Hindawi
Security and Communication Networks
Volume 2020, Article ID 5429630, 18 pages
https://doi.org/10.1155/2020/5429630

Review Article

Mobile IPv6 Vertical Handover Specifications, Threats, and Mitigation Methods: A Survey

Supriyanto Praptodiyono,[1] **Teguh Firmansyah**,[1] **Mudrik Alaydrus**,[2] **M. Iman Santoso**,[1] **Azlan Osman**,[3] **and Rosni Abdullah**[4]

[1]*Electrical Engineering Department, Universitas Sultan Ageng Tirtayasa, Banten, Indonesia*
[2]*Electrical Engineering Department, Universitas Mercu Buana, Jakarta, Indonesia*
[3]*School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia*
[4]*National Advanced IPv6 Centre, Universiti Sains Malaysia, Penang, Malaysia*

Correspondence should be addressed to Supriyanto Praptodiyono; supriyanto@untirta.ac.id

Received 25 February 2020; Revised 7 June 2020; Accepted 14 July 2020; Published 4 August 2020

Academic Editor: Fulvio Valenza

Internet users have grown substantially over the last decade, especially following the emergence of mobile technology. Most Internet connections nowadays are accessed using mobile devices in order to stay connected all the time and everywhere. Owing to the limited coverage of such access points as well as base stations, mobile devices are required to handover connectivity if there is a move to other locations. Horizontal handover is conducted when the movement is within the same network. Otherwise, there must be vertical handover when external network infrastructure is encountered. However, as the Internet is an open network that naturally lacks trust between users, the mobile nodes that move to an external network are susceptible to various attacking activities. Compromising mobile nodes may cause users to lose their data as well as destroy their mobile devices in terms of both software and hardware. Securing mobile devices is crucial in order to avoid losses in terms of not only money but also facilities. Although mobile nodes have been developed with certain security features, some researchers have found vulnerabilities. This paper surveys in detail the security vulnerabilities of mobile IPv6 vertical handover and the current relevant mitigation methods. Furthermore, we describe the mechanism of mobile IPv6 vertical handover and its security vulnerability as well as security mechanisms proposed by researchers. Based on the survey, there are apparently weaknesses in current security features that are in need of solutions to minimize the effect of malicious activities. An open direction of future research on mobile IPv6 vertical handover security is elaborated at the end of this paper.

1. Introduction

Over the last decade, the Internet has connected billions of people around the world. Based on the Internet world statistics of [1], Internet user growth reached 1,104% from 2000 to 2019. The number of Internet users in March 2019 was roughly 4,346,561,853 or 56.1% of the world population. Users connect to the Internet using various techniques, either personal computers or mobile devices. In terms of mobile devices, in recent years (2017), the number of mobile broadband subscriptions reached approximately 4.3 billion subscriptions globally [2]. This means that almost 60% of Internet users in the world are now connecting through mobile broadband. The reason for this extreme growth in the usage of the mobile Internet is because mobile broadband is more affordable than fixed broadband. Based on the document [2], from the period of 2013 to 2016, mobile broadband prices as a percentage of GNI per capita were halved. Hence, Internet users can connect to the Internet anywhere and at anytime with low charges.

According to Márquez-Barja [3], technically, the increase in wireless communications is based on factors such as the miniaturization of mobile devices, the multiple networking interfaces available, the availability of wireless technology, and the emergence of mobile applications. Besides all this, currently, Internet service providers have provided various wireless infrastructure and technology, including UMTS (Universal Mobile Telecommunications System) [4], Wireless Fidelity (Wi-Fi) [5], and 4G LTE (Long-Term Evolution) [6]. Hence, the available infrastructure allows for connectivity through various wireless and wired technology. Furthermore, a user can continue using their mobile devices at anytime and anywhere without any obstacle in terms of device connectivity, which is known as the always-connected concept [7]. The higher layer protocol should support IP mobility to make mobile devices reachable anywhere and transparent.

With mobile technology, when a mobile device moves from its current place to a new location, it should be able to handover its connection channel from the existing connected network to another network infrastructure. Based on RFC 3753 [8], if the handover occurs between access points of the same network type, such as UMTS to UMTS or WLAN to WLAN so-called horizontal handover (HHO), this involves the same signal coverage, data rate, as well as mobility. On the contrary, when the mobile node (MN) moves between different types of access points, such as UMTS to WLAN, it is known as a vertical handover (VHO) [9, 10]. Unfortunately, during the handover, a mobile device can temporarily lose its connection and thus is unable to send or receive packets. This condition could degrade the performance of mobile data communication.

Owing to the rapid growth of wireless communication users and Internet users in general, there is a problem with the availability of IP addresses [11]. To overcome the problem, IETF (Internet Engineering Task Force) has standardized a new Internet Protocol, dubbed IPv6 [12], as the successor of the current Internet Protocol, IPv4 [13]. In terms of mobile communication, IETF has also proposed a standard of IPv6 mobility in RFC 3775 [14] that is obsolete by RFC 6275 [10]. The design of mobile IPv6 combined the experience of the mobile IPv4 [15] and some new features of IPv6. One of the new features is removing the need for deploying a different router as a foreign agent. Besides, the IPv6 address belongs to the MN at home, called the Home Address (HoA), which is still the same, although it moves to a foreign network. Furthermore, mobile IPv6 is more flexible than mobile IPv4.

The nature of wireless communication, including mobile IPv6 that broadcasts messages to receivers, is explicitly prone to malicious attacks [16]. The attacks could be eavesdropping [17], DoS (denial of services) [18], spoofing [19], MiTM (Man in the Middle) [20], and falsification [21]. The 2016 Norton cybercrime [22] report stated 87% of consumers have in-home Wi-Fi, and they engage in dangerous behaviours. However, 66% of their home connections are not protected. Hence, the condition leaves them vulnerable to hackers eavesdropping on their networks and intercepting their information. Within the last year, 689 million people in 21 countries were impacted by cybercrime. Furthermore, $126 billion has been spent globally dealing with cybercrime. It has conclusively been shown that an increasing number of wireless devices could increase illicit cybercriminal activities, possibly including computer hacking, malicious attacks, data forging, and financial information theft.

A mobile device should update its status when changing its position within a heterogeneous network. The update of the information can be performed using a binding update (BU) message [14, 23]. The message is used to bind its HoA and a new care-of address (CoA) generated from the new location's access router. Information in the message is essential to inform the node's home agent, a new location, along with its new CoA. However, if no IPsec is implemented, these messages are not authenticated and therefore create serious vulnerabilities [23–25]. A malicious node might send such spoofed information containing a claim that there is a difference between the MN's new location and the real one. Attackers might also capture and learn the information transferred to an MN and redirecting the message to the sender. As a result, threats on mobile IPv6, especially in the process of VHO, are posed against confidentiality, integrity, and also availability [14].

Some papers have reviewed VHO decision mechanism as well as its security, such as [9, 26–29]. In [9, 27], the authors surveyed a comprehensive VHO decision to find out a mechanism designed that provides the required QoS of a wide-range application. It described each of the mechanisms and compared them. However, it did not talk about the implementation of the mechanism in IPv6 as well as Mobile IPv6. The authors of papers [26, 28] reviewed the VHO management process, especially pertaining to the decision-making mechanism. It focused on the lower layer that provides the fundamental features of all VHO mechanisms. The authors in [29, 30] assessed the security protocols put forward for securing Mobile IPv6. However, it focused only on the BU protocol instead of the overall VHO on Mobile IPv6.

In order to facilitate a comprehensive discussion on Mobile IPv6 VHO security, this paper surveys the security vulnerabilities of VHO on Mobile IPv6, including movement detection, address configuration, and location updates that have not been reviewed by previous studies. Besides this, it also reviews some mitigation methods proposed by various researchers. The rest of this paper consists of an overview of VHO in Mobile IPv6 in Section 2. Section 3 elaborates upon security vulnerability of the VHO mechanism especially on the BU protocol. Section 4 provides a discussion of the current security proposals for mitigating security incidents, and then, Section 5 summarizes this paper.

2. Overview of VHO in Mobile IPv6

The nature of mobility is movement from one place to another. In a new location, it may discover access router using Neighbour Discovery Protocol processes [31]. By using the router discovery [32], the MN may be connected to one or more external links. In order to continue its connection, it may generate a new IPv6 address, CoA, once it can discover an access router [33]. Hence, the MN now has two addresses: the HoA that remains the same and CoA that changes every time it connects to a new network. It generates a CoA using a subnet prefix obtained from the router attached to the external link. The MN then creates a binding between HoA and a new CoA. When the MN goes to several foreign networks, it will generate more than one CoA [34]. Furthermore, it has to determine one of them as a primary CoA [10]. The primary selected CoA is then used to communicate with the CN. All packets addressed to its CoA will be forwarded to the MN. However, the MN should register the primary CoA to ensure binding with its HoA to the HA. The communication in this condition could be classified into two communication modes.

2.1. Bidirectional Tunnelling. This mode is also called indirect communication of Mobile IP [10, 24], as illustrated in Figure 1. With this mode, a tunnel between MN and HA is created to transmit packets from HA to MN [35, 36]. However, the communication between CN and MN is still assisted by the HA. There is no direct connection between MN and CN. So, the registration of the MN's current binding is not required. The CN could be any node, including nodes without mobility support. Moreover, it need not update its binding cache.

When the CN transmits an IPv6 packet to MN, the packet will reach the HA first before the MN. The HA encapsulates and forwards the packet to the MN. Similarly, when the MN sends a packet to the CN, it will be tunnelled to HA and then forwarded generally through the network to the CN. In order to make the communication successful, the HA uses proxy neighbour discovery. This mode is sufficient to be used when the MN needs to inspect network traffic. The MN could use an IDS (Intrusion Detection System) on the home network to carry out virus scanning or firewall inspection [37].

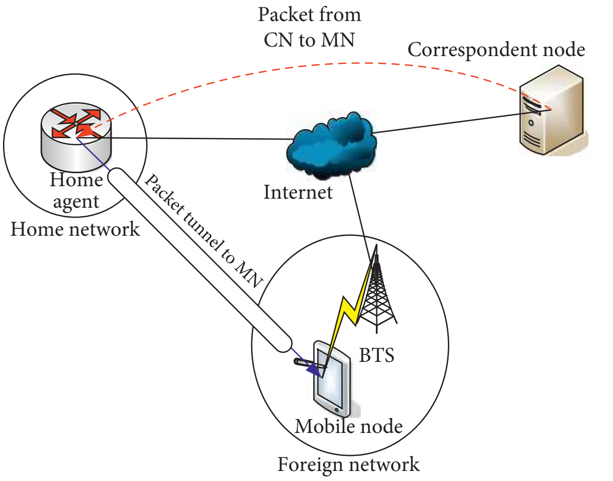

Figure 1: Bidirectional tunnelling.

