International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Survey of Mobile IP Protocols

Yunes Abdussalam Amgahd[#*] and Raghav Yadav[#]

[#]Computer Science and Information Technology, SHIATS-DU, Allahabad, India

Accepted 11 Jan 2016, Available online 16 Jan 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

In recent years, for protecting Mobile Internet Protocol, considerable researches have been made to develop various security protocols. In order to fully understand the security implications of the design constraints, it is necessary to briefly analyze the existing works on providing security in Mobile IP network. Moreover, there is no combined survey of handoff, routing, and security mechanisms in Mobile IP networks. In this paper, we present a detailed investigation of current state-of-the-art Mobile IP protocols in Mobile IP networks. Initially, the existing works on routing and handoff are discussed. After that, the existing security mechanisms are analyzed by categorizing the security mechanisms as security on route optimization and security during handoff. A brief outline of the key concept, metrics used, as well as the advantages and drawbacks of each discussed mechanism are given. Finally, the comparison table is constructed to summarize several mechanisms.

Keywords: *Mobile IP, Hand-off, Routing protocol, MANET and WSN.*

1. Introduction

1.1. Mobile IP Network

Mobile IP networks deliver mobility support to the existing IP infrastructure without the requirement of modifying applications, fixed-end hosts, and routers. Fixed-end hosts can offer additional support to optimize the route. IPv6 is an improved version of IPv4, and it can operate better with IPv4 to provide significant internetworking capabilities when compared with IPv4. In addition to this, IPv6 can resolve the unanticipated IPv4 design problems and takes the Internet to the next generation. It can achieve increased ability, scalability, quality of service (QOS), end-to-end interworking, and commercial-grade robustness for mobile connectivity, data communication, and voice over IP.

1.2. Issues in Mobile IP Network

Although MIPv6 has a lot of features when compared to MIPv4, it suffers from various security threats.

- As route optimization did not have any authentication mechanism between MN and CN, it becomes insecure.
- During connection hijacking, attacker can redirect the packets to the random non-existent address by hijacking the existing BU between two nodes to disturb the communication.
- In denial of service attacks, the attacker makes the resources unavailable to the intended users. They can also spoof BU to redirect data packets to random address, thus causing congestion in the network.
- Eavesdropping attack occurs when the attacker begins to listen to the traffic and obtain the essential information that is transferred between two other nodes (Vishwajit, *et al*, 2012).
- Impersonation attacks occur when the attacker can utilize some modifying tools to set any desired IP address in the packet.

Sometimes, the tunnels between the mobile device and the HA are attacked to make it appear that the mobile node (MN) is sending traffic when it is not.

1.3 Routing in Mobile IP Network

Some of the basic assumptions made in mobile IP are as follows:

(i) node is identified by its current location during routing; hence, its IP address should be changed when it moves and (ii) routing infrastructure is deliver packets to their intended destinations that is identified by their address.

When the mobile device leaves its network and connects to another network, it acquires a new care-of-address and informs the home agent (HA) about this. After that, HA records the new care-of address in its

*Corresponding author: **Yunes Abdussalam Amgahd**

binding table. MIPv6 routes the packet between mobile device and the correspondent nodes that existed on the IPv6 network. The correspondent node caches the care-of address using route optimization and transfers the packets directly to the mobile device.

1.4 Handoff Mechanism

Handoff is defined as the process of varying the channel (spreading code, time slot, frequency, or combination of them) associated with the current connection even when a call is in progress. Handoff can be started while crossing a cell boundary or during deterioration in signal quality of the current channel. In other words, it is defined as the process in which a MN can create a new connection and separate from its old connection.

Handoff has high handover latency and high packet loss rate by using mobile IP in a mobile computing environment. By configuring new IP addresses before entering the new subnet, fast handovers can reduce the handover latency. Hierarchical MIPv6 mobility management (HMIPv6) can reduce the registration latency and the outdated care-of address's possibility by introducing a hierarchy of mobile agents.

In order to improve the performance, HMIPv6 and fast handover can be combined. However, mobile IP cannot be completely solved the problem of high latency, and also the resulting packet loss rate is still high. In terms of high latency and packet loss, the deficiencies of the network layer-based Mobile IP becomes clear as the percentage of real-time traffic over wireless networks is gradually increasing. While performing handoff, security must be provided for avoiding the attacker nodes' entry inside the network.

1.5 Security in Mobile IP

While designing IPv6 security mechanism, one should be aware of the following aspects:

- Protecting host from scanning and attacking and also IPv6 packets
- Protecting and controlling the traffic that is exchanged with the Internet.
- Providing authorization for automatically assigned addresses and configurations.
- Providing prevention systems such as Firewalls and intrusion detection.

Hence, in this paper, a detailed investigation of current state-of-the-art mobile IP protocols is discussed in Mobile IP networks. Initially, the existing works on routing and handoff are surveyed. In addition, the security mechanisms are categorized as security on route optimization and security during handoff. Finally, the existing approaches are compared to obtain a clear idea about designing routing, handoff and security mechanisms in mobile IP.

The remainder of this paper is organized as follows. Section 2 presents the analysis of the existing works that discuss about various routing, handoff, and security issues and mechanisms. The survey of the existing mechanisms is given in section 3. Section 4 presents a comparison table that summarizes the survey. Finally, section 5 concludes the paper.

2. Related Works

Vishwajit K. Barbudhe and Aumdevi K. Barbudhe have discussed Mobile IPv6 and various threats associated with it. These threats can prevent secure communication in mobile IPv6-based nodes. Some methodologies such as IPSec, cryptographically generated addresses and so forth are discussed to make the communication secure. On studying the existing MIPv6 security mechanism, the security mechanism has been proposed that integrates all the security enhancing techniques and provide better security to MIPv6.

