B. Kervella, "An efficient D2D handover management scheme for SDN-based 5G networks," in *Proc. IEEE 17th Annu. Conf. Consum. Commun. Netw. (CCNC)*, pp. 1–6, 2020.

27. S. Monira, U. Kabir, M. Jahan, and U. Paul, "An efficient and secure handover mechanism for SDN-enabled 5Ghetnet," in *Proc. IEEE Int. Conf. Black Sea Commun. Netw. (BlackSeaCom)*, pp. 1–6, 2021.

28. P. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) URN namespace," RFC 4122, 2005.

29. C. Zhang, X. Wang, A. Dong, Y. Zhao, Q. He, and M. Huang, "Energy efficient network service deployment across multiple SDN domains," Comput. Commun., vol. 151, pp. 449–462, 2020.

30. S. Goli-Bidgoli and N. Movahhedinia, "Towards ensuring reliability of vehicular ad hoc networks using a relay selection techniques and D2D communications in 5G networks," *Wireless Pers. Commun.*, vol. 114, pp. 2755–2767, 2020.

31. Mininet documentation. [Online]. Available: https://github.com/mininet/mininet/wiki/Documentation.

32. POX manual current documentation. [Online]. Available: https://noxrepo.github.io/pox-doc/html.