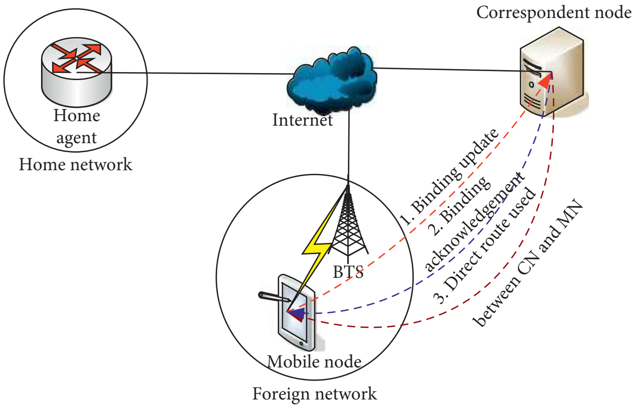

Figure 2: Route optimization.

2.2. Route Optimization. This mode is meant to optimize communication between MN and CN without continual assistance from the HA, as shown in Figure 2 [38–40]. To operate in this mode, all the CN should be supported by the Mobile IPv6 protocol. For the first packet, it travels from CN to HA to reach the MN. The MN then replies by informing the MN's new CoA to the CN (1) in the form of a BU message. Hence, the CN's binding cache can be updated by putting the new CoA in the binding list. The CN acknowledges the received BU by sending a BA message (2). Furthermore, the direct route between MN and CN has been formed, and hence, the next packets can be transmitted from CN to MN directly without traveling via HA, or vice versa (3).

Once the MN gets a new IPv6 address obtained from the external network, it has to make sure the address uniqueness by using Duplicate Address Detection mechanism [41, 42]. Moreover, the MN should handover its current communication with CN using the new binding of CoA-HoA. Handover is conducted in the same network known as horizontal handover [43, 44]. As is known, VHO is used when the MN performs handover among heterogeneous access network technology [3, 45, 46].

In general, VHO involves four steps that include underlying procedures, movement detection, address configuration, and location update [10, 47]. Masud [48] classifies the procedures into the link-layer (L2) phase and network layer (L3) phase. In the first phase, it involves the link-layer communication that includes scanning, authentication, and association phase. During the scanning phase, the MN broadcasts a request packet to all access points in the new location to inform their existence. This is also done to detect the main characteristics of the available networks, such as signal strength, the level of interference, and the bit error rate [49]. Otherwise, the MN may just listen passively for the beacon bearing all information about an access point. Right after the scanning phase has finished, the MN should authenticate the new access point immediately. This phase is essential to make sure the new access point is authentic. The last step of the L2 phase is an association to transfer the associated signal from the old access point to the new one. The next phase is the handover procedure in L3 that involves the last three procedures (movement detection, address configuration, and location update), as depicted in Figure 3.

As shown in Figure 3, there needs to be an amount of time to perform L3 handover in a Mobile IPv6 environment. The overall handover begins when the movement occurs

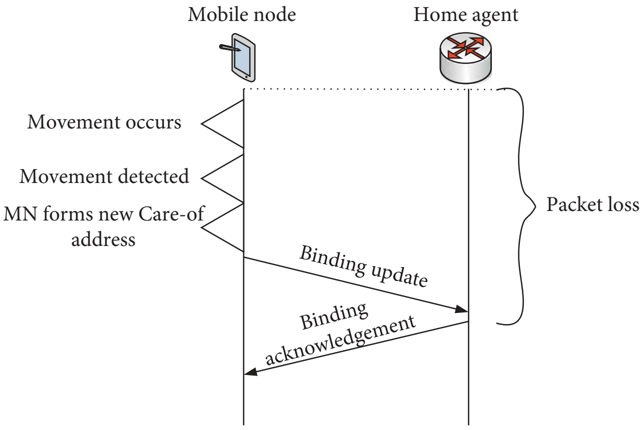

Figure 3: Handover procedure in layer 3.

until the MN obtains a BA message from its HA. Furthermore, it only could communicate with a CN when it receives a BA message from the corresponding CN. The following are the handover steps.

2.3. Movement Detection. Movement detection is defined as a process of deciding a new link-layer connection that the MN should rapidly determine whether a subnet change has occurred [50]. This process is conducted to detect the L3 handover by employing the neighbour discovery mechanism. It can be done by running Neighbour Unreachability Detection (NUD) as in RFC 7048 [51] to analyse whether the existing access router is still reachable. In the case unreachability is determined, the MN should discover a new access router by sending a router solicitation message to a group of access routers in the new location. It then analyses the router advertisement message [47] received from access routers as solicited messages. In case there is more than one access router in the new location, there is the requirement of running a vertical handover decision (VHD) algorithm [9, 46]. This will help the MN obtain the best point of attachment among candidates. Many proposals for VHD were submitted by researchers, such as in [9, 52, 53]. The movement detection process contributes to the total latency on Mobile IPv6 VHO. Some literature has studied reducing movement detection latency contributions, such as [50, 54, 55] by modelling and experimentation.

2.4. Address Configuration. Once a new access router is detected, an MN should discover routers in the new location to obtain a router advertisement (RS) message. The router advertisement contains various pieces of information, including prefix information, router, and network information, as well as the type of address configuration allowed [31]. In the case where the content of the prefix information matches its old prefix, the MN is still in the old network. The result of this analysis is the decision to configure a new CoA. The address configuration is conducted using the standard IPv6 address configuration, such as stateless address configuration as specified in RFC 4862 [56] and stateful address configuration using DHCPv6 standardized in RFC 3315 [57]. However, the new CoA is not permanent until the MN runs duplicate address detection (DAD) [58]. If there is no duplicate address detected, the MN updates its location. The process of address configuration also introduces latency to the Mobile IPv6 handover. Gregory Ian Daley [59] studied strategies for detecting network attachment in Mobile IPv6. He discussed a fast router advertisement scheme as an extension of IPv6 neighbour discovery.

2.5. Location Update. The address configured in the new location is known as CoA that should be bound with the HoA. However, the MN must inform the new address of binding to both its HA and existing CN. To perform the location update, it transmits a BU message to its HA and a corresponding CN in order to update its binding cache. The primary information included in the message is a new CoA generated for the IP address configuration phase. Once the HA or CN receives the BU message, they reply to a BA message immediately.

The VHO mechanism could be shown as in Figure 4. In the figure, for the first time, an MN (handphone) connects to a Wi-Fi network. In that location, it is communicating with a CN within the IPv6 network. The next time, the MN moves to a foreign network, but the MN wants to maintain communication with the CN. It detects a new network, which is the LTE/4G network (1). Furthermore, it seeks to build a new connection with the CN. As discussed earlier, when attached to a new network, the MN generates a new CoA using either the stateless or stateful address generation mechanism. It then engages in DAD using NDP. If no duplication is detected, the MN should update status by sending a BU message to the HA (message 2). The HA then validates the received message, updates its binding cache entry, and replies with a BA message (message 3). Finally, the MN sends a disconnection message (message 4) to the CN via the Wi-Fi network, informing the CN to terminate the original connection [60].

During VHO, the MN requires a specific amount of time to engage in movement detection, generation of new CoA, and registration of new status. This leads to a network latency problem. Overall, the latency consists of L2 handover latency and L3 handover latency [61]. The network layer latency consists of three elements [62]:

(a) Detection period (T_d) is the time for new network detection, including the receiving of a router advertisement from a new access router

(b) Address configuration interval (T_c) that is calculated from the receiving RA until the CoA configuration finishes

(c) Network registration time (T_r) is taken from the sending binding update to HA as well as CN until receiving the first packets from the CN

The total latency of the Mobile IPv6 VHO is formulated as the addition of the three periods formulated as follows:

$$\text{latency} = T_d + T_c + T_r. \tag{1}$$

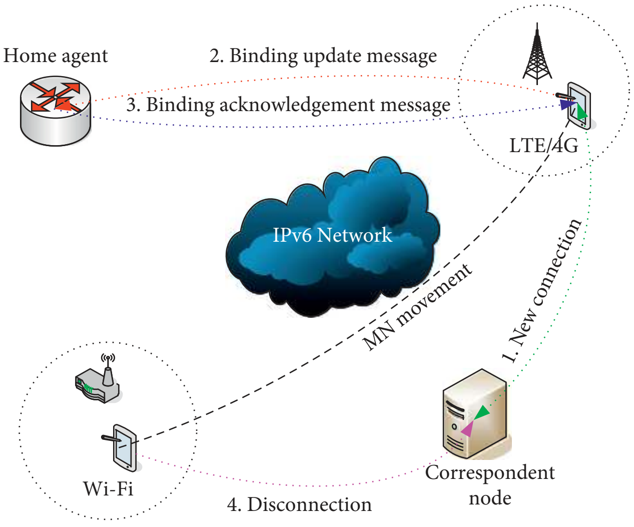

Figure 4: VHO from Wi-Fi to LTE.

A higher latency could degrade handover performance. In case route optimization is used, the latency is added by route optimization time (T_o) [63]. To reduce the network latency problem, IETF introduced a faster handover mechanism dubbed for the Mobile IPv6 mechanism (FMIPv6) in RFC 4068 [64] that was then obsoleted by RFC 5268 [65] and RFC 5568 [66]. The RFCs specified a mechanism to permit an MN to transmit IPv6 packets as soon as it attaches to a new subnet link. A number of papers had also been published to improve fast handover, such as [67–69]. The papers proposed the Flow-Based Fast Handover Method for Mobile IPv6 Network (FFHMIPv6). The protocol uses the flow label field in the IPv6 main header. Apart from this, the IETF also published RFC 4140, entitled "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," [70] that was obsoleted by RFC 5380 [71]. The RFCs specified a decrease in the number of signalling processes among MN, CN, and HA.

The authors in [26] listed several proposals for reducing the delay, such as the usage of an extra BU to reduce the tunnelling time between HA and the new access router proposed in [31]. This mechanism is performed by sending pre-BU and pre-BA before transmitting the fast BU. An Early Binding Fast Handover (EBFH) was posited in [62]. It completes the BU containing a new CoA before the link-going-down trigger. Prior to triggering signals, MN performs an early fast BU with its old access router. The authors in [72] put forth using the Router Solicitation for Proxy Advertisement (RtSolPr) message to request information to the current access router about the candidate for the new access router. Using the mechanism, the MN could obtain a Proxy Router Advertisement (PRtAdv) message containing prefix information to formulate a new CoA for the new access router, while it is still connected to the HA. Seamless MIPv6 was proposed in [9] that preconfigures bidirectional secure tunnels between HA and a new access router before performing the actual handover. It utilizes such tunnels to accelerate mobility management procedure of FMIPv6.

In order to obtain a new connection, the MN must make a network selection. The network selection had been discussed in certain references, such as [27, 28]. One of the network selection considerations is the cost-utility needed. The authors in [27] presented a formula to calculate the cost as follows:

$$F_i = \sum_k \left(\prod_j \epsilon_{ij}^k \right) \sum_j \left[f_j^k \left(\omega_j^k \right) N \left(u_{ij}^k \right) \right], \qquad (2)$$

where $N(u_{ij}^k)$ is the normalized utility of application k in network i in terms of attribute j; $f_j^k(\omega_j^k)$ is the weighting function of attribute j for application k; and ϵ_{ij}^k is the network elimination factor, either 1 or infinite, to reflect whether current network conditions are suitable for requested applications.

For example, if a network cannot guarantee the delay requirement of real-time applications, its corresponding elimination factor will be set to infinite. In this case, the corresponding cost becomes infinite, which eliminates this network.