(Kostas, *et al*,2009) have described the design and implementation of secure mobile IP architecture (SMA) for mobile IP services, which is a complete operational system. This system supports the functionality of major requirement of IP. It can achieve significant results for interesting aspects of transparent mobile connectivity. SMA depends on standard software components and it is platform independent as it supports the common operation systems. The architecture is tested on heterogeneous networks built with nodes running Linux, Solaris, and MS-Windows using both wired and wireless networks (Rathi et.al 2009) have proposed a fault-tolerant and secure framework for the networks based on mobile IPv6. This framework depends on inter-home link HA redundancy scheme and self-certified keys. The performance analysis shows that this approach has less overhead, better survivability, transparent failure detection and recovery, less system complexity and workload, and secure data transfer. Moreover, this approach is compatible with the existing mobile IP standard and does not require any architectural changes. However, there is no load balancing mechanism (Chunming et.al 2004) have surveyed the existing handoff schemes for IP-Based 4G mobile networks. Three handover algorithms are considered: Mobile IPv6 protocol, Hierarchical Mobile IPv6 protocol (HMIPv6) and IDMP-based fast handoffs. Mobile IPv6 protocols define a care-of address for MN in a new visited network. The binding between MN's home address and its care-of address is often updated to keep communication continuous. However, an MN needs to spend time in exchanging information between MN and its HA whenever its access point changes, which in turn causes a lot of traffic and packet loss, especially for high-speed multimedia applications. Although HMIPv6 and IDMP-based Fast handoff have improved handoff latency in 4G systems in some aspects, they also bring other new obstacles in handoff procedures. Those issues are not considered here.

Hero Modares *et.al* has presented an overview of the MIPv6 protocol. Moreover, using the location management, potential attacks and security threats along with the security services and requirements necessary are discussed. It studied several existing

protocols that provide some degree of protection during the correspondent registration phase of MIPv6. It is concluded that BU message should be designed on a case-by-case basis to reduce iterating steps throughout the entire protocol. Redundant repetition of sections is avoided in the protocol, and efficiency will be enhanced in response to the diminished step iteration. The correspondent registration protocol helps complete the registration procedure and reduces the computing cost of the MN. However, it did not provide any secure connection between MNs and CNs to protect BU messages against a number of devastating attacks on Mobile IPv6.

3. Survey on Mobile IP Protocols

In this section, the existing mobile IP protocols are briefly analyzed. For easy understanding, the mobile IP protocols are classified as routing protocols, handoff protocols, and security protocols. The methodologies used, advantages, and disadvantages are analyzed below.

3.1 Survey on Routing Protocols in Mobile IP Network

The existing routing protocols in Mobile IP networks are discussed below.

3.1.1 Improved Tunneling-Based Route Optimization Mechanism

Here, the performance of both standard Mobile IPv6 routing mechanisms and tunneling-based route optimization techniques are analyzed. After that, improved tunneling-based route optimization mechanism is proposed that reduces the packet overhead. For maintaining the compatibility with standard mechanisms, the tunnel manager should be changed and binding update messages must be altered. When comparing with bidirectional tunneling, route optimization and tunneling-based route optimization, the improved tunneling-based route optimization shows the reduced packet overhead. Due to less overhead for each packet, more data can be transmitted through network in case of a Mobile IP communication. The performance metrics used are overhead and delay. However, the total delay is same as that of the bidirectional tunneling, route optimization and tunneling-based route optimization mechanisms. It must be reduced.

3.1.2 Using Correspondent Information for Route Optimization Scheme

Correspondent Information Route Optimization scheme is proposed that exclude the inefficient routing paths by creating the shortest routing path in order to address the triangle routing problem. Liebsch's route optimization had heavy signaling cost among three route optimization schemes, whereas Dutta's route optimization scheme had light signaling cost among three route optimization schemes on one-path communication, but Dutta's route optimization scheme did not have binding process between MAGs, causing Duuta's route optimization scheme less accurate. The results of signaling cost performance evaluation show that performance of this scheme is better than Liebsch's route optimization scheme as 45% for mobility of the data packets sender and Dutta's route optimization scheme as 20% for mobility of the data packets sender. The performance metrics used are mobility and overhead. However, while transporting correspondent information from LMA to MAG, there is no ACK message. Hence, LMA did not know whether the binding process was complete or not. But, if the binding process was uncompleted, then LMA re-transport correspondent message on next data transmission, accordingly not too extreme on correspondent information's loss for route optimization.

3.1.3 A TOTP-Based Enhanced Route Optimization Procedure

Time-based one-time password route optimization (TOTP-RO) can overcome the problems such as longer service disruption and high overhead in case of mobile IPv6. Along with the computation of the shared secret token and authentication via TOTP technique, the correspondent node compatibility test was executed to diminish the handover signaling and delay when the correspondent node does not have an active implementation of mobile IPv6. Authentication of MN's was done via a shared secret token and TOTP that resulted in direct authentication of MN and reduced overall service disruption for real-time applications. The performance metrics are handover delay, packet loss, service disruption delay and signaling overhead. With respect to the performance metrics, TOTP-RO has considerably improved the performance. Result show that the authentication overhead has been reduced to 0% when compared to the existing procedures in which it was around 75%. However, it has more service disruption delay and overhead in the network.

