1. **CGA Option:** A public-private key pair is generated by all nodes in order to claim an address. CGA option carries the public key and the associated parameters to enable the receiver of ND messages to validate the proper binding between the owner's public key and the CGA.
2. **RSA Signature Option:** This option is used to protect all ND messages relating to Neighbor and Router discovery. The message which is sent from CGA address is signed with the address owner private key and attached the public key to the sent packet to enable the receiver to verify the identity of the sender. This signature prevents an attacker from spoofing NDP messages.
3. **Nonce Option:** This option is used to protect messages from replay attacks, and to ensure that an advertisement is a fresh response to a solicitation which is sent earlier by the node.
4. **Timestamp Option:** This option is used to protect the unsolicited advertisements (periodic RA and Redirect messages) from replay attacks.
5. **ICMPv6 Discovery Messages:**
    a. **Certificate Path Solicitation (CPS):** Is sent by hosts during the Authorization Delegation Discovery (ADD) process to request a certification path between a router and one of the host's trust anchors.
    b. **Certificate Path Advertisement (CPA):** Is sent in reply to the CPS message and contains the router certificate.

SEND protocol uses an ADD process to validate and authorize IPv6 routers to act as default gateways, and specifies the IPv6 prefixes that a router is authorized to announce on the link (Arkko et al., 2005). ADD relies on an electronic certificate issued by a trusted third party called Trust Anchor (TA). A TA is an entity that the node trusts to authorize routers to act as routers. A trust anchor configuration consists of a public key and some associated parameters (Arkko et al., 2005). Before any MN can accept a router as its default router, the MN must be configured with a TA(s) that can certify the router via certificate paths. The MN requests the router to provide its X.509 certificate path to a TA which is preconfigured on the node using ICMPv6 discovery message. Any router that could not provide the path to TA should not be trusted by nodes as the default router. SEND can be used to secure the local network of MN against attacks targeted at MN and the default HA using the various SEND options and ICMPv6 messages. Specifically, it can protect against router solicitation and advertisement attack, replay attack, duplicate address detection attack, neighbor solicitation and advertisement spoofing attack. SEND options could also be used to protect DHAAD messages between MN and HAs in the home network, if the trust relationship of MN and HA no longer assured.

HA-MN route require IPsec security because of established trust relationship between HA and MN. The HoTi and HoT messages require a non-NULL authentication algorithm and non-NULL encryption algorithm, with ESP protocol in tunnel mode. The binding updates and acknowledgement messages transmitted between the MN and HA require a non-NULL authentication algorithm and ESP protocol in transport mode.

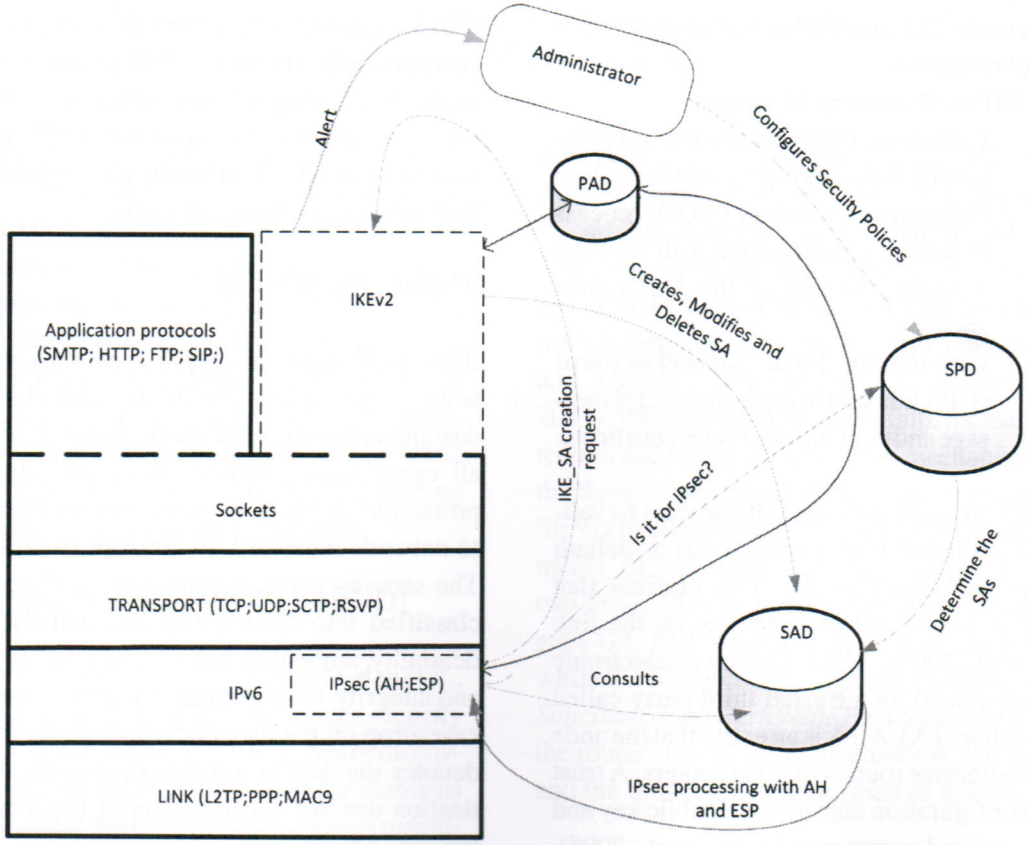
IP Security (IPsec)

IPsec is IP layer security framework consisting suite of protocols, standards, and algorithms designed to protect the traffic at the IP level and all upper layer protocols. It enables data flow protection services between host-to-host, host-to-network or network-to-network arrangements. The security services provided by IPsec can be classified into three categories namely; confidentiality, authentication with anti-replay feature and integrity. Confidentiality means no one could eavesdrop on the data communication; Integrity denotes the data is not tampered with; Authentication denotes confirmation of the identity of the data source.