Some researchers, such as [73–77], conducted a performance analysis on the fast handover mechanism. In summary, the fast handover was carried out by updating the messages related to NDP [31], such as router solicitation (RS) and RA. However, the modifications are conducted by adding information in the options field that potentially adds network overhead.

In order to reduce the overhead, Wu and Wang [77] proposed an improvement of the fast handover scheme by integrating the mechanism with the hierarchical Mobile IPv6. This scheme enhanced RS for a proxy. It starts by performing the link-layer handover process, and at the same time, the MN sends the improved RS for the proxy message to the access point. The content of the RS message is the information of the link-layer address or identifier of the targeted access point. Once the access point is identified, it will process the new CoA received representing the MN. Finally, a handover initiation message is transmitted by the access point to the access router for establishing a tunnel.

Seamless mobility in MIPv6-based wireless networks was proposed in the form of an Advanced Mobility Handover scheme (AMH) by Safa Sadiq [76]. A unique IPv6 HA is utilized by the MN to maintain communication with other CNs without the generation of a new CoA during the roaming process. This is because of the development of the MN-ID field as a permanent global address uniquely identified by the HA. Furthermore, the access point generates a temporary MN-ID when the MN is associated with a particular AP. This will temporarily save the address in an AP's table. In summary, the AMH scheme specifies the network layer-level handover process that is conducted before its default time. Thus, the communication between the MN and AP could be maintained during the network layer handover process.

3. Mobile IPv6 VHO Vulnerabilities

The Internet is an open network that naturally lacks trust between users. Furthermore, the security requirement must be considered in order to save our data as well as digital resources. Nowadays, mobile devices are the most common connected devices to the Internet (60%) [2]. Mobile IPv6 is a successor to the current mobile technology (Mobile IPv4) [15] that was developed to improve it in terms of performance as well as its security features. However, as Mobile IPv6 operates according to the mechanism discussed in previous section, it will lead to new vulnerabilities as investigated in [78]. This section elaborates the vulnerabilities of the security holes found in the Mobile IPv6 VHO. Since the Mobile IPv6 follows the operation of IPv6 in general, including the address configuration phase that uses NDP, it is also vulnerable to the IPv6 ND trust models and threats listed in RFC 3756 [79]. More comprehensive details on the NDP vulnerabilities were discussed in [80, 81]. This section focus on the vulnerabilities of the location update phase. The vulnerabilities could be on the protocol features weaknesses, configuration weaknesses, and security policy.

RFC 6275 identified the threats related to the Mobile IPv6 VHO into four categories that include threats involving BU message, those associated with the payload packets, the threat associated with prefix discovery, and the threat against the Mobile IPv6 security mechanism [10]. Since the signalling mechanism on VHO involves BU message, the threats on the BU have attracted many researchers. Most researchers such as [25, 29, 78] investigated vulnerabilities related to BUs as follows.

3.1. False BU.

3.1. False BU. A BU contains information that is used to know the current position of the MN. Employing this information, the HA and CN can obtain the updated CoA of the MN. Once the attacker has the chance to falsify the CoA or other information inside the BU message, the victim node may experience one or more of the following conditions.

3.1.1. Tampering Binding Cache Entry at the CN. The CN will update its binding cache once it receives the BU message containing CoA from the MN. It will check the cache entry to make sure the CoA information matches with the entries. If no entry is matched, the MN creates a new entry based on the information. Attackers can send a false binding update message. This will lead to tampering of the BU cache of the CN [82].

3.1.2. Tampering Binding Entry at the Home Agent. Like the CN, an HA also receives BU messages from an MN when it is attached to a foreign network. Attackers can falsify the content of BU messages to tamper with the HA's binding entry. Furthermore, when the HA wants to forward a packet to an MN, it will go to the wrong destination.

3.1.3. Connection Hijacking Attacks. It is assumed the MN is in communication with a CN, as in Figure 5. A malicious node can launch connection hijacking attacks [83] by sending a false BU message to the CN (message 1). The attacker claims that as the MN moves to a foreign network, it thus generates a new CoA. Once the CN receives the forged BU messages, it will start to communicate with the attacker instead of the MN. This condition indicates that communication between the CN and MN ceases. In such cases, the attacker could monitor the communication first before hijacking the connection. Furthermore, it obtains such information to run replay attacks as well as MiTM attacks.

3.1.4. MiTM Attacks. The attacker can insert itself into the communication path among the nodes in the Mobile IPv6. It may send a spoofed BU message to one of the targeted victims. The attacker acting as the man in the middle can then modify the BU messages, as depicted in Figure 6. This potentially hijacks the ongoing communication, tampers with the BU message, as well as creates a reflection attack [84].

3.1.5. DoS Attacks. This type of attack uses a BU message to stop the targeted victim's services. It can send a large amount of BU messages to a targeted victim to overwhelm its resources. Therefore, any positive node will not get any service because the victim's memory is already full. The attackers can also request the victim (CN or HA) to forward a message to a fake address belonging to them. A broad request can make the victim node busy and thus are not able to provide other services requested by a real node.

3.1.6. Replay Attacks. A replay attack is a continuous action after the MiTM attacks. In this case, the attacker eavesdrops on the communication between nodes in the Mobile IPv6. After receiving some information, the attacker may resend it to the recipient in order to make the victim confused [85]. For example, the attacker obtains the MN's CoA from its eavesdropping activity so that it could send a false BU message using the old MN's CoA after the MN moves away.

3.2. BU Flooding. Attackers can send fake BU messages at a very rapid rate to a victim that creates unnecessary tasks [86, 87]. They make the victim very busy processing the received BU in order to update its binding cache and, thus, denying it from handling other necessary services. The victim can be the HA, CN, or MN itself. This vulnerability can cause the binding cache memory of the victim to freeze and become full of no really meaningful entries. Hence, this valid node's entry will be prevented from being created in the binding cache.

3.3. Sending Spoofed BU. Nowadays, attackers can be anywhere in the network, including in the same link as the MN attached. This condition creates the opportunity for the attackers to monitor the communication between the MN with a CN passively. Once they know the content of the communication, they may send spoofed BU or BA messages to either the MN or CN. It may send the spoofed BU to the HA or CN, resulting in false updating binding entries. On

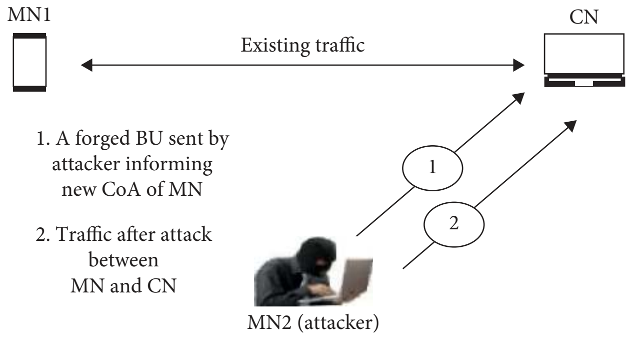
MN1
CN
Existing traffic
1. A forged BU sent by attacker informing new CoA of MN
2. Traffic after attack between MN and CN
1
2
MN2 (attacker)

Figure 5: Connection hijacking attacks.

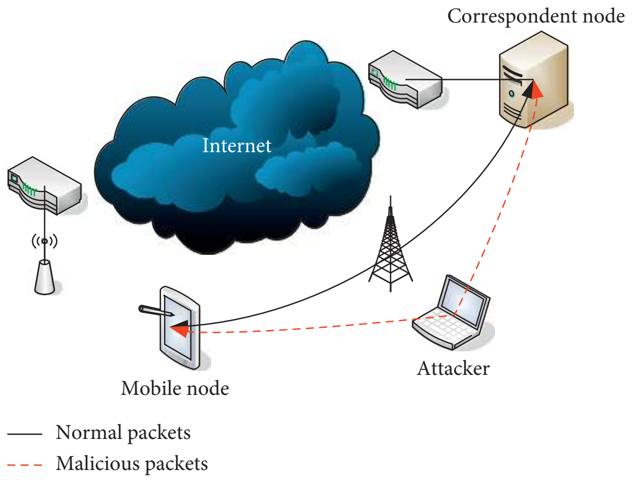

Figure 6: MiTM attacks.

the other side, the attacker may send a BA message to reply to a BU message.

3.4. Rogue Home Agent. Attackers can set up a rogue home agent that will receive messages from an MN. It may reject the HoTI or CoTI messages as the rogue HA is in the middle between the MN and CN. This can fail the return routability initiation process [24]. The rogue HA can also stop return routability by rejecting Home Tests and or Care-of-Tests sent from the CN to MN. Besides, it can also discard the BU messages resulting in no BA received by the MN.

3.5. Redirect Attacks. Redirect attacks happen when the attackers transmit redirect traffic back from a CN to a targeted destination. Based on [86, 88], redirect attacks on Mobile IPv6 can be classified into two forms: session hijacking attacks and malicious mobile node flooding. The first occurs when an intruder sends a forged BU message to a CN on behalf of the MN that moves to a new location as in the connection hijacking attacks. The attacker tries to redirect the communication between the CN and another malicious node. This attack could cause information leakage by conducting impersonation of the MN. It may also cause flooding to the other node. The second attack happens when a malicious MN informs that it has a new CoA by sending a valid BU message to its CN. The message contains a request to load a heavy file. Furthermore, the CN will reply by sending redirecting traffic that could potentially flood the targeted victim.

4. Traditional VHO Mitigation Methods

The development of Mobile IPv6 was intended to be as secure as Mobile IPv4. As IPv6 mobility support mainly involves the network layer in the OSI reference model, mitigation methods for securing Mobile IPv6 will be focused on layer 3. This section discusses the traditional security features for the mobile IPv6, especially on layer 3. As discussed in Section 1, the operation of Mobile IPv6 has been concerned with the issue of security, especially in the absence of authentication. Furthermore, the standard of Mobile IPv6 has specified the number of security features. This section discusses the provided security features in Mobile IPv6.

4.1. IP Security. As per what is standard with Mobile IPv6, there is the mandate of the usage of IPsec on securing the mobility support for IPv6, such as RFC 3775 and RFC 6275. The RFC 6275, as the latest standard of mobility support in IPv6, has been mandated to use IPSec for establishing security associations to assure the integrity and authenticity of mobility messages as important information [10]. The standard specifies the usage of IPSec by mandating the use of an ESP [89] header in transport mode. The ESP could authenticate the data origin, provide connectionless integrity, and replay attack protection.

However, as the IPSec involves certain protocols for its operation [90–92], it was not initially considered suitable for constrained devices in Mobile IPv6 such as a mobile phone [93–97]. This is because IPsec introduces high overhead and complex processing requirements [98]. Besides, as a generic authentication protocol, the integration of IPsec and IKE was purported to be exclusively for general computers [99]. It can be too high for low-end mobile devices that usually implement Mobile IPv6 [78].

Apart from computational complexity, the implementation of IPsec requires a global public key infrastructure (PKI). This is needed to support secure communication between any arbitrary pair of nodes, including mobile nodes with a different network. However, such a global PKI is not available today. Currently, the infrastructure of secure tunnels is established between an MN and its HA only as standardized in RFC 6275. Meanwhile, the IPSec covers the communication between an MN and any CN on the Internet. In addition, there is no infrastructure-based security currently available to authenticate all IPv6 nodes connected [25, 78].

