Hindawi
Security and Communication Networks
Volume 2021, Article ID 6751423, 12 pages
https://doi.org/10.1155/2021/6751423

Research Article

Secure Vertical Handover to NEMO Using Hybrid Cryptosystem

Vikram Raju Reddicherla,[1] **Umashankar Rawat**,[2] **Y. Jeevan Nagendra Kumar**,[3] **and Atef Zaguia**[4]

[1]*Department of Computer Science and Engineering, NMAM Institute of Technology, NITTE, Deralakatte 574110, India*
[2]*Department of CSE, Manipal University Jaipur, Jaipur 303007, India*
[3]*Department of Information Technology, Dean Technology and Innovation Cell, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India*
[4]*Department of Computer Science College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Umashankar Rawat; umashankar.rawat@jaipur.manipal.edu

Received 28 April 2021; Revised 1 June 2021; Accepted 9 June 2021; Published 28 June 2021

Academic Editor: Abdelouahid Derhab

To provide security to all pairs of nodes in network mobility (NEMO) while executing the handoff between different technologies, a hybrid cryptosystem with a suitable network selection mechanism is proposed. All pairs of nodes, i.e., Mobile Node (MN), Mobile Router (MR), Correspondent Node (CN) and MN, and Home Agent (HA), respectively, are considered. A proper security mechanism is proposed to provide confidentiality to Bound Update (BU) during handoff and conversation between MN, MR, and HA using the elliptic curve cryptography (ECC). In this solution, a network selection mechanism is proposed based on user preference and Received Signal Strength (RSS) in a heterogeneous network. The proposed model can protect the communication using security analysis from all NEMO standard attacks. Whenever NEMO moves, MR intimates to HA about the address change using (BU) and MR receives Binding Acknowledgement (BA) as a reply. During data (frame) exchange and registration between MN, CN, and HA, various security threats arise. In the earlier work, only the security solution is given, and the best network selection algorithm is not provided in a heterogeneous environment. Therefore, in this paper, the best network selection is contributed based on Received Signal Strength (RSS) and user preferences. A comparison of the proposed model is drawn with Return Routability Procedure (RRP). Authentication is provided for communication between MN and CN. The proof is derived using BAN logic. Many standard security attacks have been successfully avoided on all pairs of communications. It has been observed that the proposed model achieves 2.4854% better throughput than the existing models. Also, the proposed model reduces the handoff latency and packet loss by 2.7482% and 3.8274%, respectively.

1. Introduction

Many network technologies (WiMax, WiFi, 3G, 4G, 5G, and Femtocell) exist in recent years because Internet usage has grown in an exponential series. Mobility management is a primary concern in wireless networks and each technology has its mobility management architecture [1–3] for providing network services to mobile users without any delay. To give better Quality of Service (QoS) to end-users, a universal mobility management architecture is required across heterogeneous networks [4, 5]. A seamless handover execution should be without degrading QoS and QoE with the help of location-based information. The handoff execution occurs in layer 2 and layer 3, and handoff techniques are differing from layer to layer [6].

In a network field, an IP address is required in the Internet for maintaining a point of attachment and for making packets deliverable to the assigned node. Every time the device changes the address, the IP address is suitable. While maintaining a point of attachment, this IP is not suitable because this address is the same everywhere. Mobile IP [7–9] is present in the network and helps in allowing

transparency of the IP on the Internet to the nodes to avoid this problem.

The Home Address (HoA) identifies the MN (MN) on the Internet and is well known as an address that is permanent and will never change using out the lifetime of the node. An address is obtained using the foreign link if MN travels from one network to another network, called the Care-of Address (CoA). When two or more nodes move simultaneously, each MN is required to keep a specific attachment over the communication channel and to maintain session continuity using out the handoff.

NEMO is the mobility of a network where a set of nodes such as laptops, i-pad, mobiles, and PCs, move as a network. Here, a gateway referred to as MR handles the point of attachment in favor of all n numbers of MNs on the Internet. Under a single MR, there can only be n MNs and n MRs referred to as NEMO. Nested NEMO contains various hierarchic levels. When a patient has PAN connected using their smartphone, the PAN could have Body Area Networks (BAN) to send health-related information to its doctor. Here, a smartphone serves as top-level MRs, PANs, and BANs MR as nested NEMO. The health parameters are given by PAN and BAN to the top-level MR (mobile phone) and the data are sent using the Internet to the health center by this MR. This information needs to send an insecure way and an efficient security algorithm is required for the same.

1.1. Motivation. Although many researchers have contributed several approaches to NEMO and RO [5], still it is an open area of research. Many issues are still present where there is a need to concentrate more. These are mentioned as follows:

(i) Access network selection: new technologies are coming up these days with substantial bandwidth to satisfy the end-user by giving uninterrupted Internet connectivity. Many parameters need to be considered for selecting a suitable network.

(ii) Handoff: many of the researchers have contributed to an efficient handover in both nested and non-nested NEMO, regardless of horizontal handover or vertical handover. However, a better vertical handoff procedure could not be given using lightweight cryptography.

(iii) Security: security is the major worry in all domains related to networking [10–18] not only limited to NEMO. Good security architecture protects data and control frames over the networking layer in NEMO. The majority of the research works could provide security to handoff in NEMO. Security issues [19, 20] are explained in two cases clearly with NEMO basic operation.

(iv) Quality of Service (QoS): once taking care of end-to-end delay and handover delay in a reasonable way is done, better QoS can be maintained automatically in NEMO.

1.2. Contributions. The main contributions of the paper are as follows:

(i) To provide security to all pairs of nodes in network mobility (NEMO) while executing the handoff between different technologies, a hybrid cryptosystem with a suitable network selection mechanism is proposed.

(ii) All pairs of nodes, that, Mobile Node (MN), Mobile Router (MR), Correspondent Node (CN) and MN, and Home Agent (HA), respectively, are considered.

(iii) A proper security mechanism is proposed to provide confidentiality to Bound Update (BU) during handoff and conversation between MN, MR, and HA using the elliptic curve cryptography (ECC).

(iv) A network selection mechanism is also proposed based on user preference and Received Signal Strength (RSS) in a heterogeneous network.

(v) Authentication is provided for communication between MN and CN. The proof is derived using BAN logic.

(vi) Comparison of the proposed model is drawn with Return Routability Procedure (RRP) to access its efficiency.

The rest of this paper is organized as follows. Sections 2 and 3 represent the existing literature. Section 4 illustrates the basic operations of NEMO and about Route Optimization (RO). Section 5 explains the problem statement. The proposed method is discussed in Section 6. Section 7 explains the analysis and simulation results by comparing them with the existing Return Routability Procedure, and Section 8 concludes the research article.

2. Background

In recent years, many technologies came into the real world to give high-speed Internet. Parameters for vertical handoff decision layerwise [21] are mentioned in Table 1.