IPsec as specified in Security Architecture for the Internet Protocol (Kent & Seo, 2005) consist of suite of protocols, standards, and algorithms that provide security services to the Internet communications at the IP layer that include: Security Protocols-Authentication Header (AH) and Encapsulating Security Payload (ESP), Security Associations (SAs), Cryptographic algorithms for authentication and encryption, Internet Key Exchange (IKE). HA-MN route require IPsec security because of established trust relationship between HA and MN. The HoTi and HoT messages of the RR procedure require a non-NULL authentication algorithm and non-NULL encryption algorithm, with ESP protocol in tunnel mode. The binding updates and acknowledgement messages transmitted between the MN and HA require a non-NULL authentication algorithm and ESP protocol in transport mode.

The architecture of IPsec is shown in Figure 5, consisting of AH, ESP, Security Association Database (SAD), Security Policy Database (SPD), Peer Authentication Database (PAD) and IKE in relation to the Internet Protocol stack. Security Association is a one-way agreement between two communicating peers that specifies the IPsec protections to be provided to their communications, such as cryptographic algorithms, and secret keys to be applied, as well as the specific types of traffic to be protected. SAD is repository of SAs while PAD stores information necessary to conduct remote peer authentication of identities. SPD is an ordered database that expresses the security protection policies to be afforded to inbound and outbound traffics. The three general classes of traffic policies are traffics to be discarded, traffics to be allowed without IPsec protection and traffics that requires IPsec protection.

Figure 5. IPsec architecture

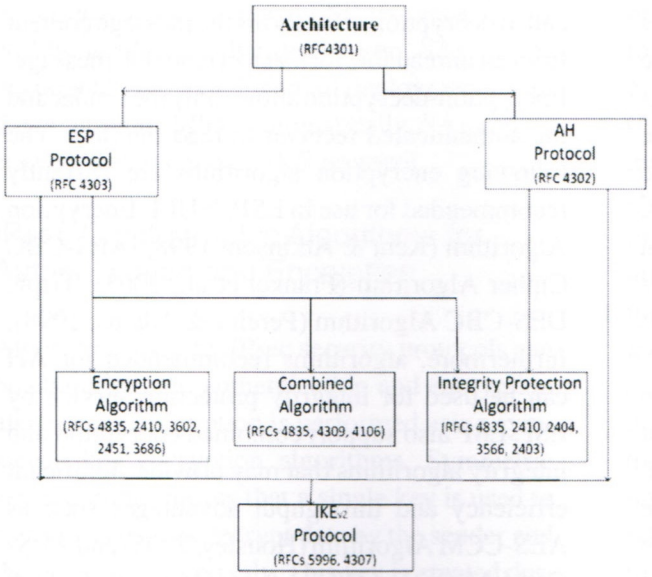


When an IP packet needs to be transmitted securely, SPD is consulted to determine if such packet is privileged to use IPsec, to be dropped or allowed without IPsec. For a privileged packet, the SA for the traffic is located in SAD and then IPsec processing with AH, ESP can start. If automated keying is to be used for IPsec processing, then IKE security association (IKE_SA) is initialized with SAs stored in SAD and IPsec processing can start.

IPsec specified in (Kent & Seo, 2005) is $IPsec_{v3}$ and obsoletes $IPsec_{v2}$. $IPsec_{v2}$, and $IPsec_{v1}$ are described in Kent and Atkinson (1998) and Atkinson (1995), respectively. The interrelationship among RFC documents that specifies the protocols, standards, and mandatory algorithms in IPsec suite is shown in Figure 6(a) with four levels.

Level one of Figure 6(a) shows the main IPsec architecture document (RFC 4301) that broadly covers the general concepts, security requirements, definitions, and mechanisms defining IPsec technology. On the next level, are ESP Protocol document (Kent, 2005b) and AH Protocol document (Kent, 2005a) that cover the packet format and general issues regarding the respective protocols. The third level consists of encryption algorithm document set specified in (Glenn & Kent, 1998; Frankel, Glenn, & Kelly, 2003; Manral, 2007). It is the set of documents describing how various encryption algorithms are used for ESP. Still on level three is the Combined Algorithm (Housley, 2005; Viega & McGrew, 2005; Manral, 2007) document set. The set of documents suggests how various combined mode algorithms are used to provide both encryption and integrity protection for ESP. The integrity protection algorithm document set (Madson & Glenn, 1998a, b; Frankel & Herbert, 2003; Manral, 2007), is the set of documents describing how various integrity protection algorithms are used for both ESP and AH. The last level shows the Key Management documents (Schiller, 2005; Eronen, Tschofenig & Sheffer, 2010), describing the IETF Standards Internet Key Exchange (IKE) protocol and cryptographic algorithms for IKE.

Figure 6. IPsec: (a) documents interrelationships, (b) cryptographic algorithms



(a)

Cryptographic algorithm	Security service	Usage status	RFC
HMAC with SHA-1	Authentication	MUST	2404
AES-XCBC-MAC-96	Authentication	SHOULD+	3566
HMAC with MD5-96	Authentication	MAY	2403
NULL	Authentication /Encryption	MUST	2410
AES-CBC Cipher	Encryption	SHOULD+	3602
Triple DES-CBC	Encryption	MUST-	2451
AES-CTR	Encryption	SHOULD	3686
AES-CCM	Encryption & Authentication	SHOULD+	4309
AES-GCM	Encryption & Authentication	-	4106
PRF_HMAC_SHA1	Key exchange	MUST	2104
PRF_AES128_CBC	Key exchange	SHOULD+	3664
1024 MO DP Group 2	Key exchange	MUST-	2409
2048 MO DP Group 14	Key exchange	SHOULD+	3526

MUST, MUST-, MAY, SHOULD and SHOULD+ are as defined in RFC2119 and RFC4835

(b)

Security Protocols

IPsec consists of two security protocols for authentication and encryption of communication between communicating hosts namely Authentication Header and Encapsulating Security Payload protocols.