3.1.4 Global Connectivity for Mobile IPv6-based Ad Hoc Networks

A self-organizing, self-addressing, and self-routing IPv6-enabled MANET infrastructure, IPv6-based MANET has been proposed to overcome the problem of connecting MANETs to global IPv6 networks by supporting IPv6 mobility. It organizes the nodes automatically into tree architecture as well as configures their global IPv6 addresses. Unicast and multicast routing protocols are designed for IPv6-based MANET on the basis of the soft-state routing cache and longest prefix matching. Mobile IPv6 is also supported, and a peer-to-peer information sharing system is designed. In order to demonstrate the possibility and efficiency of P2P information sharing system and IPv6-based MANET, a prototyping system can be implemented. The performance metrics used

are number of packets, average file search, retrieval delay. Results show the efficiency of this routing protocol and the P2P file sharing system. However, the power consumption is more.

3.1.5 Right-time Path Switching Method for Proxy Mobile IPv6 Route Optimization

A right-time path switching method has been proposed for PMIPv6 route optimization. Once the optimized path is ready, this method initiates the path switch using signaling messages. This feature prevents out-of-sequence packets and minimizes disruption duration in the route optimization procedure. This procedure is evaluated in an experimental test-bed using actual PCs. The results reveal that this method prevents out-of-sequence packets while the baseline route optimization procedure causes them. In addition, performance evaluation shows that this method can reduce the communication disruption duration in the route optimization procedure. Moreover, this method has performance improvement in TCP throughput or seamless continuity of real-time applications during the route optimization procedure. The performance metrics used are communication disruption duration, delay gap, number of out-of-sequence packets. However, it may be affected by malicious nodes in the network.

3.1.6 Smart Routers for Cross-Layer Integrated Mobility and Service Management

DMAPwSR is a cross-layer integrated mobility and service management scheme in Mobile IPv6 environments that can be used to lessen the overall mobility and service management cost for serving the mobile users with service characteristics and diverse mobility. To select the smart routers to be its dynamic mobility anchor points (DMAPs), each MN can use its cross-layer knowledge. This can be performed to balance the cost associated with packet delivery services Vs mobility services. For MIPv6 systems, these smart routers act as access routers. They can process the binding messages from the MN. After processing, it can store the MN's present location in the routing table for forwarding service packets that are destined to the MN. As the MN roams across the MIPv6 network, MN's DMAP varies dynamically; moreover, DMAP service area also varies dynamically, reflecting the dynamic MN's mobility and service behaviors. In contrast to HMIPv6, DMAPwSR considers the integrated service management and mobility. On the basis of stochastic Petri nets, an analytical model is developed for analyzing DMAPwSR and comparing its performance against MIPv6 and HMIPv6. The performance metrics are network cost. However, it has load-balancing issues during DMAP selection, and several performance metrics are not considered (Jabir. *et al*, 2012).

3.1.7 Route Optimization for Mobile IP

Route Optimization protocol is largely concerned with supplying a binding update to any correspondent node that needs one (and can process it correctly). The binding update message is used along with the previous foreign agent notification extension to allow for smooth handoffs between foreign agents. Further, some methods are presented for establishing registration keys for use by MNs and foreign agents supporting smooth handoffs. The detailed processing requirements are given for MNs, foreign agents, and HAs. Finally, the essential features of route optimization, as realized in IPv6, have been identified. The differences between IPv4 and IPv6 is discussed, with the hope that in so doing, the design space for Route Optimization will be more fully understood, and that IPv6's ability to support mobility will be more fully appreciated. However, there is no security while optimizing routes (Chuang, *et al*,2013).

3.1.8. Perceptive Approach for Route Optimization in Mobile IP

An efficient approach is proposed to overcome with triangular routing problem in Mobile IP network. Unlike the conventional Mobile IP network, all the binding update of the MN sends to the top-level routers of the network instead of the individual correspondent node. Compare to the other proposals, this mechanism increases the availability of the binding updates, which gives a better scalability. This mechanism can be applied on internetwork and intra network. This mechanism can reduce packet delay, packet loss during handoff, and registration time. However, the effect of this technique network mobility is not discussed.

3.2 Survey on Handoff Protocols in Mobile IP Network

The existing handoff protocols in Mobile IP networks are discussed below.

3.2.1 Cluster-Based Proxy Mobile IPv6 for IP-WSNs

Cluster-based sensor proxy mobile IPv6 (CSPMIPV6) can overcome the problems such as bottleneck, long-handoff latency, and route optimization. Here, the mobility access gateways (MAGs) are grouped into clusters; each cluster has a cluster Head MAG that is used to minimize the load on LMA with the help of intracluster handoff signaling and an optimized path for data communications. The performance metrics are LMA load, local handoff delay, and transmission cost. Results show that CSPMIPv6 outperforms both SPMIPv6 and PMIPv6 protocols in terms of the performance metrics. However, the other metrics such as overhead, energy consumption and so forth are not considered (Jerusha, *et al*, 2014).

3.2.2 Evaluation of Mobile IPV6 Protocols in Handover and Under Dos Attacks

Mobile IPv6 and its extensions like fast Mobile IPv6 and hierarchical Mobile IPv6 have been developed as host-based mobility management protocols. The network-based mobility management protocols such as

PMIPv6 and fast FPMIPv6 have been standardized, even though the host-based mobility management protocols were being enhanced. On the basis of handoff parameters such as handover latency, handover blocking probability, and packet loss, this system analyses the IPv6 protocols' performance. Results show that these systems can enhance the protocols performance under denial of service attack that is common in black hole attack scenario. Several analysis made are packet loss analysis, handover blocking probability analysis, and handover latency analysis. The performance metrics used are packet loss, handover latency, and handover blocking probability. However, several other parameters such as overhead, power consumption are not analyzed.