Depending on the requirement that the end-user selects the suitable network to maintain session continuity for uninterrupted Internet usage, the handoff technique is classified into two types based on execution, that is, soft handoff and hard handoff. In the soft handoff, handoff initiates with the new base station before breaking the session continuity with the old base station based on the existing RSS value. In hard handoff, handoff gets initiated after breaking the connection with the old base station. Handoff techniques are divided into two types based on the type of network during handover; these are horizontal handoff and vertical handoff.

If session transfer occurs between the same types of network technology, this handoff is called a horizontal handoff. Horizontal handoff execution occurs in 802.16 base stations as shown in Figure 1. If session transfer occurs between different network technologies, this handoff is called a vertical handoff. This handoff execution is between the 802.11 access point and the 3G base station as shown in

Table 1: Parameters for vertical handoff decision layerwise [21].

Serial number	Layers	Parameters
1	Layer 4	Preferences of end-user (e.g., cost and provider), information context (e.g., speed), parameters for QoS (e.g., delay, bandwidth, and jitter), and alerts for security (e.g., notifications)
2	Layer 3	Load on network (e.g., bandwidth available)
3	Layer 2	Available of foreign agents, preauthentication for network, configuration of network, topology of network, and routing information
4	Layer 1	Network conditions for radio access, link parameters and status, and availability of access media

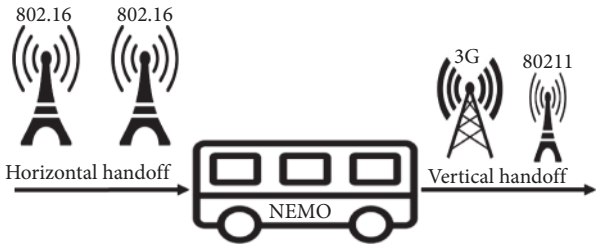

Figure 1: Handoff types.

Figure 1. Parameters like Received Signal Strength (RSS), bandwidth, necessary power, cost, safety, user preferences, and security are considered as decision parameters for selecting the best network in heterogeneous networks. Many research works have been done for better network selection in a heterogeneous network. The authors have taken network selection decisions based on RSS; user preference is the primary parameter to take a decision.

Consider n mobile nodes are progressing as a unit via different channels and using out this process, n amounts of handoffs are needed and all nodes must invest their resources (battery power and processing power) individually for executing a handoff. In IETF, NEMO [22, 23] is introduced to prevent these shortcomings of Mobile IP.

3. Literature Review

Many of the research works have been done to select the better network for host mobility and network mobility. In host mobility, deciding to select the best network is very smooth in the case of NEMO or group mobility; several users are using different applications, and choosing the right network is very difficult. Walid et al. [24] proposed to select a better network selection mechanism called group vertical handover to group mobility-based architecture by considering user preferences and congestion parameters. They used two algorithms to calculate congestion, i.e., dubbed Sastry and O-Learning algorithms. They simulated the whole scenario and shown better results by avoiding congestion with vertical hand selection and execution. User preference only considered choosing the best network and security was not provided.

Munasinghe and Jamalipour [25] proposed an architecture for NEMO which supports heterogeneous networks to select the better network with less handoff delay. They have simulated and shown results in terms of handoff latency and packet drop. They have not focused on security. Ahmed and Gati [26] proposed an intelligent technique for service or session continuity in a heterogeneous network environment. As a result, the performance of the network and QoS did not degrade. In this work, the authors incorporate mobile agents in mobile nodes to collect the necessary information to select the best network and for smooth vertical handoff execution. Frequent handoff is a critical issue in high-way due to high speed.

Ali Hassoun et al. [27] proposed a VHDA algorithm by keeping the location of the vehicle, speed of the vehicle, and jitter as parameters. Simulated results have shown that VHDA algorithm outperforms the competitve approaches. Vertical handoff decision is a critical issue in heterogeneous networks. In [28], an artificial neural network-based handover decision algorithm was utilized. Data speed and RSS value were the inputs to take VHDAs. An algorithm is proposed in [29] for taking a vertical handover decision. For performance evaluation, the attribute matrix is prepared. To take a handover decision, multiattribute QoS is considered. PROMISE algorithm is used for taking the final VHDA depending on the attribute matrix and weight vector.

In [30], a client-based vertical handover mechanism was proposed for providing efficient connectivity to end-users without any delay in a heterogeneous wireless network. There is no need to modify the existing Mobile IP stack and core network. In [31], a VHDA based on user preference (changing dynamically) was proposed. The user preferences have been assigned as simple additive weighting and multiplicative exponential weighting. In [32], a VHDA was proposed based on battery resource as a parameter to decide on vertical handover for selecting a better network. This parameter is divided into two categories such as poor and strong resource mobile nodes. Based on these parameters, the network is selected, and handover execution occurs.

In [33], a fuzzy logic theory-based model was proposed for VHDAs to select the network based on three parameters, i.e, Quality of Service, RSS value, and bandwidth. Media independent handover is a standardized protocol such as IEEE 802.21 for vertical handover purposes in heterogeneous networks. In [34], an improved IEEE 802.11 version architecture for VHDA was proposed. Dhar Roy and Vamshidhar Reddy [35] proposed a vertical handover decision based on signal strength. In [36], security for Route Optimization is provided with authentication features. In this process, HA generates a secret group mobile key to authenticate the BU. This work mainly focused on the security between CN and MR. They did not support security among HA, MR, and MN.

In [37], a secure optimization of the route for NEMO was designed using an identity-based cryptosystem known as MPB-AKA-MR2 protocol. The security is provided for MR and MN in home networks and in between CR and CN in a foreign network. Secure communication is enabled between MN and CN. Calderon et al. [38] designed two approaches: one is being the combination of the PKI certificates and the other being an infrastructureless method, which uses Cryptographically Generated Address (CGA) to flexibility. The solution will be provided with BA and BU only between CN and MN. Jo and Inamura [39] proposed a solution between pairs of communication (MR and HA and CN and MN) using the Multikey Cryptographically Generated Address (MCGA). The length of the propagation path is saved between MR and MN. However, it does not secure between the MR and MN. Chen et al. [40] proposed a bilinear pairing based dynamic key management and authentication mechanism for wireless sensor networks. The cluster nodes and the sensor nodes exchange the key using bilinear pairing in this cluster node and base station. Yeh et al. [41] proposed a secure RO using the ECC algorithm that was called the Batch-Bounded Update Scheme (BBUS) to verify multiple signatures simultaneously. It focused only on CN and MN communication. A few of them considered the latest technologies like 4G and 5G [42–45].

4. NEMO Basic Operation

Under a MR, there could be n number of MNs in NEMO. After successful registration, when the NEMO is under the home network, the existing MNs will get a permanent address or an HoA [46–48]. HA is an address registry or location and maintains the address of the MRs and all its MNs. NEMO's basic operation is explained as shown in Figure 2.