According to Nikander et al. [79], the IPSec can be efficient in securing a communication path between MN and HA in forming a long-term connection. However, they indicated the IPSec might be inefficient in protecting short-term communication between an MN and its CN. In addition, the IPSec can be a burden in the case of a communication node having low power and limited computational quantities, such as Mobile IPv6. This is because of significant calculation costs executed by the IKE protocol as an integral part of IPSec. Therefore, the usage of the IPSec mechanism cannot provide a low-cost requirement that safely executes the BU.

This is supported by Faigl et al. [100], which reveals that the usage of IPSec on Mobile IPv6 signalling between MN and HA could cause overhead for mobility performance and large space requirements. They considered the queuing theory that involves the load-independent arrival rates and service times. It focuses on the signalling processes that utilize the overall resources of the HA by the Mobile IPv6.

4.2. RRP. As the IPsec introduces overhead and complex computation, as discussed previously, RRP [101] is proposed to be an alternative infrastructure-less security platform. It is used to authenticate the validity of the MN's address. Before receiving a BU message from the MN, the CN tests whether the HoA and CoA belonging to an MN are valid. In summary, there are four phases on the RRP as follows:

(1) The first phase, the MN sends a pairing message: HoTI and CoTI message, including two different nonces (N0 and N1) to the CN with a source address being its HoA and CoA, respectively.

(2) The second phase, after the CN receives the pair of messages, HoTI and CoTI, the CN replies with another pair of messages, HoT and CoT messages, respectively. The two messages also include nonces (H1 and C1) for use in generating the home keygen token K0 and care-of-keygen token K1, respectively. The calculation of K0 and K1 is as follows [101, 102]:

$$\mathrm{K0} = \mathrm{Hash}\,(\mathrm{KCN} \,|\, \mathrm{HoA} \,|\, \mathrm{HI} \,|\, 0), \tag{3}$$

$$\mathrm{K1} = \mathrm{Hash}\,(\mathrm{KCN} \,|\, \mathrm{CoA} \,|\, \mathrm{CI} \,|\, 1), \tag{4}$$

where Hash() designates a keyed hashing MAC scheme that uses the SHA1 hash function, KCN is a secret value that is only kept in CN, and the | denotes string concatenation.

(3) The third phase, once the MN has received the HoT and CoT with the keygen token, it creates a binding key (*Kbm*). The binding key is generated by computing the received concatenation of token SHA1(K0|K1). The MN then sends a BU message containing HI, CI, and MAC generated from MAC = Hash (*Kbm*, (CoA | CN's address| BU)).

(4) The CN engages in the last phase after receiving the BU message. It should verify the validity of the message by rebuilding the *Kbm* dynamically with the assistance of home and care-of nonce index HI and CI.

If the checking results are the same between the two *Kbm*, the CN then replies by sending back an acknowledgment message with MAC as in formula (5). Otherwise, the message will be discarded:

$$\mathrm{MAC} = \mathrm{Hash}\,(Kbm,\ (\mathrm{CoA} \,|\, \mathrm{CN's\ address} \,|\, \mathrm{BA})). \tag{5}$$

This RRP feature of Mobile IPv6 could limit potential attackers to those having specific access on the Internet, such as amplification and state exhaustion DoS attacks. It also avoids forged BU messages from anywhere on the Internet [10]. However, the RRP is not adequate for protecting the messages against attackers who are on the communication path between MN and CN. Furthermore, attackers in such locations connected by the Internet are potentially performing malicious activities. In addition, during the RRP, the two keygen tokens (K0 and K1) will be published to anyone that can receive the pair of test messages (CoT and HoT), including malicious nodes. Hence, an intruder can monitor the RRP to obtain the messages. Once they find the messages, they can forge CoTI to CN that will reply with CoT back to the MN. As a result, the RRP considerably suffers from the lack of strong security [102].

The authors in [78] elaborated shortcomings on RRP implementation when the attacker is on the critical path. It can launch impersonation attacks by eavesdropping on the returning HoT message. Furthermore, it can create its CoA keygen token as required in the RRP and then send a false CoA to the CN. The CN will assume the CoA comes from a legitimate MN and thus updates its binding cache based on the false CoA. The attacker on the path between MN and CN is also able to conduct flooding attacks. For instance, if the CN is an FTP server that provides some services, the attacker can request a large file to the CN using the victim's IP address. The CN then sends the large file to the victim resulting in DoS. These are considered limitations with the usage of RRP on securing Mobile IPv6, especially when it moves to a new location.

4.3. Improvements in Security Features on VHO. IPv6 is an ultimate solution to the problem of Internet address scarcity. In addition, Mobile IPv6 has become the only solution to provide mobile devices connectivity. This affects the growth of mobile technology. As a result, research on Mobile IPv6 security has garnered attention from researchers across the world. This section discusses several proposals for improving the security of mobile IPv6. The security improvements could be classified into two groups, which are infrastructure-based security and infrastructure-less improvements [25, 29]. Special security infrastructure is needed for the first group in order to protect the process of correspondent registration. In contrast, there is no security infrastructure needed for the latter and relies on the fundamental parts of the network infrastructure instead.

4.3.1. Infrastructure-Based Improvements. This group assumes that the handover mechanism on Mobile IPv6, especially with respect to the process of BUs, requires a particular security infrastructure. The first infrastructure-based improvement was put forth in [86] using a certificate to authenticate an MN and its CoA. The protocol was then called a certificate-based binding update (CBU). Message exchange in the CBU is shown in Figure 7.

As the CBU is an improvement of the RRP, the operations of CBU are also like the RRP operation. The HA is in the middle between the MN and CN, which makes it transparent to both nodes. The MN sends a request message, REQ containing the MN's CoA, the CN's IP address, and a nonce. The request message is sent to the CN to obtain a reply message (REP) from the CN. The HA in the middle creates a cookie and sends it to the CN. Upon receiving the cookie, the CN replies with another cookie containing its identity, HoA, the cookies identity, and a nonce. The HA sends message EXCH0 containing a public key certificate that is usually based on Diffie–Hellman algorithm. The MN then verifies the certificate and replies using its pairing message, EXCH1. Finally, the HA sends a CONFIRM message to the CN and, at the same time, sends a REP message to the MN.

However, the CBU has some disadvantages, as discussed in [29, 103]. As the CBU authenticates the MN and its CoA only, it does not address HoA certificate management. The scheme mandates its authenticating each of the home link subnet prefixes, and thus, the CN is not responsible for them. In the case where more subnet prefixes are on the home link, the authentication is not very practical. Another weakness is that the MN's claim the CN could not verify the CoA address. Furthermore, the attacker could transmit a fake address to it.

To address the CBU weaknesses, Ren [103] puts forward a Hierarchical Certificate-Based Binding Update protocol (HCBU). It improves the CBU by proposing a trust delegation. In terms of trust management, the HA in a roaming link signs the binding between HoA and CoA to prove the MN's CoA ownership. Both the signature and a valid subnet prefix certificate convince the MN's HA to make sure that the CoA belongs to the MN. Furthermore, the HA proves the binding by signing it through its private key. The HCBU message exchange is depicted in Figure 8.

There are six messages in the communication process proposed in HCBU that are divided into two groups separated by a dotted line: a prehandover and a posthandover process:

(1) Binding Update Request (BUReq) consists of a BU message, nonce, HoA, and CN address.

(2) Preinformation Exchange0 (EXCH0) contains a nonce, HoA, CN address, and g^x. The g^x is a Diffie–Hellman public value from the HA.

(3) Preinformation Exchange1 (EXCH1) contains the same contents with EXCH0 plus g^y, another Diffie–Hellman public value from the CN, and a generated cookie from CN.

(4) Care-of-address registration message to register a newly generated CoA after moving to another location (handover process).

(5) BU completion message is sent by the HA to the MN as well as to CN. It sends BUReq with a certified (HoA, CoA) to the CN and also sends a Binding Update Reply (BURep) to the MN containing a key (K_{BU}).

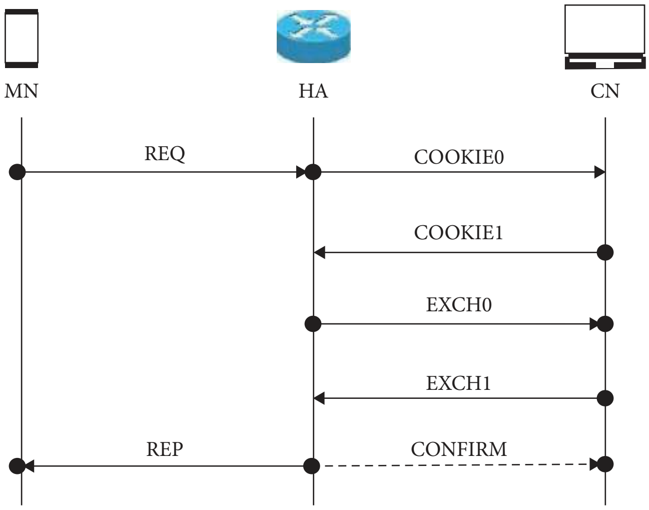

Figure 7: Message exchange in CBU.

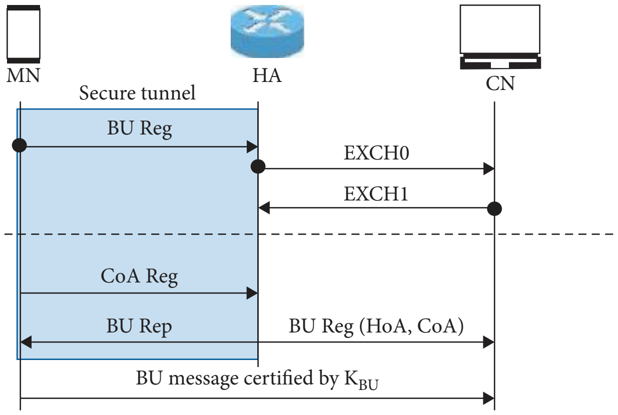

Figure 8: HCBU message exchange.

(6) Binding update message certified by the K_{BU} sent by the CN informing that it is still alive with the generated CoA.

As the HCBU is an improvement of CBU, it has the same advantages in enhancing security against malicious flooding attacks from third parties targeting the MN. However, owing to the division between prehandover and posthandover, it may be repeated several times, and this could increase signalling overhead. Adding more messages that should be forwarded by the HA as well as covering roaming MNs from other links make the HA busy with respect to conducting its original task [29].

The authors in [104] evaluated the HCBU scheme as an improvement of the CBU scheme. It was reported that the HCBU requires the use of trusted third parties to verify CoAs. The MNs and their infrastructure need them to support the authentication service. In addition, the MN might require replicating the prehandover phase continuously; hence, it will increase the signalling overhead of the registration message sequence.

In terms of computational complexity, the HCBU protocol requires computing a large amount of computation for MN, CN, and the HA. The MN must conduct four hashing functions, symmetric encryption, one exponentiation, and one signature generation. The CN should perform two hashing functions, one exponentiation, and one symmetric decryption. Finally, the HA should perform one signature generation, three hashing functions, and two exponentiations [105].