3.2.3 Improvement in the Mobility of Mobile IPv6 based Mobile Networks Using Reverse Routing Header Protocol and Fast Handoff

A wired-wireless scenario that utilizes the TCP in order to implement a fast handover is incorporated with network mobility (NEMO) for improving the mobility of the network. For solving the reverse tunneling and high data loss of NEMO, the reverse routing header (RRH) protocol is proposed as an extension. This extended protocol can allow for acknowledgments to be sent until the session completes. The performance is analyzed in terms of performance metrics such as throughput and average delay and it is concluded that the fast handover of Mobile IPv6 along with the RRH improves the performance in scenarios with CBR traffic. There is a need to conduct further testing with various types of application traffic to observe the performance of this system. The performance metrics used are throughput and average delay. However, it is not applied to real world architectures.

3.2.4 Flow-Based Fast Handover Method

Flow-based fast handover method in mobile IPv6 (FFHMIPv6) is proposed, and it is compared with both MIPv6 and HMIPv6 methods. Both in the best and the worst case handover scenarios, the analysis was performed. In addition, the handover time is significantly shorter by using FFHMIPv6 method when compared with MIPv6 and HMIPv6 methods. This method requires small changes in the MIPv6 protocol and has some computational and memory requirements. When the traffic flow property of IPv6 protocol is used, the IPv6 traffic flows' state information is implemented in all routers. Hence, this method can be implemented in mobile IPv6. The performance metrics used are handover delay, packet loss and required processing time. Results show that this method has less handover delay, processing time, and packet loss. However, overhead is increased.

3.2.5 Seamless Multimedia Handoff for Hierarchical Mobile IPv6

Hierarchical mobile IPv6 and predictive address reservation schemes are proposed in order to reduce the handoff latency in their own ways. The hierarchical mobile IPv6 allows reducing handoff latency and overhead, whereas predictive address reservation and anticipated handover use link layer information for earlier movement detection and address configuration for the new point of attachment for minimizing the disruption of the services during the handoff process. The integration of anticipated buffering reduces significantly the handoff packet losses during the handover process, but its integration with the HMIPv6 environment provides better handoff performance. Performance results will be provided in terms of handoff latency, packet loss, and jitter. However, it has more overhead and power consumption.

3.2.6 Design and Implementation of Mobile IPv6 Data Communication in Dual Networks

Dual stack mobile IPv6 is an extension of mobile IPv6, which can support devices' mobility in both IPv4 and IPv6 networks and can be implemented by combining several different modules. Behind the Network Address Translation (NAT), IPv4 private networks are present. It should be encapsulated in user datagram protocol (UDP) packets to bypass the binding update and binding acknowledgment using NAT. Hence, NAT traversal and detection can be supported by the dual stack mobile IPv6; therefore, MN can move freely from IPv6 to IPv4 network or vice-versa. In dual stack mobile IPv6; NAT module can perform the handover process without breaking the network connectivity. However, the transition from IPv4 to IPv6 will be time consuming; it will reduce the performance.

3.2.7 SF-PMIPv6: A secure fast handover mechanism

SF-PMIPv6 is a secure fast handover scheme for PMIPv6 networks that uses a buffer mechanism to prevent packet loss and avoid the out-of-sequence packet problem. It also performs a pre-handover procedure to reduce handover latency, utilizes a piggyback technique to reduce the signaling cost, and performs local authentication to reduce the authentication latency. The authentication procedure satisfies the security requirements such as anonymity, location intractability, mutual authentication to prevent several attacks, session key agreement, and no clock synchronization problem. Results demonstrate that the SF-PMIPv6 protocol provides a better solution than existing schemes. The performance metrics used are packet loss, handover latency, signaling cost, and authentication latency. However, the route optimization problem of network mobility protocol is not solved. Moreover, QoS requirements such as end-to-end transmission delay, jitter, and packet loss ratio are not discussed.

3.2.8 Cross-Layer Scheme for Handover in 802.16e Network with F-HMIPv6 Mobility

In order to achieve a better transmission performance by reconstructing handover procedures of 802.16e and fast handover hierarchical MIPv6 (F-HMIPv6), a cross-

layer scheme for handover has been proposed in 802.16e network along with F-HMIPv6 mobility. Cross-layer design refines the surviving handover techniques in 802.16e MAC layer and F-HMIPv6. Layer 2 and 3 signaling messages for handover are analyzed and combined to increase the handover performance. The performance metrics used are transmission performance and handover performance. However, the selection mechanism of an appropriate base station (BS) is not within our consideration for simulation simplification. In addition, the cross layer design did not cover the complete handover procedure and did not optimize the utilization of network resources.

3.2.9 Handover Management Scheme for Mobile IPv6 Networks

Crossover MAP-based hierarchical mobile IPv6 (HMIPv6) can reduce the signaling load for inter-domain mobility HMIPv6. Along with the existing handover management protocols, an analytical model is incorporated for the performance analysis of crossover MAP-based HMIPv6. Finally, results are analyzed in different environments and compared with the existing protocols. The performance metrics used are handover latency. The analytical model results show that this scheme performs as [F+H] MIPv6 by reducing handover latency and outperforms HMIPv6 and MIPv6. However, this method did not analyze the performance of the upper-layer protocol such as TCP, UDP, and so forth. Moreover, it did not consider the technique that can remove the packet delivery cost.

3.2.10 IPv6 Flow Handoff in Ad Hoc Wireless Networks Using Mobility Prediction

IPv6 flow handoff in ad hoc wireless networks using mobility prediction is used to anticipate the topological changes and to minimize the disruption of the connection caused by mobility. Various simulation experiments were conducted comparing the proposed scheme with other protocols. Under high mobility conditions, this scheme maintains low delay while minimizing throughput degradation. More importantly, Flow Oriented Routing Protocol (FORP) minimizes the control O/H. Thus, this scheme is suitable for real time IPv6 flows in highly ad hoc mobile wireless networks. Simulation results show that FORP has the highest throughput even at very high mobility when compared to the lightweight mobile routing and destination sequenced distance vector (DSDV). The performance metrics used are delay and throughput. However, the delay produced by FORP is greater when compared to DSDV method. This technique did not consider the propagation model that contains fading. Fading may cause several problems due to the unpredictable nature.