There are two mobile nodes, i.e., MN1, MN2 under MR and its CN. The nodes MN1 and MN2 have been communicated using wireless technology with the MR. Both will get the addresses from their respective Access Router (AR). Its basic operation is demonstrated in the following cases, i.e., NEMO under the parent network and when NEMO changes to a foreign network.

4.1. Scenario 1. Whenever the NEMO is in the parent network and gets an HoA, it must inform HA about its location or address because HA must record the movement data of the nodes in NEMO. The obtained address details require a particular layout referred to as Binding Update (BU). MR or MN transmits a BU to HA, and it obtains a Binding Acknowledgement (BA) as a confirmation from HA after receiving. A bidirectional tunnel establishes further data communications between HA and MN.

4.2. Scenario 2. Figure 1 shows that whenever the NEMO goes to a different network, MR recognizes the nearby Access Router (AR2) by transmitting router solicitation and advertisement frames. MN or MR gets a new address (Care-of Address) from a foreign network. HA should be informed about Care-of Address. It happens using BU and BA frames.

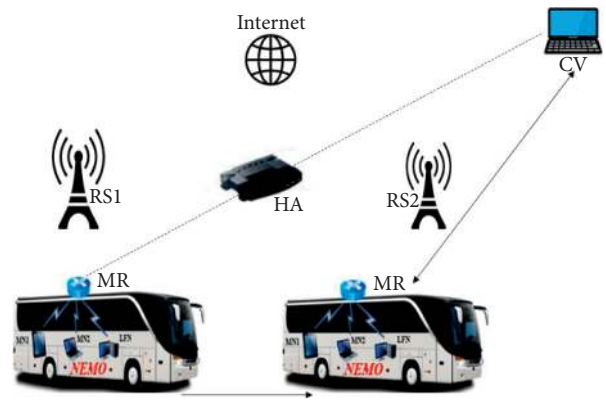

Figure 2: NEMO basic operation.

4.3. Route Optimization (RO). If MN aims to connect with CN, then MN must inform CN about its present address or location. Through BA and BU exchange, this intimation occurs. In both case 1 and case 2, the entire data has gone over HA. On account of this, data congestion occurs, and it may also lead to a bottleneck at HA. Route Optimization is a concept that is newly introduced in NEMO to prevent data congestion at HA. It is detouring HA while exchanging BA, BU between CN and MN during their communication.

5. Problem Statement

The best access point selection mechanism and security architecture for giving confidentiality Authentication & verification to RO utilizing tripartite Diffie Hellman using ECC is presented and the secure communication among MN, MR preventing handoff delay is delivered.

For providing secure NEMO, MIPV6 is derived in IETF, and Return Routability (RR) [49] is used. By executing the RR procedure, a binding key (Keybm) should be exchanged for providing authentication to the communication between MN and CN. The RRP works as shown in Figure 2. Whenever MN will want to communicate with the CN, it sends a Home test-Init test (HoTi) frame to the CN using HA. Replying to that, CN sends a HoT frame to the MN and it will prepare a key (KH). MN will send Care of Test-Init test (CoTi) frame immediately to CN and it will give CoT as acknowledgment and will prepare the key (KC). Both CN and MN will calculate the binding key (Keybm) as

$$\text{Keybm} = H(\text{KH}\|\text{KC}). \quad (1)$$

Here, MN and CN share BU and BA securely using the above key. This RRP is having the following deficiencies or issues:

Issue 1. The vicious intruder, stays in between CN and MN, accesses HoTs and CoT frames, and prepares KH and KC. Hence, the intruder prepares Keybm and violates integrity and confidentiality.

Issue 2. In RRP, security did not provide between HA, MN, and MR except between CN, MN.

Issue 3. MN must send HoT and HoTi frames via the HA, even MN is so far from the parent network to

prepare the binding key. There is not any direct procedure for the preparation of the key to giving security to CA and BU. A compressed solution is mandatory bypassing the HA to prepare the key.

Issue 4. A proper verification mechanism is not available in RRP to authenticate both parties (MN or MR, CN).

6. Proposed Solution

The whole proposed model is discussed in detail in two separate sections. Firstly, the access point selection mechanism is discussed in a heterogeneous network (802.11, 802.16, and 3G) based on RSS (Received Signal Strength) value and user preference. In the second section, the security algorithm is discussed using ECC and stream cipher cryptography (Salsa20) while executing the vertical handoff.

6.1. Network Selection Procedure. Transferring the session from a base station to another base station is called a handoff. Whenever a handoff occurs between the same technologies (between 802.11 Access Point and another 802.11 Access Point), it is called horizontal handoff. If handoff executes between different technologies (between 802.11 Access Point and 802.16 Base Station), it will be called vertical handoff. In this document, we use vertical handoff instead of handoff because in our research work three networks (802.11, 802.16, and 3G) are used. It is very easy to implement the vertical handoff for individual devices (in host mobility) because only application is running in the respective device. When NEMO comes into the picture, multiple MNs are in the network under MR and different applications are used depending on their requirements. In this situation, selecting a network for vertical handoff execution is very difficult. In this work, we are selecting a suitable network based on RSS (Received Signal Strength) and user preference. In this context, we are categorizing the applications which we got information from the online article, in which MNs are used in NEMO. The RSS value always should be $-30\,\text{dBm} < \text{RSS} < -70\,\text{dBm}$ for using any application in any MN. Tables 2 and 3 show the applications with respect to the range and priority range, respectively.

The priority is an added extra option in DHAAD (Dynamic Home Agent Discovery Address Request) frame at the initial state itself. Nevertheless, HA contains all data about its NEMO nodes including MR and all MNs. In DHAAD frame, P indicates priority; if P is enabled, the hearer containing priority data is replaced with a priority of all MN. If P is disabled, it indicates its normal packet (see Figure 3).

Network selection is based on RSS value and user priority; here, priority refers to importance to the respective application whatever they are using in their MN. If the priority is very high, we should concentrate to give the best QoS to the respective MN.

Priority nodes = high (MN_1, MN_2,. . .,MN_n).

Once deciding the priority, applications, select a suitable network technology based on the signal strength and distance between the base station and access point.

Secure architecture for vertical handoff.

Once a suitable network technology is selected by NEMO based on the above technique, vertical handoff initiation is started. In this solution, tripartite Diffie–Hellman [50] and the session key concept have been used for security between MN and CN.

In three phases, the proposed model is executed:

(a) Setting parameters

(b) Common and Router Optimization Key Preparation

(c) Generation of session keys

6.2. Setting Parameters. In this step, parameters that are used to prepare a common key are set by the home network's nodes and the foreign nodes. For the home networks and the foreign network separately, the parameter setting is explained below, and Figure 4 shows the algorithm for network selection.

6.3. Home Network. HAhom, MN, and MR are the 3 participants in the home network. Based upon the elliptical curve cryptography equation, the exchanging of two points P, Q is done.