Authentication Header

Authentication Header (AH) provides authentication and integrity protection, for IP packets with optional anti-replay protection against unauthorized retransmission of packets. AH protocol protects the packet's source address, destination address, and data from being modified along the route, the sender and receiver are authenticated with no data's confidentiality protection. This simply means that AH ensures users know whom they are communicating with, know if the communicated data is changed in transit but will not be sure if it is copied or eavesdropped while in transit due to absence of data encryption. The AH format consists of the following fields; *Next Header*, *Payload length*, *Reserved*, *Security Parameter Index (SPI)*, *Sequence Number*, and *Integrity Check Value (ICV)* (Kent, 2005a). Kent (2005a) provides more detail about AH format fields' description. AH guarantees authentication and integrity with the calculation of ICV over the packet's non changing contents, using a cryptographic algorithm, such as hash-based message authentication code (HMAC) with SHA-1 Algorithm (Madson & Glenn, 1998b), AES-XCBC-MAC-96 Algorithm (Frankel & Herbert, 2003), HMAC with MD5-96 Algorithm (Madson & Glenn, 1998a), NULL Encryption Algorithm (Glenn & Kent, 1998). A shared secret key employed by the cryptographic algorithm known to both ends, allows the recipient to compute the ICV value of the received packet. If the recipient gets the same ICV value, the sender has effectively authenticated itself to the receiver and validates the integrity of the received packet. The replay protection is achieved using the sequence number field in the AH structure.

The AH protocol operates in Transport Mode or Tunnel Mode. With Transport Mode, the AH header is inserted between the IP header and the upper layer headers. An attacker can learn the source and destination of packet, because IPsec in Transport mode does not shield the information in the IP header. In Tunnel Mode, the entire packet is encrypted, including its IP header, the AH header goes at the front of this and a new IP header is added in front of the AH header. Tunnel mode prevents an attacker from knowing the source and destination of packet. Transport Mode is for host-to-host communication while Tunnel Mode is for host-to-gateway and gateway-to-gateway communication.

Encapsulating Security Payload

Encapsulating Security Payload (ESP) can also operate in Transport or Tunnel Modes like AH protocol. ESP provides authentication, integrity, and confidentiality security protection against data tampering and message content protection that is absent in HA protocol using encryption algorithms (Kent, 2005b). Data encryption transforms a readable message into an unreadable format to hide the message content. The reverse process, called decryption, transforms the message content from an unreadable format to a readable message. Encryption-decryption allows only the sender and the authenticated receiver to read the data. The following encryption algorithms are currently recommended for use in ESP; NULL Encryption Algorithm (Kent & Atkinson, 1998), AES-CBC Cipher Algorithm (Frankel et al., 2003), Triple DES-CBC Algorithm (Pereira & Adams, 1998), furthermore, algorithms recommended for AH can be used for integrity protection service by ESP. ESP also support combined encryption and integrity algorithms that may provide significant efficiency and throughput advantages such as AES-CCM Algorithm (Housley, 2005) and AES-GCM Algorithm (Viega & McGrew, 2005). ESP authentication and integrity services are only for the payload and not for the IP header. AH and ESP

can be used together to secure the IP header and the packet payload, when additional protections are needed.

IPsec Security Association

The Security Association (SA) provides the method used by IPsec to track all the particulars concerning a given IPsec communication session. It provides logical relationships between two or more IPsec enabled systems that express what security services and related parameters to be used to communicate securely among them. The systems must agree on security protocol identifier (50 for ESP and 51 for AH) that are required along with other parameters, such as cryptographic algorithm, key, duration and SPI to be used for inbound and outbound connections. The SPI is a unique value identifying the SA and differentiating it from other SAs linked to the same destination address. Security Association Database (SAD) keeps all records of SA information including type of encryption or authentication algorithms, key lengths, and key lifetimes negotiated with each IPsec enabled system. There is an SA for each traffic direction. If a traffic stream in one direction uses both AH and ESP, two separate SA will be needed for that destination. SAs can be negotiated manually for small deployments with the creation of SPD. Automatically, SAs can be created with the use of IKE protocol.

IPsec Cryptographic Algorithms for Authentication and Encryption

Algorithms used by IPsec security protocols can be classified into authentication and encryption algorithms. Encryption is performed using symmetric key encryption algorithms. Symmetric key algorithm means that a single key is used to encrypt as well as decrypt data by the sender and the receiver respectively. This key is created during IKE's exchange. IPsec uses hash algorithms to compute Message Authentication Codes (MAC) for authentication and integrity check. The sender calculates the MAC of the message (M) using hash cryptographic function and attaching this hash to the end of the message. When the receiver gets the message, it again calculates a new MAC on the message and compares the hash it received and the new calculated MAC. If they are the same, the data was not tampered with in transit. There are several cryptographic algorithms available for use by IPsec, while new ones are coming up; some are no longer secured for IPsec use. Manral (2007) specifies a set of cryptographic algorithms that could be used in IPsec implementation and those that could not be used. A summary of these mandatory, recommended and optional algorithms with Request For Comment (RFC) numbers is shown in Figure 6(b). The usage status, MUST, MUST-, MAY, SHOULD are as defined in RFC2119 while SHOULD+ is defined in RFC4835.