Koo et al. [106] proposed a Ticket Binding Update (TBU) as an enhancement of RRP. In this scheme, the HA generates a secret key and ticket with the CN instead of the MN. It is assumed that the connection can establish a secure tunnel using IPsec. The ticket is used to assist the BU generation whenever the MN requires a BU message for the future efficiently. Furthermore, equal BU need not be repeated when the MN moves to a foreign network. The communication between MN and the future CN is shown in Figure 9.

There are two messages in Figure 9: the first message is directly transmitted by the MN to the CN containing a security parameter (Cookie_1) to the message to filter attacks. This message is a BU sent to register a new CoA. The message also carries a ticket $\text{Tck}_{\text{MN-CN}}$ to establish mutual authentication. The second message is a BA message as an acknowledgment of the first message. After receiving the BU message, the CN checks it to validate Cookie_1 and the ticket. If the checking result is positive, the CN updates its binding cache by adding the valid information and sends the BA message that includes another security parameter Cookie_2. The TBU uses a timestamp (T_{MN} and T_{CN}) for recognizing the replying message that requests a fully synchronized clock between the two communication nodes (MN and CN).

However, this protocol is still open to flooding attacks targeting the CN by sending more BU messages to force it to check each received message. This may cause the CN to deny its services. An improvement of TBU was proposed in [107] named ETBU (Extended Ticket Binding Update). As an enhancement of the TBU, this protocol extended the address configuration using Cryptographically Generated Address (CGA). The CGA is used to provide mutual authentication between the CN and MN when entering a new network.

The difference between the proposed ETBU protocol and previous CGA-based BU protocol in [102] is ETBU does not need to create a signature each time by a CN when obtaining a new CoA. As the CGA is a heavy computational algorithm, the MN and its CN issue a ticket to minimize computing costs. In addition, the ETBU protocol implements a smooth handoff or handover that can minimize the loss of network traffic. The author asserted that the performance analysis of the protocol shows that it is more efficient than the original TBU but provides the same security function.

Secure Route Optimization Protocol (SROP) was proposed in [87] to provide authentication during the connection establishment in Mobile IPv6 handover. The authentication is conducted using ESP by developing an SROP initial exchange. A security association is also established for the secure connection. To do this, the SROP protocol uses several SROP messages. An SROP UPDATE message containing a LOCATOR parameter is sent by the MN to notify the CN that it has generated a new CoA. The MN needs to ensure the reliability of the CoA by sending an UPDATE message. The message will be authenticated by the CN based on the signature and keyed hash of the message. When the message is valid, the CN could then send an IPv6 packet to the new CoA.

Kavitha et al. [87] commented that the SROP protocol is considered an initial step in the migration from mobile IP-based networks to public key-based future networks. This means the SROP protocol does not adequately protect Mobile IPv6 communication from various attacks. As the SROP protocol uses ESP as part of IPSec for its authentication, the weakness of IPSec is also a limitation of SROP.

The enhancement of security and authentication in RRP was also proposed in [108]. The approach is referred to as Return Routability Identity-Based Encryption (RR-IBE) protocol. The IBE that is used in this method requires a third party to distribute keys (i.e., Private Key Generator (PKG)). The keys are distributed to all senders simultaneously. The sender requires the identity of the receiver in order to engage in the communication. The results of the simulation and verification of the proposed method using a Murphi model checker has strong security. The attacks on return routability have been addressed by this method.

However, as RR-IBE requires a third party to generate and distribute the private keys, this method introduces a high latency owing to the usage of an infrastructure-based PKG. In addition, it causes the repetition of message exchanges between the communicants [109] because of the distribution of keys to all senders. This causes major bandwidth consumption. According to this mechanism, the HA will possibly not authenticate the CoA sent by the MN. This is because the MN might recline from its current position. Furthermore, it will entice the HA to transmit traffic to a third party that could cause a DoS attack [104].

The latest proposal on securing RRP enhancement is Certificate Less-Public Key Encryption (CLPKE) [110]. With this mechanism, both the latest location and new location informs the HA or CN. A message used by the MN includes its current CoA and the old CoA. All the messages transmitted in this mechanism contain a nonce that is encrypted using Certificate Less-Public Key Encryption. The authors claimed the mechanism provides confidentiality, integrity, authentication, and possible attack preventions. In addition, it uses a few messages that can reduce computation time significantly. Furthermore, it provides less costly BU message communication when compared to RR-IBE. Even though this protocol uses a trusted third party known as a Key Generation Centre (KGC), the third party does not have access to the private key as in RR-IBE. Instead, it supplies the entity with a partial private key. The messages needed in this protocol are shown in Figure 10.

M1 is a HOTI message from the MN to the HA that is then forwarded as HOTI' ($M1'$) to the CN. The M1 includes a message with the old CoA address of the MN ($\text{MN}_{\text{OldCoA}}$) to inform the HA or CN of the MN's preceding location. Both M1 and $M1'$ contain a nonce (N0). The MN will then compare the nonce value of M1 and M1'. If the value of N0 is

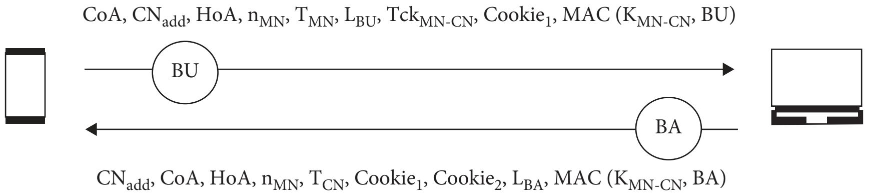
CoA, CN_{add}, HoA, n_{MN}, T_{MN}, L_{BU}, $Tck_{MN\text{-}CN}$, $Cookie_1$, MAC ($K_{MN\text{-}CN}$, BU)
BU
BA
CN_{add}, CoA, HoA, n_{MN}, T_{CN}, $Cookie_1$, $Cookie_2$, L_{BA}, MAC ($K_{MN\text{-}CN}$, BA)

Figure 9: Communication between MN and future CN.

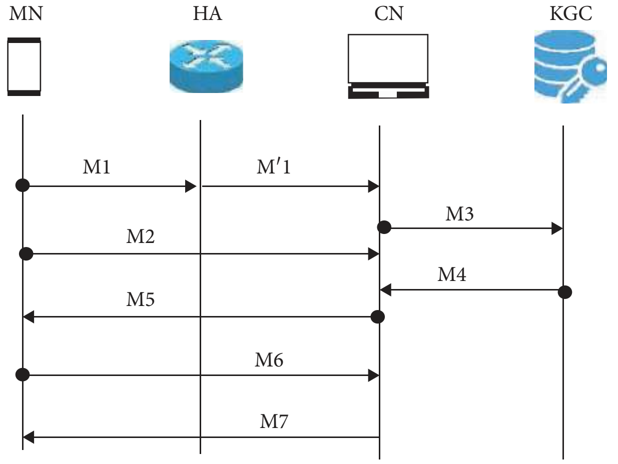

Figure 10: Message exchange on CLPKE.

the same in both, then CN sends a partial private key request to the KGC (M3). Otherwise, it will discard them.

At the same time of sending M1, the MN sends M2 (COTI) to the CN to inform its CoA. The KGC responds to the request by sending M4. Using the partial private key, the MN could authenticate the MN (M5). Finally, the MN sends a BU message (M6) to the CN and gets a reply (M7) from the CN. Table 1 summarizes the infrastructure-based security.

4.3.2. Infrastructure-Less Improvements. Infrastructure-based improvement requires some resources and configuration work to run the security improvement. In addition, the infrastructure-based security approach requires an additional message exchange that potentially increases the complexity of the mobile device as well as other related mobility agents [104]. In order to avoid the need for additional security infrastructures, several researchers have posited an infrastructure-less security approach for Mobile IPv6. This section summarizes the proposal and its performance.

An experimental implementation of CAM (Child-Proof Authentication for MIPv6) was conducted at Lancaster University [111]. The CAM protocol uses a hash function to facilitate correspondence with the generated key pair at the initialization phase of the MIPv6 node. The usage of the hash function that satisfies the hash function requirements (one-way and collision resistance) could defend against falsification attacks. However, the protocol cannot ensure MN node reliability, and it also cannot protect against DoS attacks or flooding attacks without any other security mechanisms [29].

The MN is usually a low energy node as it is not connected to a power source every time. Therefore, there is a need for a lightweight RR procedure as well as its security mechanism. The authors in [102] proposed an efficient RR scheme based on a lesser number of hash functions and simple geometric computations. In this scheme, no verification table is required in the MN and thus eliminates the maintenance of the nonce table. This scheme claimed it can assure the protection from replay attacks, eavesdropping attacks, exhausting resource attacks, location authentication, and modification attacks.

A context-aware ticket-based binding update authentication (caTBUA) protocol was proposed in [112]. It considers a balance between efficiency and security by using context information to validate an appropriate CoA dynamically. The primary context information includes the following:

(1) Trust degree of MN: it is estimated by the HA to obtain information about the MN's trust level. This information is included in the MN's ticket that is transferred to the CN.

(2) Trust degree of HA: this signifies the HA's trust level. This information is obtained from the previous trust relationship established between the HA and CN.

(3) Foreign network's trust level: this information represents the trust level of the foreign network where the MN is currently located. It is determined based on the previous trust relationship established between the CN and access router (AR) in the MN's current visiting network.

(4) Requested time: this information contains request time inside the MN's BU message.

There are two phases of the caTBUA protocol, which are ticket issue and context-aware BU. The ticket issue phase is performed at the first CN registration only. The context-aware phase is initiated by the MN by sending an Early Binding Update (EBU) message [113] to the CN. In this case, the MN attached at a foreign network that the AR has an existing trust relationship within terms of CN, and it sends a key (*Kac*) to the CN together with the EBU message.

In order to validate the proposal, the authors utilized numerical analysis to evaluate the performance of caTBUA. The evaluation was conducted by comparing the proposed method with the existing authentication protocols in terms of authentication cost and authentication message transmission latency. The results of the evaluation have confirmed that the caTBUA protocol outperforms the existing BU authentication protocols.

An enhancement of RRP was also proposed in [88] that suggested using an identity-based framework (identity-based scheme). This protocol was proposed to enhance the security of the RRP in MIPv6 without compromising the performance of mobile nodes. It includes two security primitives: encryption and signature. The encryption mechanism is used to encrypt the HoT and CoT as the response of HoTI and CoTI. These two messages include significant parameters used to extract the binding management key (Kbm), whereas the signature scheme is utilized to sign the initial messages from the MN (HoTI and CoTI). Both encryption and signature mechanisms could ensure two-way origin authentication. However, the level of security comparison is required to analyse security performance.

An authentication scheme based on the Diffie–Hellman (DH) key was also put forth in [114]. It employs the signalling on a low-layer level to exchange DH variables. This mechanism allows mobility service-provisioning entities to exchange an MN's profile securely. The authors claimed by utilizing the low-layer signalling and context transfer between relevant nodes, and the DH authentication scheme could minimize the authentication latency when the MN moves across different networks as well as does a handover. The advantage of the usage of the DH key is avoiding preestablished SAs between mobility service-provisioning entities. However, it was determined this scheme is vulnerable to DoS, MITM, and false BU attacks [115].