HAhom, MN, and MR generate some random numbers (a_{MN}), (b_{MR}), and (c_{HAhom}), respectively. And HAhom, MN, and MR will broadcast (P_{MN}, Q_{MN}), (P_{MR}, Q_{MR}), and (P_{HAhom}, Q_{HAhom}) accordingly explained as shown in Figure 5:

$$\begin{aligned} P_{\text{MR}} &= P \times a_{\text{MR}}, \\ Q_{\text{MR}} &= Q \times a_{\text{MR}}. \end{aligned} \tag{2}$$

$$\begin{aligned} P_{\text{HA}_{\text{hom}}} &= P \times b_{\text{HA}_{\text{hom}}}, \\ Q_{\text{HA}_{\text{hom}}} &= Q \times b_{\text{HA}_{\text{hom}}}. \end{aligned} \tag{3}$$

$$\begin{aligned} P_{\text{MN}} &= P \times c_{\text{MN}}, \\ Q_{\text{MN}} &= Q \times c_{\text{MN}}. \end{aligned} \tag{4}$$

6.4. Foreign Network. In this home network, HA fora, CR, and CN are three participants. Depending upon the elliptic curve cryptography equation, the exchanging of two points X, Y is done. HA fora, CN, and CR generate a random number (x_{CN}), (y_{CR}), and (z_{HAfor}), respectively. And, HA_{for} CN and CR will broadcast (X_{CN}, Y_{CN}), (X_{CR}, Y_{CR}), and (X_{HAfor}, Y_{HAfor}) accordingly explained as shown in Figure 6. Here,

Table 2: Applications with respect to the range.

Category	Name of application at MN	Range of dBm	RSS value
1	Video chat or video conference	−30 dBm	Better
2	Video streaming	−60 dBm	Good
3	Mail application and text chat application	−70 dBm	Bad

Table 3: Priority range.

S. number	Priority	Description
1	Very high	Priority needs given to respective MN by giving enough bandwidth
2	High	
3	Low	

Type	Code	Checksum		
Identifier		*R*	*P*	Reserved
Priority data				

Figure 3: DHAAD frame.

$$X_{CR} = X \times x_{CR},$$
$$Y_{CR} = X \times c_{CR}, \tag{5}$$

$$X_{HA_{for}} = X \times y_{HA_{for}},$$
$$Y_{HA_{for}} = Y \times y_{HA_{for}}, \tag{6}$$

$$X_{MN} = X \times x_{CN},$$
$$Y_{CN} = Y \times x_{MN}. \tag{7}$$

6.5. Common and RO Key Preparation. The parent network and foreign network nodes will calculate the common keys after the parameters are set as shown in equations (1)–(3) using "Weil and Tate Pairing" on the elliptical curves [50] method for the parent network and the common keys are prepared for the foreign networks as shown in equations (4)–(6). Each of the nodes uses the bilinear pairing theorem to calculate this common key explained as shown in Figure 7.

The parent network common key, i.e., $\text{Key}_{\text{MN–MR–HA}_{\text{hom}}}$, is prepared as follows:

$$\text{Key}_{\text{MN–MR–HA}_{\text{hom}}} = \text{Fr}(1, (P) - (Q), (P+Q) - (0))^{a_{\text{MN}}} b_{\text{MR}} c_{\text{HA}}. \tag{8}$$

Foreign network common key, i.e., $\text{Key}_{\text{CN–HA–MR}_{\text{for}}}$, is prepared as follows:

$$\text{Key}_{\text{CN–CR–HA}_{\text{for}}} = \text{Fr}(1, (P) - (Q), (P+Q) - (0))^{x_{\text{CN}}} b_{\text{MR}} c_{\text{HA}}. \tag{9}$$

The RO key is prepared by MN and CN later, i.e., Key_{RO}. To make this RO key by using all nodes (CR and MR, CN, and MN), a key agreement protocol must be executed. The RO key calculation is as follows:

$$\text{Key}_{\text{RO}} = H\left(\text{Key}_{\text{MN–MR–HA}_{\text{hom}}} \| \text{Key}_{\text{CN–HA–MR}_{\text{for}}}\right). \tag{10}$$

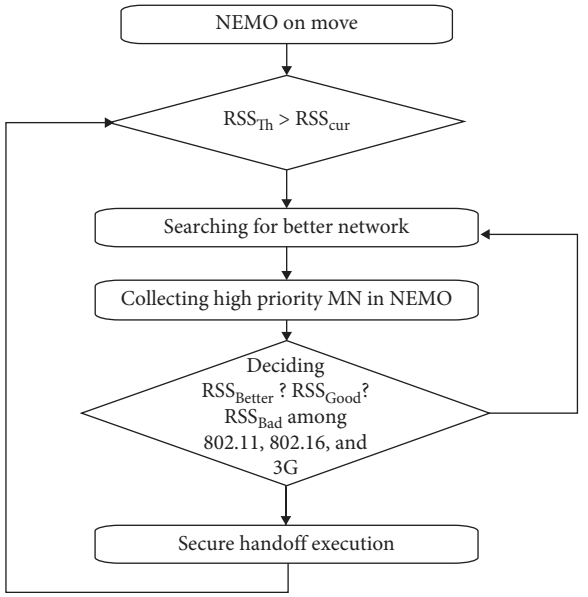

Figure 4: Algorithm for network selection.

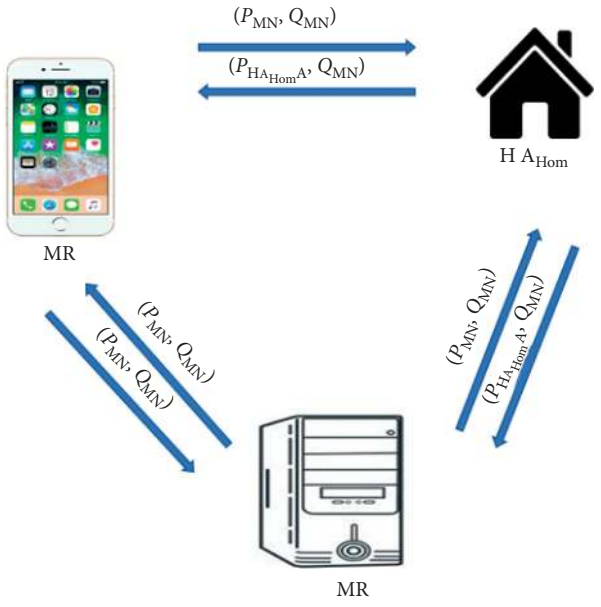

Figure 5: Parameters setting of home network.