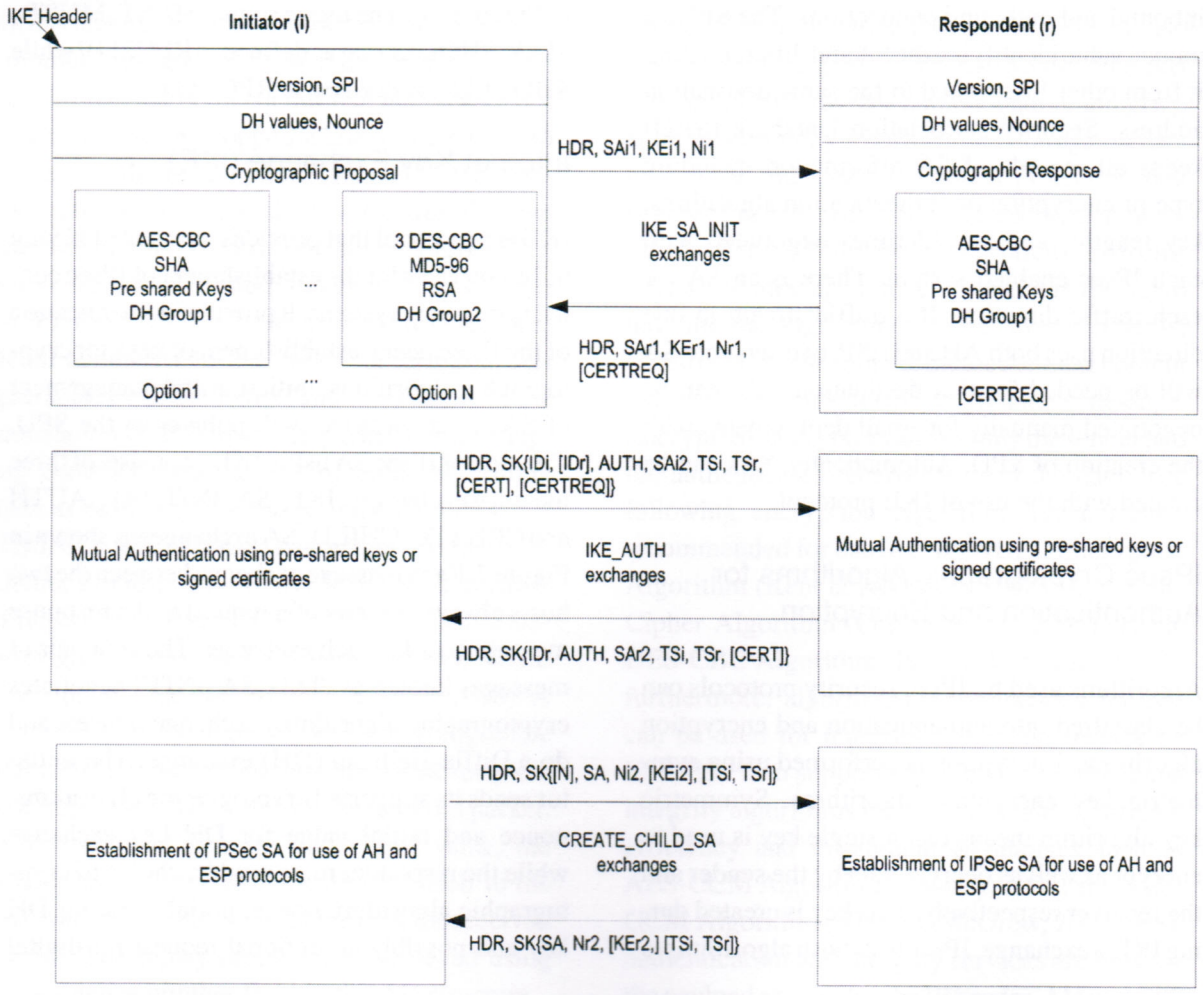
Internet Key Exchange (IKE)

IKE is a protocol that provides automated keying utility services for the establishment of IPsec connection among systems. It provides authentication of the IPsec peers, establishment of keys for cryptographic algorithms, initiation and management of SAs in accordance with policies in the SPD. Creation of IPsec SA using IKE_{v2} consists of three message exchanges: IKE_SA_INIT, IKE_AUTH and CREATE_CHILD_SA exchanges as shown in Figure 7. Each message exchange between the two hosts always consists of a request and a response message pair for each exchange. The first pair of messages known as "IKE_SA_INIT" negotiates cryptographic algorithms, exchange nonces, and do a Diffie-Hellman (DH) exchange. The initiator sends its supported cryptographic algorithms, nonce and initial value for DH key exchange while the responder must send its choice of cryptographic algorithm, nonce, initial value for DH key and possibly an optional request for digital

certificate based authentication (CERTREQ). With the first exchange completed, both parties can generate master secret key, encryption and authentication keys based on initial DH values using DH algorithm.

The second pair of messages "IKE_AUTH" authenticates the previous messages, exchange identities, traffic selectors and certificates, and establish the IKE_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE_SA_INIT exchange, so the identities of the initiator and the responder are hidden from eavesdroppers and all fields in all the messages are authenticated. The host can chose among Pre-shared secret based authentication, certificate-based authentication or Extensible Authentication Protocol (EAP)-based authentication. In certificate-based authentication, the initiator sends its signed certificate to the responder while the responder sends its signed certificate in returned. EAP-based authentication uses any of already established authentication methods such as authentication, authorization and accounting (AAA) servers (Aboba, Simon, &Eronen, 2008). No further authentication is needed if pre-shared secret is the choice and is the preferred mode in small scale environments.

Figure 7. IKE message exchanges



The CREATE_CHILD_SA is the next exchange from the initiator to the responder. The initiator sends some proposals for parameters, such as traffic selector, session key of the cryptographic algorithms which will be used for AH or ESP, the responder answers with the chosen parameters to accept the secured connection. These parameters are stored in SAD for IPsec services. This CREATE_CHILD_SA is known as IPsec SA. An established IKE SA may be used to create many IPsec SAs by including a new nonce (N) in the CREATE_CHILD_SA exchange to indicate new IPsec SA.

Securing MIPv6 Route Optimization with RR Procedure

The RR procedure overview was discussed earlier in MIPv6 Design section. RR procedure ensures that CN verifies that the MN is able to receive messages at the HoA and CoA. These verifications alleviate a number of security threats, such as flooding attacks. The procedure also eliminates the replay attack with the nonces in the computation of K_{bm}. Traffic Redirection and Traffic Hijacking attacks are mitigated by RR procedure by limiting the number of potential attackers that could spoof BU to redirect or hijack an ongoing session because the attacker must be on the route of the hijacked connection. This mitigation level is better than when every node on the Internet could be an attacker compared to few nodes on the CN-AH route. RR protocol could verify reachability of authorized nodes on CN-HA route but not address ownership and therefore could not provide totally strong security solutions to IPv6 based security threats. It was not the goal of RR to protect against attacks that were already possible before the introduction of IP mobility (Perkins et al., 2011).