The authors in [104] proposed a registration scheme with a symmetric key approach referred to as the Secure and Decentralized Registration (SDR) scheme. It is involved in security with the MIPv6 environment consisting of MN, HA, and CN. It contributed to securing communication and mutual authentication using a shared key mechanism. The registration is conducted using two phases: home registration and correspondent registration. The SDR registration scheme is portrayed in Figure 11.

The steps of HR1 to HR4 are used in the home registration, and CR1 to CR4 are employed in correspondent registrations. The authors highlighted that the three security parameters (confidentiality, integrity, and authentication) are satisfied by the SDR scheme. This was verified using a Murphi model checker and finite state machine. The verification confirmed that the method was able to defend against the rerun attack, false BU message, and MiTM attack.

A PKBU (private key-based binding update) protocol was proposed by Modares [115]. In this scheme, the authenticity of the MN's HoA and CoA ownership is required by the CN. Furthermore, it should enable the verification mechanism. The HA will be sent a confirmation message to the CN informing that the MN is the correct owner of the HoA. At this moment, the MN is connected via the CoA. It uses the interface ID part of IPv6 address (last 64 bits) to provide a cryptographic binding between the CN and the MN. The binding could be used to verify the ownership of the HoA. Once the HoA has been verified, the MN signs the encrypted CoA using the CN's public key and the HoA using its private key Algorithm 1.

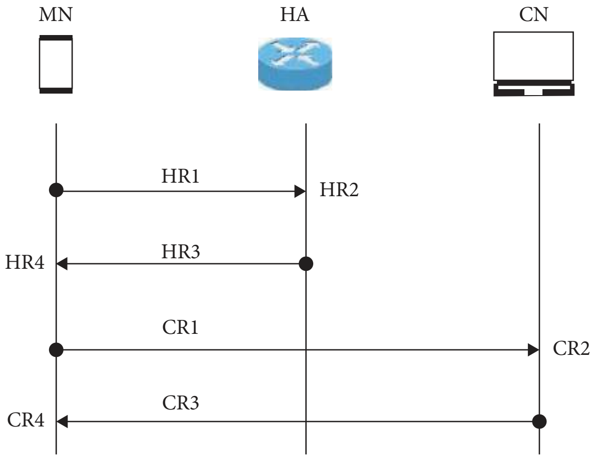

Figure 11: SDR registration scheme.

The PKBU protocol starts with phase 1 consisting of three steps to verify the ownership of the MN's address. Address ownership is assured by creating a private key, public key, and the MN's interface ID. The MN generates the private key based on the user ID hash value. It is considered secured as it cannot be guessed by the attacker. The public key is generated by the MN using the elliptic curve cryptography (ECC) method. As discussed in [116, 117], the ECC method was selected owing to its efficiency, consumption of less power, and faster computation. The last step of phase 1 is IPv6 address generation, including the 64 bit interface ID. The interface ID part is configured from the MN's private key hash value that creates a solid cryptographic binding between the ID and its private key.

In phase 2, the MN checks the reachability of the CN by sending a message containing its HoA, its public key, and a request for the CN's public key. Upon receiving the message, the CN replies by sending its public key. The process is carried out in three steps: combining the MN's CoA and HoA, encrypting the message using the CN's public key, and signing the message using a digital signature. Phase 3 consists of four steps pertaining to the validation process at the CN. It verifies the correctness of the HoA and CoA received from the MN. It uses the MN's public key to authenticate the MN's signature. If the checking process resulted in a positive value, the CN then sends the BA to the CN. Otherwise, the message will be discarded.

The latest method was proposed in [109] that is an enhancement of location update. It is completed by incorporating the optimal asymmetric encryption (OAE) based on the random oracle model to provide both security and efficiency. This method assumes that a preshared SA will be established by the pairs of MN-HA and MN-CN. The proposal consists of three parts: generating CoA, BU scheme between the MN and HA, and BU scheme between the MN and CN that can be summarized as follows.

(1) Generation of CoA. After moving to a new location, an MN will generate a new CoA. In this scheme, the MN generates the 64 bit interface ID by computing the hash-

```
Phase 1:
  Step 1: create a private key
  Step 2: create a public key
  Step 3: create an interface ID
Phase 2:
  Step 1: combine MNHoA and MNCoA
  Step 2: encrypt the message using CN public key
  Step 3: use a digital signature to sign the message
Phase 3:
  Step 1: authenticate the signature
  Step 2: confidentiality of data
  Step 3: integrity of data
  Step 4: ownership and reachability
```

Algorithm 1: There are three phases in the protocol as follows [115].

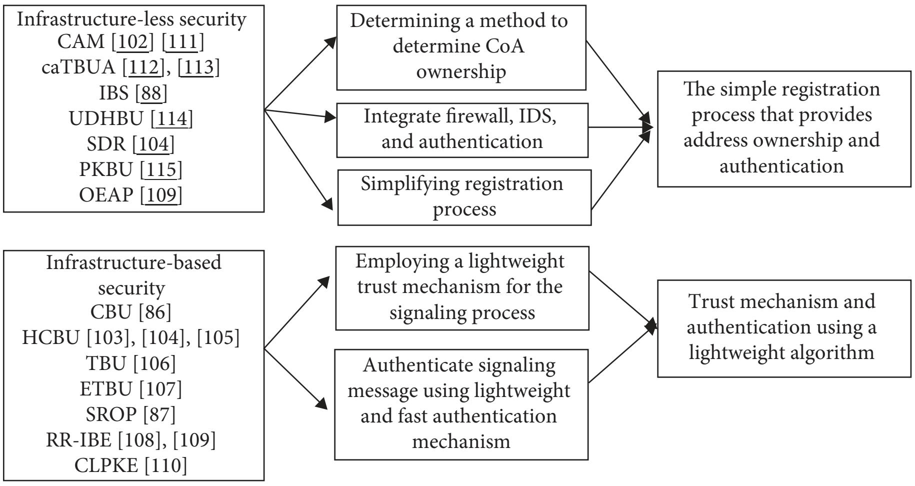
Infrastructure-less security
CAM [102] [111]
caTBUA [112], [113]
IBS [88]
UDHBU [114]
SDR [104]
PKBU [115]
OEAP [109]
Determining a method to determine CoA ownership
Integrate firewall, IDS, and authentication
Simplifying registration process
The simple registration process that provides address ownership and authentication
Infrastructure-based security
CBU [86]
HCBU [103], [104], [105]
TBU [106]
ETBU [107]
SROP [87]
RR-IBE [108], [109]
CLPKE [110]
Employing a lightweight trust mechanism for the signaling process
Authenticate signaling message using lightweight and fast authentication mechanism
Trust mechanism and authentication using a lightweight algorithm

Figure 12: Future research direction on improving MIPv6 vertical handover security.

based message authentication code algorithm. In this case, HMAC-SHA1 serves as the communication between the node in the mobility environment and the so-called K-CGA procedure. This procedure uses the principle of CGA address generation as standardized in [118].

(2) BU between MN and HA. In this part, the MN sends the BU message to register its current location with HA. The message is encrypted using the MN's public key with an OAEP field containing two cryptographic hash functions. The HA decrypts the message using its private key and extracts the OAEP field. It then verifies the field by computing the hash value and compares it with that obtained in the OAEP field. If the result does not match, the HA discards the message; otherwise, the HA replies by sending an encrypted message with an OAEP field.

(3) BU between MN and CN. The third part is a BU between the MN with the CN. As in the second part, the MN sends a BU message to the CN using a similar message with that sent to the HA, which is a BU message with the OAEP field.

As this proposal is an infrastructure-less scheme, it involves fewer security computations than the other BU schemes. The author claimed this method provides confidentiality as well as data integrity services by implementing asymmetric encryption and a hash function. It also provides authentication by using the HMAC mechanism. In addition, it provides security defending from several attacks, including replay attacks, MiTM attacks, and false BU attacks. However, as this method uses CGA in the generation of CoA as well as an encryption mechanism, this introduces demanding computational work.

Furthermore, the attacker could send many messages to create a DoS attack. In addition, the design of a BU scheme for distributed IP mobility (compatible architecture) with all correspondent nodes, including those that do not support route optimization, is a point of further research. Table 2 lists the summary of infrastructure-less security for MIPv6 VHO.

From the previous discussion on both infrastructure-less security and infrastructure-based security, each has weaknesses. This could drive the next research direction, as depicted in Figure 12. The block diagram shows there are two future research avenues for improving security on MIPv6 VHO. Future research could be carried out to find a simple registration process that provides address ownership and a lightweight authentication algorithm.

Table 1: Summary of infrastructure-based security.

Infrastructure-based security	Basic operations	Main strength	Main weakness
CBU [86]	Authenticate an MN and its CoA using a certificate	Public key certificate uses Diffie–Hellman algorithm	It does not address the HoA certificate management
HCBU [103–105]	Trust delegation	Enhancing security against malicious flooding attacks	Signalling overhead
TBU [106]	The ticket is used to assist BU generation	Fully synchronized clocks between the two communication nodes	Open to flooding attacks targeting the CN
ETBU [107]	The address generated using CGA	It minimizes the loss of network traffic	Heavy calculation
SROP [87]	Authentication based on the signature and keyed hash of the message	A security association is also established for the secure connection	Does not fully protect Mobile IPv6 communication from various attacks
RR-IBE [108, 109]	The keys are distributed to all senders simultaneously	The attacks in return routability have been addressed by this method	Introduces a high latency based on the usage of an infrastructure-based PKG
CLPKE [110]	Both the latest location and new location is informed to the HA or CN	Providing less cost of BU messages	This protocol requires trusted third party

Table 2: Summary of infrastructure-less security.

Infrastructure-less security	Main operation	Main strength	Main weakness
CAM [102, 111]	Correspondence with the generated key pair at the initialization phase	Defence against falsification attack	The protocol cannot ensure MN node reliability
caTBUA [112, 113]	Using context information to validate an appropriate CoA dynamically	It outperforms the existing BU authentication protocols	Requires more information to build the context
IBS [88]	It includes two security primitives: encryption and signature	Ensures two-way origin authentication	Requires comparing levels of security
UDHBU [114]	It utilizes the signalling on a low-layer level to exchange DH variables	It does not require having preestablished SAs between relevant MAGs	Vulnerable to DoS, MITM, and false BU attacks
SDR [104]	Home registration and correspondent registration	Defence against rerun attack, false BU message, and MiTM attacks	The registration requires time
PKBU [115]	Provide a cryptographic binding between the CN and MN	The address ownership is assured	It does not cover the CoA ownership
OEAP [109]	Incorporating the OAE based on the random oracle model to provide both security and efficiency	Involves fewer security computations than the other BU schemes	Introduces high computational work

5. Conclusion

Mobile IPv6 is an ultimate solution to the IP address problem assigned to mobile technology as it has many advantages, especially its large address structure. However, it is vulnerable to various malicious activities owing to the natural character of the Internet as an open network. Furthermore, security of an Internet protocol should be given more attention from researchers. As discussed before, even though there were many security mechanisms proposed on securing the Mobile IPv6 handover mechanism, malicious attacks still cannot be neglected. This section elaborates on certain future challenges as well as additional work on the discourse of security on Mobile IPv6 vertical handover that could be integrated with the research direction depicted in Figure 12.