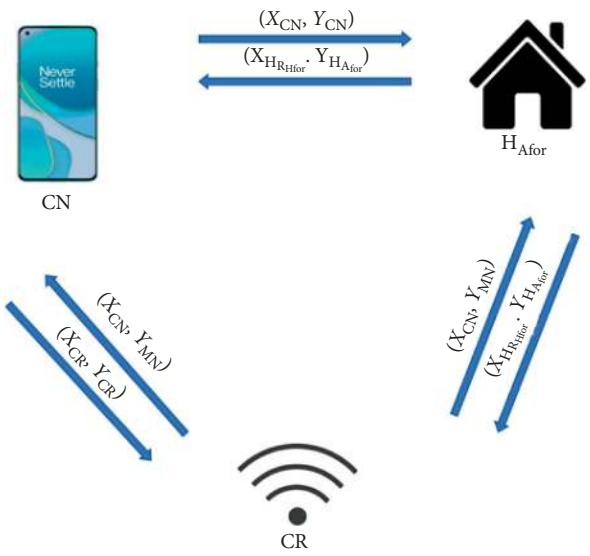

Figure 6: Parameters setting of the foreign network.

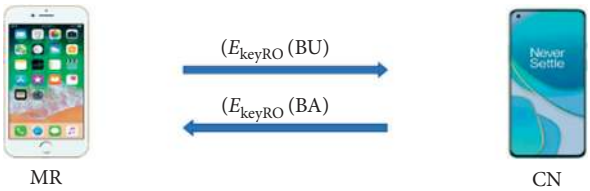

Figure 7: Key exchange between MN and CN.

To secure the BU and BA exchanges, MN and CN use symmetric cryptography used for avoiding the standard malicious threats or any attacks as shown in Figure 8.

To verify as part of authentication, we have used one method using chain hashing. For this, we have modified BU and BA format to send the necessary information to do the verification.

In the above BU header format, we have added an extra bit called A. A refers to authentication. If A is enabled, we need to check for Authentication Data while sending the secure BU encrypted RO key. If A value is disabled, no need to check Authentication Data. Here, Authentication Data contains a randomly generated number which is always a maximum of three bits which represents a single digit and the many times the key is doing hashing. For example, if the digit is 6, MN will do chain hashing (6 times) and keep the result of Authentication Data along with the digit. Once CN receives the BU, it decrypts BU using the RO key and checks for A bit. If A bit is enabled and it checks for Authentication Data, based on the numerical digit, it will do chain hashing many times and verify with the received one. If both are the same, the verification is a success; otherwise, discard the BU and asks for fresh BU explained as shown in Figure 8.

In the above BA header format, we have added an extra bit called A. If A is enabled which is received by MN from CN, it will think the verification is a success explained, as shown in Figure 9.

								Sequence number
A	*H*	*L*	*K*	*M*	*R*	*A*	Reserved	Lifetime
Authentication data								

Figure 8: Modified BU.

	Status	*K*	*R*	*A*	Reserved
Sequence number	Lifetime				

Figure 9: Modified BA.

6.6. Session Key Preparation. The algorithm Salsa20 is used in stream cipher cryptography to provide confidentiality to Router Optimization. This utilizes the XOR operation and is lightweight cryptography, especially for low power/small mobiles, and this is the benefit of using salsa20. To give it, another level of security between CN and MN, session key concept is used.

Session key concept used

$$\begin{aligned} \text{Key}_1 &= H(\text{Key}_{RO}), \\ \text{Key}_2 &= H(\text{Key}_1), \\ \text{Key}_3 &= H(\text{Key}_2), \\ \text{Key}_n &= H(\text{Key}_{n-1}). \end{aligned} \tag{11}$$

We use the word "session," which is the time network mobility spends over a single network or other network and is called a session. The time threshold value is used if NEMO spends additional time not including moving and it is also considered a session if the NEMO stays below the threshold value of time.

7. Results and Analysis

While comparing with other protocols, we have been considering some of the assumptions while comparing other protocols. To execute the remaining proposed model at home network and foreign network for concerned nodes, all these nodes MR, MN, and HA need to have some basic information. While maintaining communication with CN, we have been considering sessions when the NEMO moves to various networks. To enhance our proposed model for calculating the handoff delay and end-to-end delay, NS2 (ns2.29) [51–55] is used. Although it would not support the NEMO, Mobiwan (Thierry Ernst, 2002) patch is in use to give support to the NEMO, that is, an enhancement of MobileIP version 6 (it will support ns2.28 and ns2.29) [56, 57]. With regard to security, the comparison is done with our results with the standard RRP explained as shown in Table 4.

The summation of the time for registering and the time for obtaining the latest address from another network by interchanging BA and BU is called handoff delay explained as shown in Figure 10. Using the NS2 simulator, this kind of delay is obtained. This delay is denoted in the form of mill seconds as shown in Table 1. We can achieve a small difference in the handover delay compared to the existing RRP. For security, our proposed model is to avoid using standard attacks.

Table 4: Performance comparison.

Protocol	Vertical handoff delay	Security between nodes			
		MN, MR	MN, HA	MR, HA	MN, CN
RRP	0.210716	×	×	×	√
NEMO-ECC	0.203062	√	√	√	√

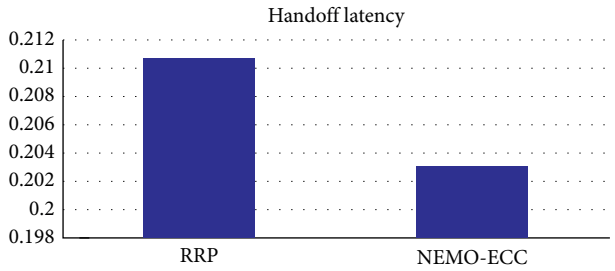

Figure 10: Handoff latency.

Figures 11 and 12 show the throughput and packet loss analysis, respectively. It is found that the proposed model consistently achieves better throughput and lesser packet loss, respectively.

7.1. Solution for Issue 1. An intruder cannot calculate the RO key because he does not have the awareness about the common keys for the home network and foreign network by sitting in between CN and MN.

7.2. Solution for Issue 2. Between MN, HA; MR, HA; and MN, MR, RRP did not provide security. Here, in our solution, we are able to provide security inside the parent network using sharing a common key (KeyCN-CR-HAhom) among CN, MR, and MN using the triplicate ECC method. Using a single-pass communication, MR, MN, and HA can have the same key because of the triplicate ECC algorithm.

7.3. Solution of Issue 3. In RRP, to authenticate CN, MN must send the required parameters via HA. This is the solution we need not go using HA repeatedly, so the bottleneck is avoided.

Here, we are enabling the security between CN and MN based on the Route Optimization key. We have introduced the concept of the session key and we have maintained a unique key for every session using the concept of chain hashing. Because we use different keys, an intruder cannot guess the key.

7.4. Solution for Issue 4. The same number of operations occurs at CN for verification purposes if n number of hashing operations occurs at MN. If the verification is a success between MN and CN, both think that BU, BA frames are valid.

Using BAN logic, the authentication proof is given between MN and CN.