Several proposals for securing BU exist such as the Early Binding Updates (EBU) protocol (Vogt, Bless, Doll, & Kuefner, 2004), Child-Proof Authentication for MIPv6 (O'Shea & Roe, 2001), Applying Cryptographically Generated Addresses to Optimize MIPv6 (Haddad, Madour, Arkko, & Dupont, 2004), Certificate-based Binding Update (CBU) protocol (Deng, Zhou, & Bao, 2002), Hierarchical Certificate-based Binding Update (HCBU) protocol (Ren et al., 2006) and many other related proposals. Most of these protocols based on CGA are computationally intensive while others are infrastructure based protocol.

Securing MIPv6 with Firewall

Firewalls are an integral aspect of a majority of IP networks that provide some security services against security threats and vulnerabilities to data networks. Firewalls are not aware of MIPv6 protocol details, will probably interfere with the smooth operation of the protocol. Therefore, smooth running of MIPv6 and security threat mitigation using firewall depend on proper implementation and configuration of firewall filtering rules. Firewall filtering rules are based on the following parameters, source IP address, destination IP address, protocol type, and source port number, destination port number to allow a traffic packet or to drop the packet.

To allow smooth operation of MIPv6 in a network, the following MIPv6 messages should be allowed by the firewall at the network perimeter (Davies & Mohacsi, 2007):

- Type 2 routing header based packets (IPv6 header type 43), Destination option header with home address option for all MN originated packets (type 201).
- Mobility headers messages (type 1-6) used by MN and HA for binding updates and acknowledgement; and RR procedure.
- ICMPv6 message type 144, 145 (HAAD request/reply).

- ICMPv6 message type 146, 147 (Mobile prefix solicitation/advertisement reply).
- ESP and AH headers are allowed according to the security policy.
- While Type 0 routing header based packets, expired binding life time packets should be dropped.

FUTURE RESEARCH DIRECTIONS

It is evident that huge and successful researches have gone into the mobility management and security concerns in MIPv6 in recent time. These concerns were not seen as weakness of MIPv6 but motivation for enhancement as evidenced in huge research output in this filed, however more research still need to be done in the following areas; Securing MN-CN route, Layer 2 handover latency enhancement, mobility of MN in Heterogeneous networks, flat MIPv6 architecture that do away with some entities such as AH, MAP, MAG, etc., authentication, authorization and accounting of MN in visited foreign network domains.

More importantly, the research into securing MN-CN route with infrastructure based security such as IPsec has been a challenge due to complexity of developing and managing global PKI to handle automatic keying needed for this form of security. HCBU protocol (Ren et al., 2006) could be a promising proposal in this regard using hierarchical PKI and possible extension to cover heterogeneous networks. This is possible due to the ongoing current standardization of Resource PKI (RPKI) framework designed to secure the Internet's routing infrastructure for Border Gateway Protocol (BGP) (Kent, Kong, Seo, & Watro, 2012).

Research into performance of mobility and multihoming management of MN in heterogeneous networks such as WiFi, General Packet Radio Services (GPRS), CDMA, LTE, WiMax, etc. is a promising area due to increasing acceptance of IP based mobility in these heterogeneous networks and an increasing proportion of mobile devices are outfitted with more than one radio access technology.

CONCLUSION

Mobility and security concerns are very important to this generation of telecommuting users due to rapid reduction in price, increase processing power, and portability of computing devices. MIPv6 has shown a remarkable potential to be the preference in mobility management of computing devices used insecure, ubiquitous mobile computing and general communication services. This chapter has presented the design and operation of MIPv6, pointing out the design and security assumptions leading to the use infrastructure less RR and SEND protocol on one hand and traditional infrastructure based IPsec protocol suite on the other hand. Management of mobility of MN in relation to CN was discussed based on IETF standardized mobility management protocols such as HMIPv6, FMIPv6, PMIPv6, FPMIPv6 and other promising proposal such as F-HMIPv6 with a summary of their performances with respect to handover latency. The standardized mobility management protocols have relative ease of implementation, security threats similar to MIPv6 and interoperability with existing Internetworking platforms than other proposed mobility management scheme for MIPv6. Sources of security concerns, security threats, and security threat counter proposals were discussed with detail explanation of the security protocols for eradicating these threats. Security wise, MIPv6 is not as vulnerable as being portrait, as most of the identified vulnerabilities have been researched with positive results and are already taken care of in the design and the implementation.

REFERENCES

Aboba, B., Simon, D., & Eronen, P. (2008). *Extensible authentication protocol (EAP) key management framework*. Internet Engineering Task Force (IETF), Request for Comments: 5247. Retrieved from http://tools.ietf.org/html/rfc5247

Arkko, J., Devarapalli, V., & Dupont, F. (2004). *Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents*. Internet Engineering Task Force (IETF), Request for Comments: 3776. Retrieved from http://tools.ietf.org/html/rfc3776

Arkko, J., Kempf, J., Zill, B., & Nikander, P. (2005). *Secure neighbor discovery (SEND)*. Internet Engineering Task Force (IETF), Request for Comments: 3971. Retrieved from http://tools.ietf.org/html/rfc3971

Atkinson, R. (1995). *Security architecture for the internet protocol*. Internet Engineering Task Force (IETF), Request for Comments: 1825. Retrieved from http://tools.ietf.org/html/rfc1825

Aura, T. (2005). *Cryptographically generated addresses (CGA)*. Internet Engineering Task Force (IETF), Request for Comments: 3972. Retrieved from http://tools.ietf.org/html/rfc3972

Aura, T., & Roe, M. (2006). Designing the mobile IPv6 security protocol. *Annales des Télécommunications*, *61*(3-4), 332–356. doi:10.1007/BF03219911.