5.1. Integrating Security and Performance. Security is a necessary need for Mobile IPv6 VHO. However, all security mechanisms usually impact network performance. Generally, a security mechanism adds some security features to the original network transmission that could increase network overhead. It could be adding an algorithm cryptographically for both on IPv6 packets as well as the machine involved in the protection. The extension security features may reduce network performance and, at the same time, consume more energy to process it. Hence, optimal security and network performance is a challenge to researchers. For Mobile IPv6 that uses limited energy, the integration of security requirements and performance should be considered to save machine energy and other resources.

5.2. Mixed Attacks in VHO. As known, the Internet is an open network that can be accessed by anyone in the world. This allows malicious users to engage in harmful activities, such as launching malicious messages as well as worms. As discussed, there are many types of attacking activities that could be used by the attacker to steal user resources. The proposed security mechanism may address one or two attacks, as in Tables 1 and 2. However, if many attackers perform various attacking activities at one time, it may make it challenging to address. Furthermore, a mixed attack on Mobile IPv6 VHO requires attention from researchers.

5.3. Lower Layer Security. Mobile IPv6 works on the network layer of the OSI reference model. However, layer 3 does not work alone, and it is only a part of the networking model. All network traffic should flow through the lower layer. From a security point of view, the attackers may exploit attacking activities via the lower layer. Furthermore, attention to lower layer security should be paid.

Data Availability

The data supporting this systematic survey are from previously reported studies and datasets, which have been cited.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was funded by the Directorate of Higher Education, Ministry of Education and Culture, Republic of Indonesia.

References

[1] Internet World Stats, 2019, http://www.internetworldstats.com/.

[2] I. T. D. Bureau, *International Telecommunication Union*, ICT Facts and Figures, Boston, London, 2017.

[3] J. Márquez-Barja, "An overview of vertical handover techniques: algorithms, protocols and tools," *Computer Communications*, vol. 34, no. 8, pp. 985–997, 2011.

[4] X. Lin, "An overview of 3GPP device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. No. 4, pp. 40–48, 2014.

[5] B. G. Lee and S. Choi, *Broadband Wireless Access and Local Networks: Mobile WiMAX and WiFi*, Artech House, Boston, London, 2008.

[6] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-advanced for Mobile Broadband*, Academic Press, Burlingto, USA, 2013.

[7] S. Busanelli, "Vertical handover between WiFi and UMTS networks: experimental performance analysis," *International Journal of Energy, Information and Communications*, vol. 2, no. 1, pp. 75–96, 2011.

[8] J. Manner and M. Kojo, "Mobility related terminology," *RFC 3753*, vol. 2, 2004.

[9] L. Zhang, L. J. Zhang, and S. Pierre, "Performance analysis of seamless handover in mobile IPv6-based cellular networks," in *Proceedings of the InTech, Cellular Networks-Positioning, Performance Analysis*, Burlingto, USA, 2011.

[10] C. Perkins, D. Johnson, and J. Arkko, "Mobility support in IPv6," *RFC 6275*, vol. 2, 2011.

[11] S. Praptodiyono, RK. Murugesan, IH. Hasbullah, CY. Wey, MM. Kadhum, and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," in *Proceedings of the ICACOMIT*, pp. 31–36, Bandung, Indonesia, 2015.

[12] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," *RFC 8200*, vol. 2, 2017.

[13] J. Postel, "Transmission control protocol," *RFC 793*, vol. 2, 1981.

[14] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," *RFC 3775*, vol. 2, 2004.

[15] C. Perkins, P. Calhoun, and J. Bharatia, "Mobile IPv4 challenge/response extensions (revised)," *RFC 4721*, vol. 2, 2007.

[16] Y. Zou, "A survey on wireless security: technical challenges, recent advances, and future trends," *IEEE*, vol. 104, pp. 1727–1765, 2016.

[17] S. Lakshmanan, CL. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proceedings of the. International Conference on Distributed Computing Systems ICDCS'08*, pp. 19–27, Bandung, Indonesia, 2008.

[18] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008.

[19] B. Kannhavong, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Communications*, vol. 14, no. 5, 2007.

[20] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, ACM, New York, NY, USA, 2004.

[21] T. Ohigashi and M. Morii, "A practical message falsification attack on WPA," *JWIS*, vol. 14, 2009.

[22] S. Norton, "Norton cyber security insights report," 2016.

[23] T. Aura, "Mobile IPv6 security," *Presented at International Workshop on Security Protocols*, Springer, Berlin, Germany, 2002.

[24] S. Hogg and E. Vyncke, *IPv6 Security*, Pearson Education, Indianapolis, USA, 2008.

[25] T. Aura and M. Roe, "Designing the mobile IPv6 security protocol," *Annales des Télécommunications*, Springer, pp. 332–356, Berlin, Germany, 2006.

[26] M. Alnas, I. Awan, and R. D. W. Holton, "Performance evaluation of fast handover in mobile IPv6 based on link-layer information," *Journal of Systems and Software*, vol. 83, no. 10, pp. 1644–1650, 2010.

[27] L. Wang and G.-S. G. S. Kuo, "Mathematical modeling for network selection in heterogeneous wireless networks - a tutorial," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 271–292, 2013.

[28] S. Wang, C. Fan, C.-H. Hsu, Q. Sun, and F. Yang, "A vertical handoff method via self-selection decision tree for internet of vehicles," *IEEE Systems Journal*, vol. 10, no. 3, pp. 1183–1192, 2016.

[29] H. Modares, A. Moravejosharieh, J. Lloret, and R. Salleh, "A survey of secure protocols in mobile IPv6," *Journal of Network and Computer Applications*, vol. 39, pp. 351–368, 2014.

[30] S. K. Mathi and M. L. Valarmathi, "A secure and efficient binding update scheme with decentralized design for next generation IP mobility," in *Proceeding of the Artificial Intelligence and Evolutionary Algorithms in Engineering Systems*, Springer, pp. 423–431, New Delhi, India, 2015.

[31] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," 2007.

[32] J. Zhang, J. Liu, Z. Xu, J. Li, and X. M. Ye, "TRDP: a trusted router discovery protocol," *International Symposium on*

Communications and Information Technologies, vol. 39, pp. 660–665, 2007.

[33] S. Thomson, T. Narten, and T. Jinmei, "IPv6 stateless address autoconfiguration," *RFC 4862*, vol. 39, 2007.

[34] H. Soliman, *Mobile IPv6: Mobility in a Wireless Internet*, Addison-Wesley Profesional, Texas, USA, 2004.

[35] L. Burness, P. Eardley, J. Eisl, R. Hancock, E. Hepworth, and A. Mihailovic, "Efficient alternatives to bi-directional tunnelling for moving networks," in *Proceedings of the International Conference on Telecommunications*, Springer, pp. 1128–1135, Berlin, Heidelberg, 2004.

[36] D. Le and J. Chang, "Tunnelling-based route optimization for mobile IPv6," in *Proceedings of the 2010 IEEE International Conference on Wireless Communications, Networking and Information Security*, IEEE, pp. 509–513, Berlin, Heidelberg, 2010.

[37] R. Koodli and C. Perkins, "Mobile IPv6 fast handovers," *RFC 5568*, vol. 39, 2009.

[38] J. Arkko, W. Haddad, and C. Vogt, "Enhanced route optimization for mobile IPv6," *RFC 4886*, vol. 39, 2007.

[39] F. Johansson, "Route optimization technique for mobile IP," 2008.

[40] C. E. Perkins and D. B. Johnson, "Route optimization for mobile IP," *Cluster Computing*, vol. 1, no. 2, pp. 161–176, 1998.

[41] M. H. Masud, F. Anwar, O. M. Mohamed, S. M. S. Bari, and A. F. Salami, "A parallel duplicate address detection (pdad) mechanism to reduce handoff latency of mobile internet protocol version 6 (mipv6)," in *Proceedings of the 2011 4th International Conference on Mechatronics (ICOM)*, IEEE, pp. 1–6, Berlin, Heidelberg, 2011.

[42] S. Praptodiyono, I. H. Hasbullah, M. M. Kadhum, C. Y. Wey, R. K. Murugesan, and A. Osman, "Securing duplicate address detection on IPv6 using distributed trust mechanism," *Computer Communications*, vol. 17, no. 26, 2016.

[43] B. K. Kim, Y. C. Jung, I. Kim, and Y. T. Kim, "Enhanced FMIPv4 horizontal handover with minimized channel scanning time based on media independent handover (MIH)," in *Proceedings of the NOMS Workshops 2008-IEEE Network Operations and Management Symposium Workshops*, IEEE, pp. 52–55, Berlin, Heidelberg, 2008.

[44] A. Dhiman and K. S. G. Sandha, "Vertical and horizontal handover in heterogeneous wireless networks," 2013.

[45] M. Kassar, B. Kervella, and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," *Computer Communications*, vol. 31, no. 10, pp. 2607–2620, 2008.

[46] N. Rajule, B. Ambudkar, and A. Dhande, "Survey of vertical handover decision algorithms," *International Journal of Innovations in Engineering and Technology*, vol. 2, no. 1, pp. 362–368, 2013.

[47] N. Montavont and T. Noel, "Handover management for mobile nodes in IPv6 networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 38–43, 2002.

[48] M. H. Masud, "Vertical handoff reduction mechanism using IEEE 802.21 standard in mobile IPv6 (MIPv6) network," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 13, no. 6, p. 76, 2013.

[49] I. Chattate, J. Bakkoury, A. Khiat, and M. El Khaili, "Overview on technology of vertical handover and MIH architecture," in *Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, Berlin, Heidelberg, 2016.

[50] Y.-H. Han and S.-H. Hwang, "Movement detection analysis in mobile IPv6," *IEEE Communications Letters*, vol. 10, no. 1, pp. 59–61, 2006.

[51] E. Nordmark and I. Gashinsky, "Neighbor unreachability detection is too impatient," 2011.

[52] R. Radhakrishnan, M. Jamil, and S. Mehfuz, "A robust return routability procedure for mobile IPv6," *International Journal of Computer Science and Network Security*, vol. 8, pp. 234–240, 2008.

[53] M. Baushke, "More modular exponentiation (MODP) Diffie-hellman (DH) key exchange (KEX) groups for secure shell (SSH)," 2017.

[54] Y.-H. Han and S.-H. Hwang, "Analysis of movement detection process for IPv6 mobile nodes," in *Proceedings of the International Workshop on Mobile Agents for Telecommunication Applications*, Springer, Berlin, Heidelberg, 2005.

[55] J. Carmona-Murillo, J. L. G. Sánchez, and I. Guerrero-Robledo, "Handover performance analysis in mobile IPv6-A contribution to fast detection movement," *WINSYS*, vol. 8, 2008.

[56] N. Ineke, C. Wangi, R. V. Prasad, M. Jacobsson, and I. Niemegeers, "Address autoconfiguration in wireless ad hoc networks: protocols and techniques," *IEEE Wireless Communications*, vol. 15, no. 1, pp. 70–80, 2008.

[57] R. Droms, *DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6*, DHCPv6), New York, NY, USA, 2003.