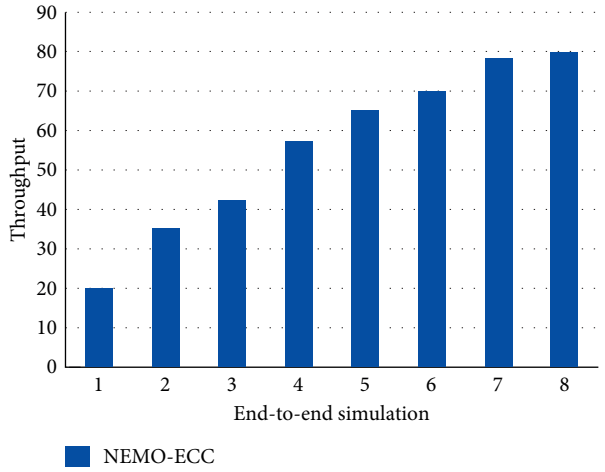

Figure 11: Throughput analysis.

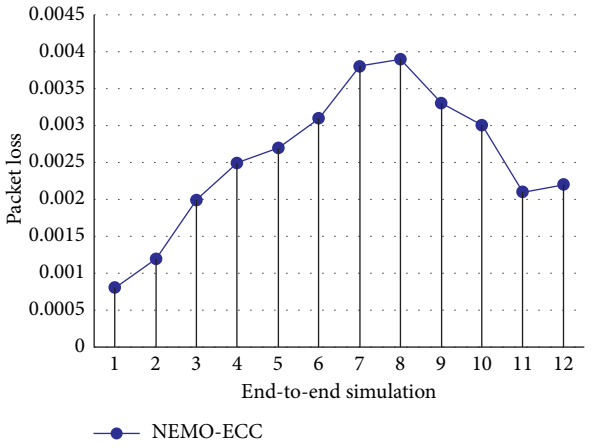

Figure 12: Packet loss analysis.

7.5. Solution Analysis Using BAN Logic. BAN logic is utilized to evaluate the strength of authentication.

7.5.1. BAN Logic. The BAN logic can be defined as

$$\begin{cases} S| \equiv D: S \text{ believes } D \\ S\Delta X: S \text{ sees } X \\ S| \sim X: \text{ Monce said } X \\ S \Rightarrow X: S \text{ has jurisdiction over } X \\ \#(X): X \text{ is fresh} \\ \{X\}_{\text{key}}: X \text{ is encrypted with key} \\ S \xrightarrow{\text{Key}} \text{DS and } D \text{ shares } a \text{ secret} - \text{Key} \end{cases}. \quad (12)$$

Here, S is the source node and D is the destination node, respectively.

7.5.2. BAN Logic Interference Rules. Simulated results have shown that VHDA algorithm outperforms the competitve approaches. These rules are presented as follows.

7.5.3. R1: The Frame Means Rule.

$$\frac{S| \equiv (S \xrightarrow{\text{Key}} S),\ S\Delta\{X\}_{\text{key}}}{S| \equiv (D\Delta X)}. \tag{13}$$

It states that M considers that a key is communicated among S and D, S perceives X encrypted with key, and S considers sometimes D may utilize the value of X.

7.5.4. R2: Nonce-Verification Rule.

$$\frac{S| \equiv \#(X),\ S| \equiv \{D\Delta X\}}{S| \equiv (D| \equiv X)}. \tag{14}$$

It states that S considers the inventiveness of X and S considers that D said on X, S considers D considers X.

7.5.5. R3: Jurisdiction Rule.

$$\frac{S| \equiv (D \Rightarrow X),\ S| \equiv (D| \equiv X)}{S| \equiv X}. \tag{15}$$

This rule says that S believes that D controls X, S believes D believes X, and S believes the same information nothing but X.

7.6. Objectives for Authentication. In the proposed model, four objectives have been selected to prove the authentication between MR and MNN. The primary concern is to assure trust worthies should communicate data by preventing intruder nodes to retrieve secure transmission. The defined objectives are as follows:

$$\begin{cases} \text{Goal 1: } \text{MN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \\ \text{Goal 2: } \text{CN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \\ \text{Goal 3: } \text{MN}| \equiv \text{CN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \\ \text{Goal 4: } \text{CN}| \equiv \text{MN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \end{cases}. \tag{16}$$

These four frames are required to be communicated between MNN and MR:

$$\begin{cases} \text{Message1: MN} \longrightarrow \text{CN: Auth1 (BU}||\text{Nonce1}||)_{\text{Key}_{\text{RO}}}) \\ \text{Message2: CN} \longrightarrow \text{MN: Auth2 (BA}||\text{Nonce2}||)_{\text{Key}_{\text{RO}}}) \\ \text{Message3: MN} \longrightarrow \text{CN: Auth3 (Success} - \text{MN})_{\text{Key}_{\text{RO}}}) \\ \text{Message 4: CN} \longrightarrow \text{MN: Auth4 (Success} - \text{CN})_{\text{Key}_{\text{RO}}}) \end{cases}. \tag{17}$$

Certain beliefs are utilized for the analysis of MNN MR pair communication authentication as follows:

$$\begin{cases} \text{MN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \\ \text{CN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN} \\ N| \equiv \left(\text{CN} \Rightarrow \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}\right) \\ \text{CN}| \equiv \left(\text{CN} \Rightarrow \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}\right) \\ \text{MN}| \equiv \#(\text{Nonce1}) \\ \text{CN}| \equiv \#(\text{Nonce2}) \end{cases}. \tag{18}$$

7.7. Proof of Authentication. Once frame 1 by CN is received from MN, apply R1 on supposition (b):

$$\text{CN}| \equiv \text{MN}| \sim (\text{BU}, \text{Nonce1}). \tag{19}$$

By applying Nonce rule (R2), rule with

$$\text{CN}| \equiv \#(\text{Nonce2}). \tag{20}$$

Integrate equations (19) and (20):

$$\text{CN}| \equiv \text{MN}| \equiv (\text{BU}, \text{Nonce1}). \tag{21}$$

After receiving frame 2 from CN to MN, apply R1 rule on assumption (a):

$$\text{CN}| \equiv \text{MN}| \sim (\text{BU}, \text{Nonce1}). \tag{22}$$

By applying the Nonce rule (R2), rule with

$$\text{MR}| \equiv \#(\text{Nonce1}). \tag{23}$$

Once frame 3 is obtained from MN to CN, implement R3 with assumption (d):

$$\text{CN}| \equiv \left(\text{CN} \Rightarrow \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}\right)_{\text{Key}_{\text{RO}}}. \tag{24}$$

Implementing R1 to equation (24), one can accomplish Objective 4.