Choi, H.-Y., Kim, K.-R., Lee, H.-B., Min, S.-G., & Han, Y.-H. (2011). Smart buffering for seamless handover in proxy mobile IPv6. *Wireless Communication and Mobile Computing*, *11*(4), 491–499. doi:10.1002/wcm.843.

Conta, A., Deering, S., & Gupta, M. (2006). *Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification*. Internet Engineering Task Force (IETF), Request for Comments: 4443. Retrieved from http://tools.ietf.org/html/rfc4443

Davies, E., & Mohacsi, J. (2007). *Recommendations for filtering ICMPv6 messages in firewalls*. Internet Engineering Task Force (IETF), Request for Comments: 4890. Retrieved from http://tools.ietf.org/html/rfc4890

Deng, R. H., Zhou, J., & Bao, F. (2002). Defending against redirect attacks in mobile IP. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, (pp. 59–67). New York, NY: ACM.

Devarapalli, V., & Dupont, F. (2007). *Mobile IPv6 operation with IKEv2 and the revised IPsec architecture*. Internet Engineering Task Force (IETF), Request for Comments: 4877. Retrieved from http://tools.ietf.org/html/rfc4877

Devarapalli, V., Wakikawa, R., Petrescu, A., & Thubert, P. (2005). *Network mobility (NEMO) basic support protocol*. Internet Engineering Task Force (IETF), Request for Comments: 3963. Retrieved from http://tools.ietf.org/html/rfc3963

Droms, R., Bound, E. J., Volz, B., Lemon, T., Perkins, C., & Carney, M. (2003). *Dynamic host configuration protocol for IPv6 (DHCPv6)*. Internet Engineering Task Force (IETF), Request for Comments: 3315. Retrieved from http://tools.ietf.org/html/rfc3315

Ernst, T. (2007). *Network mobility support goals and requirements*. Internet Engineering Task Force (IETF), Request for Comments: 4886. Retrieved from http://tools.ietf.org/html/rfc4886

Eronen, P., Tschofenig, H., & Sheffer, Y. (2010). *An extension for EAP-only authentication in IKEv2*. Internet Engineering Task Force (IETF), Request for Comments: 5998. Retrieved from http://tools.ietf.org/html/rfc5998

Frankel, S., Glenn, R., & Kelly, S. (2003). *The AES-CBC cipher algorithm and its use with IPsec*. Internet Engineering Task Force (IETF), Request for Comments: 3602. Retrieved from http://tools.ietf.org/html/rfc3602

Frankel, S., & Herbert, H. (2003). *The AES-XCBC-MAC-96 algorithm and its use with IPsec*. Internet Engineering Task Force (IETF), Request for Comments: 3566. Retrieved from http://tools.ietf.org/html/rfc3566

Glenn, R., & Kent, S. (1998). *The NULL encryption algorithm and its use with IPsec*. Internet Engineering Task Force (IETF), Request for Comments: 2410. Retrieved from http://tools.ietf.org/html/rfc2410

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., & Patil, B. (2008). *Proxy mobile IPv6*. Internet Engineering Task Force (IETF), Request for Comments: 5213. Retrieved from http://tools.ietf.org/html/rfc5213

Haddad, W., Madour, L., Arkko, J., & Dupont, J. (2004). *Applying cryptographically generated addresses to optimize MIPv6 (CGA-OMIPv6)*. Expired Internet Engineering Task Force (IETF) Internet draft. Retrieved from http://tools.ietf.org/html/draft-haddad-mip6-cga-omipv6-04

Housley, R. (2005). *Using advanced encryption standard (AES) CCM mode with IPsec encapsulating security payload (ESP)*. Internet Engineering Task Force (IETF), Request for Comments: 4309. Retrieved from http://tools.ietf.org/html/rfc4309

Jung, H., Soliman, H., Koh, S., & Lee, J. Y. (2005). *Fast handover for hierarchical MIPv6 (F-HMIPv6)*. Expired Internet Engineering Task Force (IETF) Internet draft. Retrieved from http://tools.ietf.org/html/draft-jung-mobopts-fhmipv6-00

Kaufman, C., Hoffman, P., Nir, Y., & Eronen, P. (2010). *Internet key exchange protocol version 2 (IKEv2)*. Internet Engineering Task Force (IETF), Request for Comments: 5996. Retrieved from http://tools.ietf.org/html/rfc5996

Kent, S. (2005a). *IP authentication header*. Internet Engineering Task Force (IETF), Request for Comments: 4302. Retrieved from http://tools.ietf.org/html/rfc4302

Kent, S. (2005b). *IP encapsulating security payload (ESP)*. Internet Engineering Task Force (IETF), Request for Comments: 4303. Retrieved from http://tools.ietf.org/html/rfc4303

Kent, S., & Atkinson, R. (1998). *Security architecture for the internet protocol*. Internet Engineering Task Force (IETF), Request for Comments: 2401. Retrieved from http://tools.ietf.org/html/rfc2401

Kent, S., Kong, D., Seo, K., & Watro, R. (2012). *Certificate policy (CP) for the resource public key infrastructure (RPKI)*. Internet Engineering Task Force (IETF), Request for Comments: 6484. Retrieved from http://tools.ietf.org/html/rfc6484

Kent, S., & Seo, K. (2005). *Security architecture for the internet protocol*. Internet Engineering Task Force (IETF), Request for Comments: 4301. Retrieved from http://tools.ietf.org/html/rfc4301

Koodli, R. (2009). *Mobile IPv6 fast handovers*. Internet Engineering Task Force (IETF), Request for Comments: 5568. Retrieved from http://tools.ietf.org/html/rfc5568

Madson, C., & Glenn, R. (1998a). *The use of HMAC-MD5-96 within ESP and AH*. Internet Engineering Task Force (IETF) Request for Comments: 2403. Retrieved from http://tools.ietf.org/html/rfc2403

Madson, C., & Glenn, R. (1998b). *The use of HMAC-SHA-1-96 within ESP and AH*. Internet Engineering Task Force (IETF) Request for Comments: 2404. Retrieved from http://tools.ietf.org/html/rfc2404

Manral, V. (2007). *Cryptographic algorithm implementation requirements for encapsulating security payload (ESP) and authentication header (AH)*. Internet Engineering Task Force (IETF) Request for Comments: 4835. Retrieved from http://tools.ietf.org/html/rfc4835

Na, J., Ryu, S., Lee, K., & Mun, Y. (2010). Enhanced PMIPv6 route optimization handover using PFMIPv6. *IEICE Transactions on Communications. E (Norwalk, Conn.), 93-B*(11), 3144–3147.