3.2.11. Framework of Handoffs in Wireless Overlay Networks Based on Mobile IPv6

In wireless overlay networks based on mobile IPv6, a framework of handoffs has been proposed and the problems regarding horizontal and vertical handoffs and the integrated WLAN and WAAN networks' architecture based on mobile IPv6 are discussed. HiMIPv6+ is a mobility management scheme that reduces the signaling overhead on the Internet and packet loss during handoff. It eases the HA's and CN's loads and interoperates with mobile IPv6 nodes. WLAN bandwidth measurement is defined using handoff decision algorithm. Wireless network transport capability and user service requirement are considered by QoS-based vertical handoff algorithm, and MN selects a suitable access network and makes vertical handoff at the appropriate time. The performance metrics used are signaling overhead and packet loss. The performance of this framework is analyzed by prototype evaluations and simulations. However, several QOS parameters such as degree of congestion, and the packet loss rate are not considered.

3.2.12 Cross-Layer Partner-Based Fast Handoff Mechanism

A cross-layer partner-based fast hand-off mechanism based on HMIPv6 is called as PHMIPv6 protocol. Their PHMIPv6 protocol is a cross-layer, layer-2 + layer-3, approach. A new node, called partner node is adopted in PHMIPv6 protocol. Layer-2 trigger scheme in PHMIPv6 protocol is used to accurately predict the next Access Point (AP) and to invite a possible partner node in the area of the next AP. With the aid of the partner node, CoA can be pre-acquired and Duplicate Address Detection (DAD) operation can be pre-executed by the partner node before the MN initializes the hand-off request. PHMIPv6 protocol can significantly reduce the hand-off delay time and packet losses. The experimental results also illustrate that PHMIPv6 protocol actually achieves the performance improvements in the handoff delay time, the packet loss rate, and the hand-off delay jitter [40]. The performance metrics used are handoff delay time, packet loss rate, and hand-off delay jitter. However, there is no security mechanism discussed.

3.3 Survey on Mobile IP Security

The existing security mechanisms in Mobile IP are broadly classified based on the purpose for which it is used. They are

1) Security on Route Optimization
2) Security during Handoff

Security on Route Optimization

3.3.1 Enhancing Security in Mobile IP

This is a lightweight protocol that has some strong security features in order to protect the binding update (BU) messages. This protocol utilizes IPv6 address format for providing communication between MN and CN to secure the BU framework. Furthermore, this

protocol dealt with several attacks on MN and CN namely false BU attack, man-in-the-middle attack, and denial-of-service attacks. When MN and CN send the control signal to each other through route optimization, there are no shared secrets or trusted certificates during communication between MN and CN. Return route ability (RR) is standardized to protect control messages in RO and to prevent third party attacks. This protocol has low latency, ensures faster handover, and provides efficient communication. However, RR can be easily broken by the attacker.

3.3.2 Robust Secured Mechanism for Mobile IPv6 Threats

Methodologies such as IPSec and cryptographically generated addresses are discussed for providing secure communication. After that, a security mechanism can be used for encryption of message and secret key shared by the communicating users before and after packet transmission. This mechanism is computationally efficient in detection, prevention, and recovery of probable threats in mobile IPv6. This mechanism can discriminate both unsecured and secured transmission and administer total communication during the data delivery. It can improve the security by providing the protection in terms of authentication, confidentiality and key exchange. However, there is no implementation of this security mechanism.

3.3.3 Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption

In this approach, identity-based encryption (IBE) can be applied using IBE-based authentication in the four-way IKE handshake instead of X.509 certificate-based authentication. IBE can also be applied by embedding IBE-based key agreement method in EAP. IBE-authentication can be implemented between MN and HA and between MN and CN. They considered the environments in which MN and CN use the same Public Key Generator (PKG) different PKGs. Finally, the performance evaluation of the signaling protocols is performed. The performance measurements show that costs of pairing-based cryptographic IBE operations are higher than that of RSA/DSA/ECC-based cryptographic operations in a PKI. However, there is not security analysis of the used protocols.

3.3.4 Improved Security Mechanism for Mobile IPv6

In order to improve the security and performance of the return route ability procedure, hash chain-based security mechanism has been proposed in mobile IPv6. Hash chain element can be used by this authentication mechanism as an extra certificate to MN in providing authentication on binding updates, while running the routing process. By eliminating the necessity of the home test procedure in the RR test, this mechanism can lessen the binding update latency. This mechanism's security strength can be analyzed under different adversary scenarios. When compared with the original RR test, it reduces the average latency of binding updates, the threats from adversaries between the HAs and CNs, the probability of authentication packets traversing the home network and the HA's burden. However, there is no mechanism to detect and recover from several types of attacks.

3.3.5 MIPv6 Route Optimization Security Design

MIPv6 Route Optimization Security Design discusses the security design rationale for mobile IPv6 route optimization and defines the problems related to mobility. After that, they provided an overview of the actual mechanisms used. This design was never intended to be fully secure. Instead, the goal was to provide security as immobile IPv4. Simulation result shows that this design is slightly less secure than IPv4; however, the difference is negligible and most likely to be insignificant in real life. The route optimization based security mechanisms are also provided. However, there is no new mechanism that provides security.

3.3.6 Public-Key Based Secure Mobile IP

Public key-based management satisfies the mobile IP's security requirements by protecting packet redirection with IPSec protocols and authenticating mobile IP control messages. They tested its first prototype on a test bed with a HA, five wireless MNs, and five foreign agents. They demonstrated both authenticated registration and end-to-end IPSec tunneling. In scalable implementations of secure route-optimized mobile IP and IPSec-supported virtual private networking of mobile IP traffic, this scheme is utilized. However, it did not contain an efficient management of security associations based on security policies of network domains.