Implementing the freshness rule (R2) to equation (2) with assumption (f), it is shown that the frame is new:

$$\text{CN}| \equiv \text{MN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}. \tag{25}$$

Once frame 4 obtained CN to MN, implement R3 with supposition (c):

$$\text{MN}| \equiv \left(\text{CN} \Rightarrow \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}, \text{Nonce}_2\right)_{\text{Key}_{\text{RO}}}. \tag{26}$$

Implement R1 on equation (26) to get Objective 3:

$$\text{MN}| \equiv \text{CN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{CN}. \tag{27}$$

Once packet 4 is received from MN to CN, then apply R1 on hypothesis (a):

$$\text{MN}| \equiv \text{MN} \xrightarrow{\text{Key}_{\text{RO}}} \text{MR}. \tag{28}$$

By utilizing R1 on hypothesis (b),

$$\text{CN}| \equiv \text{MNN} \xrightarrow{\text{Key}_{\text{RO}}} \text{MR}. \tag{29}$$

Thus, we have proved the authentication using BAN logic between MN and CN.

8. Conclusion

In this paper, RSS and user preference were used to obtain the safest available access network within the range in a heterogeneous network environment. Once network selection was done, handoff execution starts, and session transfer occurs to the newly selected network. The proposed method gave a solution that provides security in the NEMO for every pair of communications among HAhom, MR, and MN at all home networks and for CR and CN at the foreign networks during handoff execution. At first-level security, secure Route Optimization was provided, so that the frames are exchanged in a secure way between MN and CN. We were able to provide second-level security between MN and CN using the chain hashing technique. The various keys were utilized in every session by considering the chain hashing algorithm. Security was provided to RO using RRP. The proposed model provided better security as compared to the solutions with RRP. Guessing attacks, DoS, and replay attacks were avoided using the secure method. It provided significant performance in the form of vertical handoff delay. The total scenario was simulated using NS2 to find the handoff delay and packet loss values. Experimental results revealed that the proposed model is better than the existing models. Using BAN logic, the authentication has been provided to RO.

In near future, we will utilize other optimization approaches to improve the results. Additionally, the proposed model will be tested on real-time applications. Also, we will extend the proposed work by using the deep learning models.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflict of interest regarding the publication of this paper.

Acknowledgments

This work was supported by Taif University, supporting project no. TURSP-2020/114, Taif University, Taif, Saudi Arabia.

References

[1] P. Mather, "Mobility management in wireless networks," *Communications Engineer*, vol. 2, no. 5, pp. 46-47, 2004.

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

[3] I. F. Akyildiz, X. Jiang Xie, and S. Mohanty, "A survey of mobility management in next-generation all-IP-based wireless systems," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 16–28, 2004.

[4] A. Mukherjee and D. De, "Location management in mobile network: a survey," *Computer Science Review*, vol. 19, pp. 1–14, 2016.

[5] H. Tuncer, S. Mishra, and N. Shenoy, "A survey of identity and handoff management approaches for the future Internet," *Computer Communications*, vol. 36, no. 1, pp. 63–79, 2012.

[6] S. Mohanty and I. F. Akyildiz, "A cross-layer (layer 2 + 3) handoff management protocol for next-generation wireless systems," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1347–1360, 2006.

[7] C. E. Perkins, "Mobile IP," *IEEE Communications Magazine*, vol. 35, no. 5, pp. 84–99, 1997.

[8] C. Guo, H. Wu, K. Tan et al., "End-system-based mobility support in IPv6," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 11, pp. 2104–2117, 2005.

[9] S. Chen, Y. Shi, B. Hu, and M. Ai, "Mobility management at network layer," in *Mobility Management. Signals and Communication Technology*, Springer, Berlin, Heidelberg, 2016.

[10] A. Abdullah, S. Aljawarneh, S. Masadeh, and E. Abu-Taieh, "A secure data transmission mechanism for cloud outsourced data," *International Journal of Cloud Applications and Computing*, vol. 3, no. 1, pp. 34–43, 2013.

[11] S. R. Masadeh, S. Aljawarneh, A. Odeh, and A. Alhaj, "Secure communication: a proposed public key watermark system," *International Journal of Information Security and Privacy (IJISP)*, vol. 7, pp. 1–10, 2013.

[12] S. Aljawarneh, M. B. Yassein, and W. A. Talafha, "A resource efficient encryption algorithm for multimedia big data," *Multimedia Tools and Applications*, vol. 76, no. 21, 2017.

[13] S. A. Aljawarneh, R. A. Moftah, and A. M. Maatuk, "Investigations of automatic methods for detecting the polymorphic worms signatures," *Future Generation Computer Systems*, vol. 60, pp. 67–77, 2016.

[14] S. Aljawarneh, "A web engineering security methodology for e-learning systems," *Network Security*, vol. 2011, no. 3, 15 pages, 2011.

[15] S. A. Aljawarneh and M. O. Bani Yassein, "A conceptual security framework for cloud computing issues," *International Journal of Intelligent Information Technologies*, vol. 12, no. 2, 2016.

[16] S. Aljawarneh, M. B. Yassein, and W. A. Talafha, "A multithreaded programming approach for multimedia big data: encryption system," *Multimedia Tools and Applications*, vol. 77, p. 10997, 2018.

[17] A. Imran, A. Shadi, and K. Sakib, "Web data amalgamation for security engineering: digital forensic investigation of open source cloud," *Journal of Universal Computer Science*, vol. 22, no. 4, pp. 494–520, 2016.

[18] A. Z. M. Shahriar, M. Atiquzzaman, and W. Ivancic, "Route optimization in network mobility: solutions, classification, comparison, and future research directions," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 1, pp. 24–38, 2010.

[19] S. Jung, F. Zhao, S. F. Wu, and H. Kim, "Threat analysis on NEtwork MObility (NEMO)," in *Information and Communications Security. ICICS 2004. Lecture Notes in Computer Science*, J. Lopez, S. Qing, and E. Okamoto, Eds., Springer, Berlin, Heidelberg, 2004.

[20] M. Y. Rhee, "Network layer security," in *Wireless Mobile Internet Security*, p. 528, Wiley Telecom, Washington, DC, USA, 2013.

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

[22] E. Perera, V. Sivaraman, and A. Seneviratne, "Survey on network mobility support," *SIGMOBILE Mobile Computing and Communications Review*, vol. 8, no. 2, pp. 7–19, 2004.

[23] V. Raju R, K. Garg, A. K. Dahiya, and J. Kuriakose, "A review on host vs. Network Mobility (NEMO) handoff techniques in heterogeneous network," in *Proceedings of the 3rd International Conference on Reliability*, pp. 1–5, Infocom Technologies and Optimization, Noida, India, October 2014.

[24] A. Walid, A. Kobbane, A. Mabrouk, E. Sabir, T. Taleb, and M. El Koutbi, "Group vertical handoff management in heterogeneous networks," *Wireless Communications and Mobile Computing*, vol. 16, no. 10, Article ID 12561270, 2015.

[25] K. S. Munasinghe and A. Jamalipour, "NEtwork MObility (NEMO) support in interworking heterogeneous mobile networks," in *Proceedings of the 2010 IEEE Wireless Communication and Networking Conference*, pp. 1–6, IEEE, Sydney, Australia, April 2010.