Narten, T., Draves, R., & Krishnan, S. (2007). *Privacy extensions for stateless address autoconfiguration in IPv6, RFC 4941*. Internet Engineering Task Force (IETF). Retrieved from http://tools.ietf.org/html/rfc4941

Narten, T., Nordmark, E., Simpson, W., & Soliman, H. (2007). *Neighbor discovery for IP version 6 (IPv6)*. IETF Request for Comments: 4861. Retrieved from http://tools.ietf.org/html/rfc4861

Nikander, P., Arkko, J., Aura, T., Montenegro, G., & Nordmark, E. (2005). *Mobile IP version 6 route optimization security design background.* Internet Engineering Task Force (IETF), Request for Comments: 4225, Dec. 2005. Retrieved from http://tools.ietf.org/html/rfc4225

Nikander, P., Kempf, J., & Nordmark, E. (2004). *IPv6 neighbor discovery (ND) trust models and threats*. Internet Engineering Task Force (IETF) Request for Comments: 3756. Retrieved from http://tools.ietf.org/html/rfc3756

O'Shea, G., & Roe, M. (2001). Child-proof authentication for MIPv6 (CAM). *SIGCOMM Computer Communications Review, 31*(2), 4–8. doi:10.1145/505666.505668.

Pereira, R., & Adams, R. (1998). *The ESP CBC-mode cipher algorithms*. Internet Engineering Task Force (IETF) Request for Comments: 2451. Retrieved from http://tools.ietf.org/html/rfc2451

Perkins, C., Johnson, D., & Arkko, J. (2011). *Mobility support in IPv6*. Internet Engineering Task Force (IETF), Request for Comments: 6275. Retrieved from http://tools.ietf.org/html/rfc6275

Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J., & Deng, R. H. (2006). Routing optimization security in mobile IPv6. *Computer Networks, 50*(13), 2401–2419. doi:10.1016/j.comnet.2005.09.019.

Ryu, S., & Mun, Y. (2005). The tentative and early binding update for mobile IPv6 fast handover. In *Proceedings of the First International Conference on Mobile Ad-Hoc and Sensor Networks*, (pp. 825–835). Berlin: Springer-Verlag.

Ryu, S., & Mun, Y. (2007). A scheme to enhance TEBU scheme of fast handovers for mobile IPv6. In *Proceedings of the 3rd International Conference on Embedded Software and Systems*, (pp. 773–782). Berlin: Springer-Verlag.

Schiller, J. (2005). *Cryptographic algorithms for use in the internet key exchange version 2 (IKEv2)*. IETF Request for Comments: 4307. Retrieved from http://tools.ietf.org/html/rfc4307

Shih, C.-H., Kuo, J.-L., Huang, C.-H., & Chen, Y.-C. (2011). A proxy-based fast handover scheme for hierarchical mobile IPv6. In *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*, (pp. 21:1–21:10). New York, NY: ACM.

Soliman, H., Castelluccia, C., ElMalki, K., & Bellier, L. (2008). *Hierarchical mobile IPv6 (HMIPv6) mobility management*. Internet Engineering Task Force (IETF), Request for Comments: 5380. Retrieved from http://tools.ietf.org/html/rfc5380

Thomson, S., Narten, T., & Jinmei, T. (2007). *IPv6 stateless address autoconfiguration*. RFC 4862. Internet Engineering Task Force (IETF). Retrieved from http://tools.ietf.org/html/rfc4862

Viega, J., & McGrew, D. (2005). *The use of galois/counter mode (GCM) in IPsec encapsulating security payload (ESP)*. IETF Request for Comments: 4106. Retrieved from http://tools.ietf.org/html/rfc4106

Vogt, C., Bless, R., Doll, M., & Kuefner, T. (2004). *Early binding updates for mobile IPv6*. Expired Internet Engineering Task Force (IETF) Internet draft. Retrieved from http://tools.ietf.org/html/draft-vogt-mip6-early-binding-updates-00

Yokota, H., Chowdhury, K., Koodli, R., Patil, B., & Xia, F. (2010). *Fast handovers for proxy mobile IPv6*. Internet Engineering Task Force (IETF), Request for Comments: 5949. Retrieved from http://tools.ietf.org/html/rfc5949

Yoo, H., Tolentino, R. S., Park, B., Chang, B. Y., & Kim, S.-H. (2009). ES-FHMIPv6: An efficient scheme for fast handover over HMIPv6 networks. *International Journal of Future Generation Communication and Networking*, *2*(2), 11–24.

ADDITIONAL READING

Bernardos, C. J., Soto, I., & Calderón, M. (2007). IPv6 network mobility. *The Internet Protocol*, *10*(2), 16–27.

Elgoarany, K., & Eltoweissy, M. (2007). Security in mobile IPv6: A survey. *Elsevier Information Security Technical Report*, *12*, 32–43. doi:10.1016/j.istr.2007.02.002.

Faigl, Z., Lindskog, S., & Brunstrom, A. (2010). Performance evaluation of IKEv2 authentication methods in next generation wireless networks. *Security Communications Networks*, *3*, 83–98. doi: doi:10.1002/sec.114.

Hogg, S., & Vyncke, E. (2008). *IPv6 security*. Indianapolis, IN: Cisco Press.