3.3.7 Improved Authentication Scheme of Binding Update Protocol

This is an efficient and secure Ticket based Binding Update (TBU) protocol for MIPv6 networks. When MN first executes the binding update (BU), its correspondent node (CN) issues a ticket to MN. This ticket assists that it is able to do efficiently the BU whenever MN requires the BU for the future. TBU protocol need not be repeated equal BU course whenever the MN moves to foreign link or network and is able to be executed in environment of not operating the HA. It also makes easy scalability. Security analysis is described through attack scenarios by comparing previous protocol schemes. However, the location authentication against requester of BU is not discussed, thereby reducing the security.

3.3.8. Distributed Authentication Mechanism for Mobile IP Route Optimization

The distributed authentication mechanism is presented that can be able to successfully install an

authenticated binding cache at the correspondent node, mapping the mobile host to its current care-of address. This care-of address can be used by the correspondent node to directly tunnel packets destined to the mobile host, to its care-of address. The authentication mechanism is robust, efficient, involves minimum overhead, and requires no additional infrastructure support. The solution is scalable and distributed and does not require pre-configuration of a shared secret key between the HA and the correspondent node. However, several Q0S parameters are not considered that may reduce the network performance.

Security during Handoff

3.3.9 Enhancing MISP with Fast Mobile IPv6 Security

A secure fast handover scheme is proposed that combines the advantages of MIS protocol (MISP) and fast mobile IP (FMIPv6). This scheme is robust against session key, off-line dictionary, and DOS attacks, although it provides the reduced handover latency when compared with the existing scheme. The security correctness of this scheme has been verified through the formal security analysis with BAN-Logic. This scheme is based on FMIPv6, which is a host-based mobility support protocol. The recent approach for mobility support is network-based mobility support wherein a MN is not involved in any mobility signaling. However, they did not study the applicability of this scheme to network-based mobility support.

3.2.10 Enhanced Security Scheme for Fast Handover

This enhanced security scheme for fast handover (ESS-FH) is proposed in hierarchical mobile IPv6. It uses cryptographically generated address (CGA) method and public key cryptography in order to provide strong key exchange and key independence. Simultaneously, it defends against the DoS and redirection attacks. In ESS-FH, handover occurs fast even when the MNs perform inter-handover between different hierarchical mobile IPv6 domains. Formal security analysis and performance analysis is made to show its superiority. Results show that this scheme achieves high efficiency and strong security. However, latency is more.

3.2.11 Enhancing SVO Logic for Mobile IPv6 Security Protocols

This is an extension of SVO logic in order to achieve the true formal verification on the mobile IPv6 security protocols. Some new notations and axioms that support the new security features typically adopted by mobile IPv6 security protocols are defined. This logic was applied for formally analyzing the four security protocols, that is, child-proof authentication for mobile IPv6 (CAM), enhanced route optimization for mobile IPv6 (ERO), Kempf-Koodli's protocol (KKP), and You, Hori and Sakurai protocol (YHSP), while showing its effectiveness in precisely reasoning about their security. Finally, its effectiveness is shown by applying it to four security protocols. However, QOS parameters are not considered that reduces the performance.

3.2.12 Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6

Secure relay-assisted handover protocol is a new protocol for reducing handoff delay and packet lost using relay nodes over long-term evolution (LTE) networks. The security issue is considered when selecting relay nodes during handoff. During the relay node discovery, the access network discovery and selection function (ANDSF) in 3GPP specifications are extended to help mobile station or user equipment (UE) to obtain the information of relay nodes. The mobile station or UE performs the pre-handover procedure that includes security operation and proxy binding update using relay nodes for significantly reducing the handover latency and packet loss. Results show that this protocol actually achieves the performance improvements in the handoff delay time and the packet loss rate.

3.2.13 Implication of the Security Key Exchange during Mobile IPv6 Smooth Handoff

This is an enhanced smooth handoff with security consideration for mobile IPv6. MN sends a request forwarding to the old access router before the MN starts to execute the binding update. The key exchange method is also discussed to combine the main mode of IKE and finish handoff during return route ability procedure and key exchange for mobile IPv6. This method can reduce the incidence of out-of-sequence packets and execute Internet key exchange in smooth handoff. Results show that this method establishes a better environment for mobile network. However, the security requirements, such as authentication, integrity etc. are not considered.

3.2.14 Security-Effective Fast Authentication Mechanism for Network Mobility

Under the network evaluation of wired/wireless integration of network mobility supporting mobility and network-based Proxy Mobile IPv6 (PMIPv6), security is reinforced. Symmetric key-based local-lighted authentication mechanism (SK-L2AM) mainly depends on a simple key that minimizes authentication delay costs and code calculation. For reducing reduce handoff delay time in PMIPv6, fast handoff technique is used, and for supporting global mobility, extension of fast handoff for PMIPv6 (X-FPMIPv6) is used. In addition, with the help of piggybacks method, authentication extension X-FPMIPv6 integrated SK-L2AM and X-FPMIPv6 in order to reduce the overhead of authentication and signaling. From the performance analysis, this extension technique shows better authentication and less handoff delay than the existing schemes. However, there is an increased overhead that may reduce the network performance in mobile IP network.