[58] S. Praptodiyono, I. Hasbullah, M. Kadhum, R. Murugesan, C. Wey, and A. Osman, "Improving security of duplicate address detection on IPv6 local network in public area," *AMS*, vol. 8, 2015.

[59] G. I. Daley, *Strategies for Detecting Network Attachment in the All-IPv6 Wireless and Mobile Internet*, Monash University, New York, NY, USA, 2007.

[60] B. J. Chang and S. Y. Lin, "Mobile IPv6-based efficient vertical handoff approach for heterogeneous wireless networks," *Wireless Communications and Mobile Computing*, vol. 6, no. 5, pp. 691–709, 2006.

[61] B. R. Chandavarkar and G. R. M. Reddy, "Survey paper: mobility management in heterogeneous wireless networks," *Procedia Engineering*, vol. 30, pp. 113–123, 2012.

[62] R. Chakravorty, P. Vidales, K. Subramanian, I. Pratt, and J. Crowcroft, "Performance issues with vertical handovers-experiences from GPRS cellular and WLAN hot-spots integration," in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications*, IEEE, Berlin, Heidelberg, 2004.

[63] D. Celentano, "Secure mobile IPv6 for mobile networks based on the 3GPP IP multimedia subsystem," 2007.

[64] R. Koodli, "Fast handovers for mobile IPv6," *RFC 4068*, vol. 30, 2005.

[65] R. Koodli, "Mobile IPv6 fast handovers," *RFC 5268*, vol. 30, 2008.

[66] R. Koodli, "Mobile IPv6 fast handovers," *RFC 5566*, vol. 30, 2009.

[67] T. Ghebregziabher, "Security analysis of flow-based fast handover method for mobile IPv6 networks," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications AINA'06*, IEEE, Berlin, Heidelberg, 2006.

[68] M. Sulander, "Flow-based fast handover method for mobile IPv6 network," in *Proceedings of the 2004 IEEE 59th Vehicular Technology Conference*, IEEE, Berlin, Heidelberg, 2004.

[69] A. Viinikainen, J. Puttonen, M. Sulander, T. Hämäläinen, T. Ylönen, and H. Suutarinen, "Flow-based fast handover for mobile IPv6 environment-implementation and analysis," *Computer Communications*, vol. 29, no. 16, pp. 3051–3065, 2006.

[70] H. Soliman, L. Bellier, and K. E. Malki, "Hierarchical mobile IPv6 mobility management (HMIPv6)," *RFC 4140*, vol. 29, 2005.

[71] H. Soliman, K. ElMalki, L. Bellier, and C. Castelluccia, "Hierarchical mobile IPv6 mobility management," *RFC 5380*, vol. 29, 2008.

[72] D. Thaler, M. Talwar, and C. Patel, "Neighbor discovery proxies (ND Proxy)," *RFC 4389*, vol. 29, 2014.

[73] S. Ryu, K.-J. Park, and J.-W. Choi, "Enhanced fast handover for network mobility in intelligent transportation systems," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 357–371, 2014.

[74] J. Lundberg, "An analysis of the fast handovers for mobile ipv6 protocol," in *Proceedings of the Mobile Networks Based on IP Protocols and Unlicensed Radio Spectrum Seminar on Internetworking*, Berlin, Heidelberg, 2003.

[75] R. Li, "An enhanced fast handover with low latency for mobile IPv6," *IEEE Transactions on Wireless Communications*, vol. 7, no. 1, 2008.

[76] A. Safa Sadiq, "Advanced mobility handover for mobile ipv6 based wireless networks," *The Scientific World Journal*, vol. 7, 2014.

[77] C.-W. Wu and P. Wang, "Improved fast handover scheme for hierarchical mobile ipv6," in *Proceedings of the 4th International Conference on Computer Science & Education ICCSE'09*, Berlin, Heidelberg, 2009.

[78] K. Elgoarany and M. Eltoweissy, "Security in mobile IPv6: a survey," *Information Security Technical Report*, vol. 12, no. 1, pp. 32–43, 2007.

[79] P. Nikander, J. Kempf, and E. Nordmark, "IPv6 neighbor discovery (ND) trust models and threats," *RFC 3756*, vol. 12, 2004.

[80] J. Supriyanto, "Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods," *IETE Technical Review*, vol. 30, no. 1, pp. 64–71, 2013.

[81] A. S. A. M. S. Ahmed, R. Hassan, and N. E. Othman, "IPv6 neighbor discovery protocol specifications, threats and countermeasures: a survey," *IEEE Access*, vol. 5, pp. 18187–18210, 2017.

[82] A. Moravejosharieh, H. Modares, and R. Salleh, "Overview of mobile IPv6 security," in *Proceedings of the Third International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, Berlin, Heidelberg, 2012.

[83] K. Cheng, M. Gao, and R. Guo, "Analysis and research on HTTPS hijacking attacks," in *Proceedings of the Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC)*, Berlin, Heidelberg, 2010.

[84] K. Kalajdzic and A. Patel, "Active detection and prevention of sophisticated ARP-poisoning man-in-the-middle attacks on switched Ethernet LANs," in *Proceedings of the 6th International Workshop Digit, Forensics Incident Anal (WDFIA'11)*, pp. 81–92, Berlin, Heidelberg, 2011.

[85] R. Pries, W. Yu, X. Fu, and W. Zhao, "A new replay attack against anonymous communication networks," in *Proceedings of the IEEE International Conference on Communications, ICC'08*, Berlin, Heidelberg, 2008.

[86] R. H. Deng, J. Zhou, and F. Bao, "Defending against redirect attacks in mobile IP," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ACM, pp. 59–67, Berlin, Heidelberg, 2002.

[87] D. Kavitha, E. Murthy, and S. Hug, "A secure route optimization protocol in mobile IPv6," *International Journal of Computer and Network Security (IJCSNS)*, vol. 9, pp. 27–33, 2009.

[88] F. Al Hawi, C. Y. Yeun, and K. Salah, "Secure framework for the return routability procedure in MIPv6," in *Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom)*, Berlin, Heidelberg, 2013.

[89] S. Kent, "IP encapsulating security payload (ESP)," *RFC 4303*, vol. 9, 2005.

[90] S. Kent and K. Seo, "Security architecture for the internet protocol," *RFC 4301*, vol. 9, 2005.

[91] S. Kent, "IP authentication header," *RFC 4302*, vol. 9, 2005.

[92] C. Kaufman, "Internet key exchange (IKEv2) protocol," *RFC 4306*, vol. 9, 2008.

[93] J. Arkko, V. Devarapalli, and F. Dupont, "Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents," *RFC 3776*, vol. 9, 2004.

[94] V. Devaparalli and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," *RFC 4877*, vol. 9, 2007.

[95] A. J. Jara, "Lightweight MIPv6 with ipsec support," *Mobile Information Systems*, vol. 10, no. 1, pp. 37–77, 2014.

[96] R. A. Khan and A. Mir, "IPsec in mobile IP: a survey," *Semantic Scholar*, vol. 10, 2013.

[97] J. Caldera, D. De-Niz, and J. Nakagawa, "Performance analysis of IPSec and IKE for mobile IP on wireless environments," *Information Networking Institute*, vol. 10, 2000.

[98] J. Granjal, R. Silva, E. Monteiro, J. Silva, and F. Boavida, "Why is IPSec a viable option for wireless sensor networks," in *Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2008*, Berlin, Heidelberg, 2008.

[99] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet key exchange protocol version 2 (IKEv2)," *RFC 7296*, vol. 10, 2014.

[100] Z. Faigl, P. Fazekas, S. Lindskog, and A. Brunstrom, "Performance analysis of IPsec in mobile IPv6 scenarios," *Mobile and Wireless Communications Summit*, vol. 10, 2007.

[101] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, "Mobile IP version 6 route optimization security design background," *RFC 4225*, vol. 10, 2005.

[102] Y.-C. Chen and F.-C. Yang, "An efficient MIPv6 return routability scheme based on geometric computing," *Proceedings of World Academy of Science, Engineering and Technology*, vol. 10, pp. 437–442, 2009.

[103] K. Ren, "Routing optimization security in mobile IPv6," *Computer Networks*, vol. 50, no. 13, pp. 2401–2419, 2006.

[104] S. K. Mathi and M. Valarmathi, "A secure and decentralized registration scheme for IPv6 network-based mobility," *Computer Networks*, vol. 5, no. 5, 2013.

[105] S. Rajkumar, M. Ramkumar Prabhu, and A. Sivabalan, "Securing binding updates in routing optimizaton of mobile IPv6," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 12, pp. 1633–1636, 2012.

[106] J. D. Koo, J. Koo, and D. C. Lee, "A new authentication scheme of binding update protocol on handover in mobile IPv6 networks," *International Conference on Embedded and Ubiquitous Computing*, vol. 4, 2006.

[107] J.-D. Koo and D.-C. Lee, "Extended ticket-based binding update (ETBU) protocol for mobile IPv6 (MIPv6) networks," *IEICE Transactions on Communications*, vol. 90, no. 4, pp. 777–787, 2007.

[108] W. A. A. Alsalihy and M. S. S. Alsayfi, “Integrating identity-based encryption in the return routability protocol to enhance signal security in mobile IPv6,” *Wireless Personal Communications*, vol. 68, no. 3, pp. 655–669, 2013.

[109] S. Mathi and M. Valarmathi, “An enhanced binding update scheme for next generation internet protocol mobility,” *Journal of Engineering Science and Technology*, vol. 13, no. 3, pp. 573–588, 2018.

[110] S. Mathi, “A certificateless public key encryption based return routability protocol for next-generation IP mobility to enhance signalling security and reduce latency,” *Sādhanā*, vol. 42, no. 12, pp. 1987–1996, 2017.

[111] G. O’shea and M. Roe, “Child-proof authentication for MIPv6 (CAM),” *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, pp. 4–8, 2001.

[112] I. You, J. H. Lee, and B. Kim, “caTBUA: context-aware ticket-based binding update authentication protocol for trust-enabled mobile networks,” *International Journal of Communication Systems*, vol. 23, no. 11, pp. 1382–1404, 2010.

[113] C. Vogt, R. Bless, M. Doll, and T. Kuffner, “Early binding updates for mobile IPv6,” *Wireless Communications and Networking Conference*, vol. 31, 2005.

[114] H. Kim and J.-H. Lee, “Diffie-Hellman key based authentication in proxy mobile IPv6,” *Mobile Information Systems*, vol. 6, no. 1, pp. 107–121, 2010.

[115] H. Modares, “Enhancing security in mobile IPv6,” *ETRI Journal*, vol. 36, no. 1, pp. 51–61, 2014.

[116] G. M. De Dormale, P. Bulens, and J.-J. Quisquater, “An improved Montgomery modular inversion targeted for efficient implementation on FPGA,” in *Proceedings IEEE International Conference on Field-Programmable Technology*, New York, NY, USA, 2004.

[117] H. Modares, Y. Salem, R. Salleh, and M. T. Shahgoli, “A bit-serial multiplier architecture for finite fields over galois fields,” *Journal of Computer Science*, vol. 6, no. 11, pp. 1237–1246, 2010.

[118] T. Aura, “Cryptographically generated addresses (CGA),” *RFC 3972*, vol. 6, 2005.