Kim, H., & Kim, Y. (2006). An early binding fast handover for high-speed mobile nodes on MIPv6 over connectionless packet radio link. In *Proceedings of the Seventh International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (pp. 237–242). Las Vegas, NV: IEEE Computer. doi:10.1109/SNPD-SAWN.2006.17

Park, J. T., & Chun, M. N. (2011). Extension of hierarchical mobility management with multicasting tunnels in heterogeneous wireless networks. In *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication*. Seoul, Korea: ACM. doi:10.1145/1968613.1968640

Sousa, B. M., Pentikousis, K., & Curado, M. (2011). Multihoming management for future networks. *Mobile Network Application Journal*, *16*(4), 505–517. doi:10.1007/s11036-011-0323-5.

Wei, A., Wei, G., & Dupeyrat, G. (2009). Improving mobile IPv6 handover and authentication in wireless network with E-HCF. *International Journal of Network Management, 19*(6), 479–489. doi:10.1002/nem.723.

You, Y. H., & Sakurai, K. (2011). Enhancing SVO logic for mobile IPv6 security protocols. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*, 26–52.

Zhou, H., Zhang, H., Qin, Y., Wang, H., & Chao, H. C. (2010). A proxy mobile IPv6 based global mobility management architecture and protocol. *Mobile Networks and Applications, 15*, 530–542. doi:10.1007/s11036-009-0185-2.

KEY TERMS AND DEFINITIONS

Handover Latency: Is the time interval between an MN detaching from its current network to when it first receive packets in the new attached network.

HMIPv6: Is an extension to MIPv6 that support mobility of IPv6 based host device with enhanced performance than basic MIPv6.

IKEv2: Internet Key Exchange version two is an application layer abstraction that provides automatic keying services used by IPsec security protocols.

IPsec: Is an inbuilt set of security protocol in IPv6 for securing communication between two communicating parties to prevent security attacks.

MIPv6: Is the mobility management protocol designed for IPv6 based devices that are capable of moving from one network to the other transparently in the Internet without disruption to ongoing communication.

PMIPv6: Is an extension to MIPv6 that support mobility of IPv6 based host device. This support is provided by the network rather than the host device itself as contrasted from MIPv6 and HMIPv6 that are host-based support.

Route Optimization: Is the removal of triangular routing of packets from a correspondent mobile device destined to a mobile device that has roamed to a foreign network by its home network router known as home agent.

SEND: Is a security protocol that is used to secure automatic address configuration procedures of hosts and routers in a network against address spoofing related attacks.

APPENDIX

List of Abbreviations

- **AC:** Address Configuration
- **ADD:** Authorization Delegation Discovery
- **AH:** Authentication Header
- **AP:** Access Point
- **AP-ID:** Access Point ID
- **AR:** Access Router
- **AR:** Access Router
- **AR:** Access Router
- **BA:** Binding Acknowledgment message
- **BU:** Binding Update message
- **CGA:** Cryptographically Generated Addresses
- **CN:** Correspondent Node
- **CoA:** Care of Address
- **CoT:** Care-of Test message
- **DAD:** Duplicate Address Detection
- **DHAAD:** Dynamic Home Agent Address Discovery
- **DHCPv6:** Dynamic Host Configuration Protocol for IPv6
- **DoS:** Denial of Service
- **EAP:** Extensible Authentication Protocol
- **ESP:** Encapsulated Security Payload
- **FBack:** Fast Binding Acknowledgement
- **FBU:** Fast Binding Update ()
- **F-HMIPv6:** Fast Handovers for Hierarchical MIPv6
- **FMIPv6:** Fast Handover MIPv6
- **FPMIPv6:** Fast Handovers for Proxy MIPv6
- **HA:** Home Agent
- **HMAC:** Hash-Based Message Authentication Code
- **HMIPv6:** Hierarchical MIPv6
- **HoA:** Home Address
- **HoT:** Home Test message
- **ICMPv6:** Internet Control Message Protocol for IPv6
- **ICV:** Integrity Check Value
- **IDi; IDr:** Identification of the initiator; Identification of the responder
- **IKE:** Internet Key Exchange ()
- **IKE_SA:** IKE security association
- **IPsec:** IP security
- **Kbm:** Binding management key
- **Kcn:** Node Key
- **KE:** Diffie-Hellman values Key Exchange

- **LCoA:** On-Link CoA
- **LMA:** Local Mobility Anchor
- **LTE:** Long Time Evolution
- **MAG:** Mobility Access Gateway
- **MAP:** Mobility Anchor Point
- **MD:** Movement Detection
- **MIPv6:** Mobile IPv6
- **MN:** Mobile Node
- **MR:** Mobile Router
- **N:** Negotiation of new IPsec SA
- **NAR:** New Access Router
- **NCoA:** New CoA
- **NDP:** Neighbor Discovery Protocol
- **NEMO:** Network Mobility
- **Ni; Nr:** Nonce of initiator; Nonce of responder
- **Nonce:** Random value for freshness
- **PAD:** Peer Authentication Database
- **PAR:** Previous Access Router
- **PCoA:** Previous CoA
- **PCoA:** Proxy CoA
- **PFMIPv6:** Proxy-Based Fast Handovers for Mobile IPv6
- **PKI:** Public Key Infrastructure
- **PMIPv6:** Proxy MIPv6
- **PrRtAdv:** Proxy Router Advertisement
- **RA:** Router Advertisement
- **RCoA:** Regional CoA
- **RO:** Route Optimization
- **RR:** Return Routability Protocol
- **RS:** Router Solicitation
- **RtSolPr:** Router Solicitation for Proxy Advertisement
- **SA:** Security Association proposal; SAi2 and SAr2 are negotiations of IPSec SA algorithms.
- **SAD:** Security Association Database
- **SEND:** SEcure Neighbor Discovery
- **SK{}:** Encrypted payload
- **SLAAC:** Stateless Address Auto-configuration
- **SPD:** Security Policy Database
- **SPI:** Security Parameter Index
- **TA:** Trust Anchor
- **TSi; TSr:** Traffic Selector of the initiator; Traffic Selector of the responder
- **WiFi:** Wireless Fidelity (IEEE 802.11x)
- **WiMax:** Worldwide Interoperability for Microwave Access