4. Comparison Table

The survey is summarized in the following table

Table1 Comparison Table

Techniques	Category	Performance Metrics	Advantages	Disadvantages
Improved Tunneling-Based Route Optimization Mechanism	Routing	Overhead, delay	Less overhead	More total delay
Using Correspondent Information for Route Optimization Scheme	Routing	Mobility, overhead	Better performance	While transporting correspondent information from LMA to MAG, there is no ACK message
TOTP-Based Enhanced Route Optimization Procedure	Routing	Handover delay, packet loss, service disruption delay and signaling overhead	Improved performance in terms of handover delay, packet loss, and signaling overhead	More service disruption delay and overhead in the network
Global Connectivity for Mobile IPv6-based Ad Hoc Networks	Routing	Number of packets, average file search, retrieval delay	Can solve the issue of connecting MANETs to global IPv6 networks	High power consumption
Right-time Path Switching Method for Proxy Mobile IPv6 Route Optimization	Routing	Communication disruption duration, delay gap, number of out-of-sequence packets	Less communication disruption duration in the route optimization procedure	It may be affected by malicious nodes in the network
Smart Routers for Cross-Layer Integrated Mobility and Service Management	Routing	Overall network cost	Reduce the overall mobility and service management cost for serving mobile users with diverse mobility and service characteristics	Load balancing issues during DMAP selection
Route Optimization for Mobile IP	Routing	-	Enable foreign agents to offer smooth handoffs for mobile nodes	There is no security while optimizing routes
Perceptive Approach for Route Optimization in Mobile IP	Routing	Packet delay, packet loss	Solve triangular routing problem in Mobile IP network. Can be applied on internetwork and intra network. Also, it can reduce packet delay, packet loss during handoff, and registration time.	The effect of this technique network mobility is not discussed
Cluster-Based Proxy Mobile IPv6 for IP-WSNs	Handoff	LMA load, local handoff delay, and transmission cost	Perform well in terms of performance metrics such as LMA load, local handoff delay, and transmission cost	Metrics such as overhead, energy consumption etc., are not considered
Evaluation of Mobile IPV6 Protocols In Handover And Under Dos Attacks	Handoff	Packet loss, handover latency, handover blocking probability	Better performance under denial of service attack that is common in black hole attack scenario	Parameters such as overhead, power consumption are not analyzed
Improvement in the Mobility of Mobile IPv6 Based Mobile Networks Using Reverse Routing Header Protocol And Fast Handoff	Handoff	Throughput and average delay	Fast handover of Mobile IPv6 along with the RRH improves the performance in scenarios with CBR traffic	It is not applied to real world architectures
Flow-Based Fast Handover Method	Handoff	Handover delay, packet loss and required processing time	Less handover delay. Also, perform well in both the best and the worst case handover scenarios	More overhead
Seamless Multimedia Handoff for Hierarchical Mobile IPv6	Handoff	Handoff latency, packet loss, and jitter	Reduce the handoff latency and packet loss along with providing better performance during handoff	More overhead and power consumption
Design and Implementation of Mobile IPv6 Data Communication in Dual Networks	Handoff	-	Support mobility of devices irrespective of IPv4 and IPv6 networks	The transition from IPv4 to IPv6 will be time consuming, that reduces the performance of the network
SF-PMIPv6: A secure fast handover mechanism	Handoff	Packet loss, handover latency, signaling cost, and authentication	Prevent packet loss, avoid the out-of-sequence packet problem, and reduce	The route optimization problem of network mobility protocol is not solved.

		latency.	handover latency, signaling cost, and authentication latency.	Moreover, QOS requirements such as end-to-end transmission delay, jitter, and packet loss ratio are not discussed
Cross-Layer Scheme for Handover in 802.16e Network with F-HMIPv6 Mobility	Handoff	Transmission performance, handover performance	Achieve better transmission performance and optimize the handover performance	The selection mechanism of an appropriate Base Station (BS) is not within our consideration for simulation simplification. Also, the cross layer design did not cover the complete handover procedure and optimize the utilization of network resources
Handover Management Scheme for Mobile IPv6 Networks	Handoff	Handover latency	This scheme performs almost similar to [F+H] MIPv6 in terms of reducing handover latency	This method did not analyze the performance of the upper-layer protocol such as TCP, UDP etc. and not consider the technique to remove the packet delivery cost
IPv6 Flow Handoff in Ad Hoc Wireless Networks Using Mobility Prediction	Handoff	Delay, throughput	Under high mobility conditions, it maintains low delay while minimizing throughput degradation. Suitable for real time IPv6 flows in highly ad hoc mobile wireless networks.	The delay produced by FORP is greater when compared to DSDV method. This technique did not consider the propagation model that contains fading. Fading may cause several problems due to the unpredictable nature.
Framework of Handoffs in Wireless Overlay Networks Based on Mobile IPv6	Handoff	Signaling overhead and packet loss	Reduce the signaling overhead on the Internet and minimize packet loss	Several QoS parameters such as degree of congestion, and the packet loss rate are not considered
Cross-Layer Partner-Based Fast Handoff Mechanism	Handoff	Handoff delay time, the packet loss rate, and the hand-off delay jitter	Accurately predict the next AP, reduce the hand-off delay time and packet losses	No security mechanism
Techniques	**Category**	**Attacks/Security Threats Handled**	**Advantages**	**Disadvantages**
Enhancing Security in Mobile IP	Security on route optimization	False binding update, man-in-the-middle, and denial-of-service attacks	Verify the reach ability of mobile node, have low latency, ensure faster handover, and provide efficient communication	RR can be easily broken by the attacker.
Robust Secured Mechanism for Mobile IPv6 Threats	Security on route optimization	Authentication, confidentiality and integrity	Improved security by providing the protection in terms of authentication, confidentiality and key exchange.	There is no implementation of this security mechanism
Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption	Security on route optimization	Authentication	Provide efficient authentication.	There is not security analysis of the used protocols.
Improved Security Mechanism for Mobile IPv6	Security on route optimization	Authentication and return route ability	Reduce average latency of binding updates, the threats from adversaries on the path between the HAs and CNs, the burden of HA, and the probability of authentication packets traversing the home network	There is no mechanism to detect and recover from several types of attacks.
MIPv6 Route Optimization Security Design	Security on route optimization	-	Better analysis of security rationale.	No new mechanism that provides security is designed.
Public-Key Based Secure Mobile IP	Security on route optimization	Authentication, location management and key management	Scalable implementations of secure route optimized Mobile IP	No efficient management of security associations based on security policies of network domains
Improved Authentication Scheme of Binding Update Protocol	Security on route optimization	Denial of Service (DoS) attack, redirect attack, and neighbor bombing attack	Promote efficiency by reducing iterating courses of entire protocol	The location authentication against requester of BU is not discussed, thereby reducing the security
Enhancing MISP with Fast Mobile IPv6 Security	Security During Handoff	Authentication	Provide network-based mobility support.	Applicability of this scheme to network-based mobility support is not studied.