[26] L. M.-B. Ahmed and D. Gati, "An intelligent agentbased scheme for vertical handover management across heterogeneous networks," *Annals of Telecommunications-Annales Des Telecommunications*, vol. 66, pp. 583–602, 2011.

[27] M. Ali Hassoune, Z. Mekkakia Maaza, and S. M. Senouci, "Vertical Handover Decision Algorithm for Multimedia Streaming in VANET," *Wireless Peers Communication*, vol. 95, no. 4, pp. 4281–4299, 2017.

[28] A. Çalhan and C. Çeken, ""Artificial neural network based vertical handoff algorithm for reducing handoff latency" wireless," *Peers Communication*, vol. 71, no. 4, pp. 2399–2415, 2013.

[29] S. Liu, Z. Zheng, and S. Pan, "A novel PROMSIS vertical handoff decision algorithm for heterogeneous wireless networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 9, 2013.

[30] Y.-S. Kim, D.-H. Kwon, and Y.-J. Suh, "A client-based vertical handoff approach for seamless mobility in next generation wireless networks," in *Proceedings of the 2008 33rd IEEE Conference on Local Computer Networks (LCN)*, pp. 419–426, Montreal, Canada, October 2008.

[31] P. Goyal, D. K. Lobiyal, and C. P. Katti, "Dynamic user preference based network selection for vertical handoff in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 98, no. 1, pp. 725–742, 2018.

[32] D. He, C. Chi, S. Chan et al., "A simple and robust vertical handoff algorithm for heterogeneous wireless mobile networks," *Wireless Personal Communications*, vol. 59, no. 2, pp. 361–373, 2011.

[33] X. Liu and L. J. Jiang, "A novel vertical handoff algorithm based on fuzzy logic in aid of grey prediction theory in wireless heterogeneous networks," *Journal of Shanghai Jiaotong University*, vol. 17, no. 1, pp. 25–30, 2012.

[34] N. Omheni, F. Zarai, M. S. Obaidat, K. Hsiao, and L. Kamoun, "A novel media independent handover-based approach for vertical handover over heterogeneous wireless networks," *International Journal of Communication Systems*, vol. 27, pp. 811–824, 2014.

[35] S. Dhar Roy and S. R. Vamshidhar Reddy, "Signal strength ratio based vertical handoff decision algorithms in integrated heterogeneous networks," *Wireless Personal Communications*, vol. 77, no. 4, pp. 2565–2585, 2014.

[36] J. Koo, S. Oh, and D. Lee, "Authenticated route optimization scheme for network mobility (NEMO) support in heterogeneous networks," *International Journal of Communication Systems*, vol. 23, pp. 1252–1267, 2010.

[37] K. J. Kim and C. L. Dong, "Secure route optimization scheme for network mobility support in heterogeneous mobile networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 331–349, 2017.

[38] M. Calderon, C. J. Bernardos, M. Bagnulo, and I. Soto, "Securing route optimisation in NEMO," in *Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, pp. 248–254, IEEE, Trentino, Italy, April 2005.

[39] M. Jo and H. Inamura, "Secure route optimization for Mobile Network Node using secure address proxying," in *Proceedings of the NOMS 2008 - 2008 IEEE Network Operations and Management Symposium*, pp. 137–143, Salvador, Bahia, April 2008.

[40] C. L. Chen, T. F. Shih, Yu T. Tsai, and D. K. Li, "A bilinear pairing-based dynamic key management and authentication for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 534657, 14 pages, 2015.

[41] L. Y. Yeh, C. C. Yang, J. G. Chang, and Y. L. Tsai, "A secure and efficient batch binding update scheme for route optimization of nested NEtwork MObility (NEMO) in VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 284–292, 2013.

[42] H. Yu, Y. Ma, and J. Yu, "Network selection algorithm for multiservice multimode terminals in heterogeneous wireless networks," *IEEE Access*, vol. 7, pp. 46240–46260, 2019.

[43] R. Vikram Raju, U. Rawat, and K. Garg, "A bilinear pairing based key management security scheme to NEMO in heterogeneous networks," in *Proceedings of the Fourth International Conference on Engineering & MIS 2018 (ICEMIS '18)*, Association for Computing Machinery, Istanbul, Turkey, June 2018.

[44] V. R. Reddicherla, U. Rawat, and K. Garg, "Securing NEMO using a bilinear pairing-based 3-party key exchange (3PKE-NEMO) in heterogeneous networks," *Foundations of Science*, vol. 25, pp. 1125–1146, 2020.

[45] V. Chauhan, N. Pal, R. V. Raju, S. Joshi, and R. Bhatnagar, "A new method for minimizing unnecessary handoff in 802.11," in *Proceedings of the 2017 IEEE 7th International Advance Computing Conference (IACC)*, pp. 349–354, Hyderabad, India, January 2017.

[46] J. Sun, Z. Qian, X. Wang, and X. Wang, "ES-DQN based vertical handoff algorithm for heterogeneous wireless networks," *IEEE Wireless Communications Letters*, vol. 9, no. 8, 2020.

[47] C. Xue, W. Li, L. Yu, J. Shang, X. Chen, and S. Lu, "SERO: a model-driven seamless roaming framework for wireless mesh network with multipath tcp," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1284–1296, 2019.

[48] X. Zhang, H. Zhang, W. Liu, B. Song, H. Zhang, and S. Zhu, "An optimal transmission channel selection algorithm for emergency communication," in *Proceedings of the 6th International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS)*, pp. 27–30, Chongqing, China, September.

[49] R. Kong and H. Zhou, "Analysis and improvement of Return routability procedure for network mobility," in *Proceedings of the 2006 International Conference on Wireless Communications*, pp. 1–4, Networking and Mobile Computing, Wuhan, China, July 2006.

[50] A. Joux, "A one round protocol for tripartite diffie–hellman," in *Proceedings of the International Algorithmic Number Theory Symposium ANTS 2000 Lecture Notes in Computer Science*, Springer, Leiden, Netherland, July 2000.

[51] I. Teerewat and H. Ekram, *Introduction to Network Simulator NS2 Ser. Springer Link*, Springer, Bücher, Germany, 2012.
[52] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 22–33, 2020.
[53] M. Kaur and D. Singh, "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption," *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.
[54] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Transactions on Intelligence Technology*, vol. 5, no. 1, pp. 55–65, 2020.
[55] M. Kaur, D. Singh, and V. Kumar, "Color image encryption using minimax differential evolution-based 7D hyper-chaotic map," *Applied Physics B*, vol. 126, no. 9, pp. 1–19, 2020.
[56] B. Gupta, M. Tiwari, and S. S. Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.
[57] M. Kaur, D. Singh, and R. Singh Uppal, "Parallel strength Pareto evolutionary algorithm-II based image encryption," *IET Image Processing*, vol. 14, no. 6, pp. 1015–1026, 2020.