Enhanced Security Scheme for Fast Handover	Security During Handoff	Denial-of-Service attacks and redirect attacks	Achieve high efficiency and strong security.	More latency.
Enhancing SVO Logic for Mobile IPv6 Security Protocols	Security During Handoff	Redirect attack, man-in-the middle attack, and denial-of-service attack	Achieve true formal verification on the mobile IPv6 security protocols.	QOS parameters are not considered that reduces the performance.
Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6	Security During Handoff	Secure handover and mobility	Achieve performance improvements in the handoff delay time and the packet loss rate.	This protocol increases the overhead that reduces the performance.
Implication of the Security Key Exchange during Mobile IPv6 Smooth Handoff	Security During Handoff	Key exchange	Reduce the incidence of out-of-sequence packets and execute Internet key exchange in smooth handoff.	Security requirements such as authentication, integrity etc., are not considered.
Security-Effective Fast Authentication Mechanism for Network Mobility	Security During Handoff	Calculation costs, authentication latency, handoff latency and signaling cost	Provide authentication and handoff delay	Increased overhead that may reduce the network performance in mobile IP network

Conclusion

In this paper, a detailed investigation of existing routing, handoff, and security mechanisms in Mobile IP networks has been analyzed. Initially, the existing works on routing and handoff are discussed along with their key concept, metrics used, as well as the advantages and drawbacks. In addition, the survey is made by categorizing the security mechanisms as security on route optimization and security during handoff. The comparison table is constructed to summarize several mechanisms. Finally, it can be concluded that this survey can be helpful in developing new techniques by understanding the existing techniques.

References

Chitra Dhawale, Aumdevi K.Barbudhe, Vishwajit K.Barbudhe (2012) A Robust Secured Mechanism for Mobile IPv6 Threats, International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 6, pp.918-921.

Kostos Siozios, Pavlos Efraimidis and Alexnadros Karakos (2002) Design and Implementation of a Secure Mobile IP Architecture.

Rathi S and Thanuskodi K (2009) A Secure and Fault-tolerant framework for Mobile IPv6 based networks, International Journal of Computer Science and Information Security (IJCSIS), Vol. 5, No. 1.

Chunming Liu and Chi Zhou (2004) Challenges and Solutions for Handoff Issues in 4G Wireless Systems An Overview, International Latin American and Caribbean Conference for Engineering and Technology (LACCEI'), 2-4 June 2004, Miami, Florida, USA.

Martin Ehmke and Harri Forsgren (2009) Securing Control Signaling in Mobile IPv6 with Identity-Based Encryption, Issues in Informing Science and Information Technology Volume 6,.

Jing Li, Po Zhang, and Srinivas Sampalli (2008) Improved Security Mechanism for Mobile IPv6, International Journal of Network Security, Vol.6, No.3, PP.291–300,

Pekka Nikander, Jari Arkko, Tuomas Aura and Gabriel Montenegro, Mobile IP version 6 (MIPv6) Route Optimization Security Design.

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan and Isidro Castineyra (1999) A public-key based secure Mobile IP, Wireless Networks 373–390.

Ilsun You, Jong-Hyouk Lee, Yoshiaki Hori and Kouichi Sakurai (2011) Enhancing MISP with Fast Mobile IPv6 Security, Mobile Information Systems 7 271–283.

Ilsun You, Jong-Hyonk Lee, Kouichi Sakurai, Yoshiaki Hori (2010) ESS-FH: Enhanced Security Scheme for Fast Handover in Hierarchical Mobile Ipv6, IEICE Trans. Inf. & Syst., Vol. E93-D, No. 5,.

Adnan J Jabir, Shamala K Subramaniam, Zuriati Z Ahmad and Nor Asilah Wati A Hamid (2012) A cluster-based proxy mobile IPv6 for IP-WSNs, Journal on Wireless Communications and Networking :173.

Anline Jerusha J, K.Seetha Lakshmi (2014) Evaluation of Mobile IPV6 Protocols In Handover And Under Dos Attacks, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Special Issue1.

Authors

Yunes Abdussalam Amgahd is a student of Ph.D in the department of Computer science and Information technology from SHIATS, Allahabad. And also received his M.Tech degree From SHIATS, Allahabad.

Raghav Yadav is an assistant professor in Sam Higginbottom Institute of Agriculture, Technology and Sciences (SHIATS), Allahabad, India. He obtained Ph.D. and M.Tech degree in computer science and engineering from (MNNIT), Allahabad and B.E. degree in electronics engineering from Nagpur University. He guided various project and research at undergraduate and postgraduate level. He has published more than 15 research papers in national/international conferences and refereed journals. His research interests are in the field of optical network survivability, ad-hoc networks, and fault tolerance systems.